

GE Healthcare

MUSE™ v9

Cardiology Information System
Devices and Interfaces Instruction Manual
2059568-013 J



MUSE v9 Cardiology Information System
English
© 2015-2019 General Electric Company.
All Rights Reserved.

Publication Information

The information in this document applies only to MUSE Cardiology Information System Version 9.0. It does not apply to earlier product versions. Due to continuing product innovation, specifications in this document are subject to change without notice.

MUSE, MARS, CASE, and MACCRA 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	18 March 2015	Initial release.
B	17 July 2015	Customer release.
C	1 September 2015	Change made to support HCSDM00336108.
D	16 October 2015	Updated to include information for the MUSE v9 DICOM.
E	23 May 2016	Updates to support HCSDM00401589. Updated the Configure the System DICOM Modality Worklist Client Service section.
F	1 December 2016	Updates to support HCSDM00433985.
G	30 June 2017	Updated to support HCSDM00436636.
H	5 October 2018	Updated to support HCSDM00528040.
J	13 March 2019	Updated to support HCSDM00547818

To access other GE Healthcare Diagnostic Cardiology documents, go to the Common Documentation Library (CDL), located at 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 qualified GE Healthcare service engineers and third-party service engineers authorized by GE Healthcare.

NOTE:

Do not attempt to install the MUSE system devices and interfaces if you are not part of the intended audience or have not read and understood these instructions in their entirety.

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)	<p>This service manual is available in English only.</p> <ul style="list-style-type: none"> • If a customer's service provider requires a language other than English, it is the customer's responsibility to provide translation services. • Do not attempt to service the equipment unless this service manual has been consulted and is understood. • Failure to heed this warning may result in injury to the service provider, operator, or patient, from electric shock, mechanical or other hazards.
ПРЕДУПРЕЖДЕНИЕ (BG)	<p>Това упътване за работа е налично само на английски език.</p> <ul style="list-style-type: none"> • Ако доставчикът на услугата на клиента изиска друг език, задължение на клиента е да осигури превод. • Не използвайте оборудването, преди да сте се консултирали и разбрали упътването за работа. • 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.
警告 (ZH-CN)	<p>本维修手册仅提供英文版本。</p> <ul style="list-style-type: none"> • 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。 • 未详细阅读和完全理解本维修手册之前，不得进行维修。 • 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。
警告 (ZH-TW)	<p>本維修手冊只提供英文版。</p> <ul style="list-style-type: none"> • 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。 • 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。 • 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。
UPOZORENJE (HR)	<p>Ove upute za servisiranje dostupne su samo na engleskom jeziku.</p> <ul style="list-style-type: none"> • Ukoliko korisnički servis zahtijeva neki drugi jezik, korisnikova je odgovornost osigurati odgovarajući prijevod. • Nemojte pokušavati servisirati opremu ukoliko niste konzultirali i razumjeli ove upute. • Nepoštivanje ovog upozorenja može rezultirati ozljedama servisnog osoblja, korisnika ili pacijenta prouzročenim električnim udarom te mehaničkim ili nekim drugim opasnostima.
VAROVÁNÍ (CS)	<p>Tento provozní návod existuje pouze v anglickém jazyce.</p> <ul style="list-style-type: none"> • V případě, že externí služba zákazníkům potřebuje návod v jiném jazyce, je zajištění překladu do odpovídajícího jazyka úkolem zákazníka. • Nesnažte se o údržbu tohoto zařízení, aniž byste si přečetli tento provozní návod a pochopili jeho obsah. • 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.

Service Manual Language Information (cont'd.)

ADVARSEL (DA)	<p>Denne servicemanual findes kun på engelsk.</p> <ul style="list-style-type: none"> • Hvis en kundes tekniker har brug for et andet sprog end engelsk, er det kundens ansvar at sørge for oversættelse. • Forsøg ikke at servicere udstyret medmindre denne servicemanual har været konsulteret og er forstået. • Manglende overholdelse af denne advarsel kan medføre skade på grund af elektrisk, mekanisk eller anden fare for teknikeren, operatøren eller patienten.
WAARSCHUWING (NL)	<p>Deze service manual is alleen in het Engels verkrijgbaar.</p> <ul style="list-style-type: none"> • Indien het onderhoudspersoneel een andere taal nodig heeft, dan is de klant verantwoordelijk voor de vertaling ervan. • Probeer de apparatuur niet te onderhouden voordat deze service manual geraadpleegd en begrepen is. • 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.
HOIATUS (ET)	<p>Käesolev teenindusjuhend on saadaval ainult inglise keeles.</p> <ul style="list-style-type: none"> • Kui klienditeeninduse osutaja nõuab juhendit inglise keelest erinevas keeles, vastutab klient tõlketeenuse osutamise eest. • Ärge üritage seadmeid teenindada enne eelnevalt käesoleva teenindusjuhendiga tutvumist ja sellest aru saamist. • Käesoleva hoiatuse eiramine võib põhjustada teenuseosutaja, operaatori või patsiendi vigastamist elektrilöögi, mehaanilise või muu ohu tagajärjel.
VAROITUS (FI)	<p>Tämä huolto-ohje on saatavilla vain englanniksi.</p> <ul style="list-style-type: none"> • Jos asiakkaan huoltohenkilöstö vaatii muuta kuin englanninkielistä materiaalia, tarvittavan käännöksen hankkiminen on asiakkaan vastuulla. • Älä yritä korjata laitteistoa ennen kuin olet varmasti lukenut ja ymmärtänyt tämän huolto-ohjeen. • Mikäli tätä varoitusta ei noudateta, seurauksena voi olla huoltohenkilöstön, laitteiston käyttäjän tai potilaan vahingoittuminen sähköiskun, mekaanisen vian tai muun vaaratilanteen vuoksi.
ATTENTION (FR)	<p>Ce manuel technique n'est disponible qu'en anglais.</p> <ul style="list-style-type: none"> • 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. • Ne pas tenter d'intervenir sur les équipements tant que le manuel technique n'a pas été consulté et compris. • 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.

Service Manual Language Information (cont'd.)

<p>WARNUNG (DE)</p>	<p>Diese Serviceanleitung ist nur in englischer Sprache verfügbar.</p> <ul style="list-style-type: none"> Falls der Kundendienst eine andere Sprache benötigt, muss er für eine entsprechende Übersetzung sorgen. Keine Wartung durchführen, ohne diese Serviceanleitung gelesen und verstanden zu haben. Bei Zuwiderhandlung kann es zu Verletzungen des Kundendiensttechnikers, des Anwenders oder des Patienten durch Stromschläge, mechanische oder sonstige Gefahren kommen.
<p>ΠΡΟΕΙΔΟΠΟΙΗΣΗ (EL)</p>	<p>Το παρόν εγχειρίδιο σέρβις διατίθεται στα αγγλικά μόνο.</p> <ul style="list-style-type: none"> Εάν το άτομο παροχής σέρβις ενός πελάτη απαιτεί το παρόν εγχειρίδιο σε γλώσσα εκτός των αγγλικών, αποτελεί ευθύνη του πελάτη να παρέχει υπηρεσίες μετάφρασης. Μην επιχειρήσετε την εκτέλεση εργασιών σέρβις στον εξοπλισμό εκτός εάν έχετε συμβουλευτεί και έχετε κατανοήσει το παρόν εγχειρίδιο σέρβις. 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.
<p>FIGYELMEZTETÉS (HU)</p>	<p>Ez a szerviz kézikönyv kizárólag angol nyelven érhető el.</p> <ul style="list-style-type: none"> Ha a vevő szerviz ellátója angoltól eltérő nyelvre tart igényt, akkor a vevő felelőssége a fordítás elkészítése. Ne próbálja elkezdni használni a berendezést, amíg a szerviz kézikönyvben leírtakat nem értelmezték és értették meg. Ezen figyelmeztetés figyelmen kívül hagyása a szerviz ellátó, a működtető vagy a páciens áramütés, mechanikai vagy egyéb veszélyhelyzet miatti sérülését eredményezheti.
<p>AÐVÖRUN (IS)</p>	<p>Þessi þjónustuhandbók er eingöngu fáanleg á ensku.</p> <ul style="list-style-type: none"> Ef að þjónustuveitandi viðskiptamanns þarfnast annars tungumáls en ensku, er það skylda viðskiptamanns að skaffa tungumálþjónustu. Reynið ekki að afgreiða tækið nema þessi þjónustuhandbók hefur verið skoðuð og skilin. Brot á að sinna þessari aðvörun getur leitt til meiðsla á þjónustuveitanda, stjórnanda eða sjúklingi frá raflosti, vélrænum eða öðrum áhættum.
<p>PERINGATAN (ID)</p>	<p>Manual servis ini hanya tersedia dalam bahasa Inggris.</p> <ul style="list-style-type: none"> Jika penyedia jasa servis pelanggan memerlukan bahasa lain selain dari Bahasa Inggris, merupakan tanggung jawab dari penyedia jasa servis tersebut untuk menyediakan terjemahannya. Jangan mencoba melakukan servis terhadap perlengkapan kecuali telah membaca dan memahami manual servis ini. Mengabaikan peringatan ini bisa mengakibatkan cedera pada penyedia servis, operator, atau pasien, karena terkena kejutan listrik, bahaya mekanis atau bahaya lainnya.

Service Manual Language Information (cont'd.)

AVVERTENZA (IT)	<p>Il presente manuale di manutenzione è disponibile soltanto in Inglese.</p> <ul style="list-style-type: none"> Se un addetto alla manutenzione richiede il manuale in una lingua diversa, il cliente è tenuto a provvedere direttamente alla traduzione. Si proceda alla manutenzione dell'apparecchiatura solo dopo aver consultato il presente manuale ed averne compreso il contenuto. 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.
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"> 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。 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。 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。
CẢNH BÁO (VI)	<p>Tài Liệu Hướng Dẫn Sửa Chữa chỉ có bản tiếng Anh.</p> <ul style="list-style-type: none"> 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. Không được sửa chữa thiết bị trừ khi đã tham khảo và hiểu Tài liệu Hướng dẫn Sửa chữa. 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.
ЕСКЕРТУ (KK)	<p>Бұл қызмет көрсету бойынша нұсқаулығы тек ағылшын тілінде қолжетімді.</p> <ul style="list-style-type: none"> Тұтынушының қызмет провайдері ағылшын тілінен басқа тілдегі нұсқаны талап етсе, аудару бойынша қызметтерімен қамтамасыз ету тұтынушы жауапкершілігінде болуы тиіс. Бұл қызмет көрсету бойынша нұсқаулығын назарға алып, түсінбегенше, жабдыққа қызмет көрсетуден бас тартыңыз. Бұл ескертуді елемей қызмет провайдері, оператор немесе емделушінің электр шоғынан, механикалық немесе басқа қауіптер нәтижесінде жарақат алуына әкелуі мүмкін.
BRĪDINĀJUMS (LV)	<p>Šī apkalpotāju rokasgrāmata ir pieejama tikai anglu valodā.</p> <ul style="list-style-type: none"> Ja apkalpošanas sniedzējam nepieciešama informācija citā, nevis anglu, valodā, klienta pienākums ir nodrošināt tās tulkošanu. Neveiciet aprīkojuma apkopi, neizlasot un nesaprotot apkalpotāju rokasgrāmatu. Šī brīdinājuma neievērošana var radīt elektriskās strāvas trieciena, mehānisku vai citu risku izraisītu traumu apkopes sniedzējam, operatoram vai pacientam.
ISPĖJIMAS (LT)	<p>Šis eksploatavimo vadovas yra prieinamas tik anglų kalba.</p> <ul style="list-style-type: none"> Jei kliento paslaugų tiekėjas reikalauja vadovo kita kalba - ne anglų, numatyti vertimo paslaugas yra kliento atsakomybė. Nemėginkite atlikti įrangos techninės priežiūros, nebent atsižvelgėte į šį eksploatavimo vadovą ir jį supratote. Jei neatkreipsite dėmesio į šį perspėjimą, galimi sužalojimai dėl elektros šoko, mechaninių ar kitų paslaugų tiekėjui, operatoriui ar pacientui.

Service Manual Language Information (cont'd.)

ADVARSEL (NO)	<p>Denne servicehåndboken finnes bare på engelsk.</p> <ul style="list-style-type: none"> • Hvis kundens serviceleverandør trenger et annet språk, er det kundens ansvar å sørge for oversettelse. • Ikke forsøk å reparere utstyret uten at denne servicehåndboken er lest og forstått. • Manglende hensyn til denne advarselen kan føre til at serviceleverandøren, operatøren eller pasienten skades på grunn av elektrisk støt, mekaniske eller andre farer.
OSTRZEŻENIE (PL)	<p>Niniejszy podręcznik serwisowy dostępny jest jedynie w języku angielskim.</p> <ul style="list-style-type: none"> • Jeśli dostawca usług klienta wymaga języka innego niż angielski, zapewnienie usługi tłumaczenia jest obowiązkiem klienta. • Nie należy serwisować wyposażenia bez zapoznania się i zrozumienia niniejszego podręcznika serwisowego. • Niezastosowanie się do tego ostrzeżenia może spowodować urazy dostawcy usług, operatora lub pacjenta w wyniku porażenia elektrycznego, zagrożenia mechanicznego bądź innego.
AVISO (PT-BR)	<p>Este manual de assistência técnica só se encontra disponível em inglês.</p> <ul style="list-style-type: none"> • 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. • Não tente reparar o equipamento sem ter consultado e compreendido este manual de assistência técnica. • O não cumprimento deste aviso pode por em perigo a segurança do técnico, operador ou paciente devido a choques elétricos, mecânicos ou outros.
AVISO (PT-PT)	<p>Este manual técnico só se encontra disponível em inglês.</p> <ul style="list-style-type: none"> • Se a assistência técnica do cliente solicitar estes manuais noutro idioma, é da responsabilidade do cliente fornecer os serviços de tradução. • Não tente reparar o equipamento sem ter consultado e compreendido este manual técnico. • O não cumprimento deste aviso pode provocar lesões ao técnico, ao utilizador ou ao paciente devido a choques eléctricos, mecânicos ou outros.
AVERTISMENT (RO)	<p>Acest manual de service este disponibil numai în limba engleză.</p> <ul style="list-style-type: none"> • Dacă un furnizor de servicii pentru clienți necesită o altă limbă decât cea engleză, este de datoria clientului să furnizeze o traducere. • Nu încercați să reparați echipamentul decât ulterior consultării și înțelegerii acestui manual de service. • Ignorarea acestui avertisment ar putea duce la rănirea depanatorului, operatorului sau pacientului în urma pericolelor de electrocutare, mecanice sau de altă natură.
ПРЕДУПРЕЖДЕНИЕ (RU)	<p>Настоящее руководство по обслуживанию предлагается только на английском языке.</p> <ul style="list-style-type: none"> • Если сервисному персоналу клиента необходимо руководство не на английском, а на каком-то другом языке, клиенту следует обеспечить перевод самостоятельно. • Прежде чем приступать к обслуживанию оборудования, обязательно обратитесь к настоящему руководству и внимательно изучите изложенные в нем сведения. • Несоблюдение требований данного предупреждения может привести к тому, что специалисты по обслуживанию, операторы или пациенты получат удар электрическим током, механическую травму или другое повреждение.

Service Manual Language Information (cont'd.)

UPOZORENJE (SR)	<p>Ovo servisno uputstvo je dostupno samo na engleskom jeziku.</p> <ul style="list-style-type: none"> Ako klijentov serviser zahteva neki drugi jezik, klijent je dužan da obezbedi prevodilačke usluge. Ne pokušavajte da opravite uređaj ako niste pročitali i razumeli ovo servisno uputstvo. Zanemarivanje ovog upozorenja može dovesti do povređivanja serviser, rukovaoca ili pacijenta usled strujnog udara, ili mehaničkih i drugih opasnosti.
VAROVANIE (SK)	<p>Tento návod na obsluhu je k dispozícii len v angličtine.</p> <ul style="list-style-type: none"> Ak zákazníkov poskytovateľ služieb vyžaduje iný jazyk ako angličtinu, poskytnutie prekladateľských služieb je zodpovednosťou zákazníka. Nepokúšajte sa o obsluhu zariadenia skôr, ako si neprečítate návod na obsluhu a neporozumiete mu. Zanedbanie tohto varovania môže vyústiť do zranenia poskytovateľa služieb, obsluhujúcej osoby alebo pacienta elektrickým prúdom, mechanickým alebo iným nebezpečenstvom.
OPOZORILO (SL)	<p>Ta servisni priročnik je na voljo samo v angleškem jeziku.</p> <ul style="list-style-type: none"> Če ponudnik storitve stranke potrebuje priročnik v drugem jeziku, mora stranka zagotoviti prevod. Ne poskušajte servisirati opreme, če tega priročnika niste v celoti prebrali in razumeli. Če tega opozorila ne upoštevate, se lahko zaradi električnega udara, mehanskih ali drugih nevarnosti poškoduje ponudnik storitev, operater ali bolnik.
ADVERTENCIA (ES)	<p>Este manual de servicio sólo existe en inglés.</p> <ul style="list-style-type: none"> 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. No se deberá dar servicio técnico al equipo, sin haber consultado y comprendido este manual de servicio. 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.
VARNING (SV)	<p>Den här servicehandboken finns bara tillgänglig på engelska.</p> <ul style="list-style-type: none"> Om en kunds servicetekniker har behov av ett annat språk än engelska ansvarar kunden för att tillhandahålla översättningstjänster. Försök inte utföra service på utrustningen om du inte har läst och förstår den här servicehandboken. 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.
UYARI (TR)	<p>Bu servis kılavuzunun sadece İngilizcesi mevcuttur.</p> <ul style="list-style-type: none"> Eğer müşteri teknisyeni bu kılavuzu İngilizce dışında bir başka lisandan talep ederse, bunu tercüme ettirmek müşteriye düşer. Servis kılavuzunu okuyup anlamadan ekipmanlara müdahale etmeyiniz. Bu uyarıya uyulmaması, elektrik, mekanik veya diğer tehlikelerden dolayı teknisyen, operatör veya hastanın yaralanmasına yol açabilir.

Service Manual Language Information (cont'd.)

<p>ЗАСТЕРЕЖЕННЯ (UK)</p>	<p>Дане керівництво з сервісного обслуговування постачається виключно англійською мовою.</p> <ul style="list-style-type: none">• Якщо сервісний інженер потребує керівництво іншою мовою, користувач зобов'язаний забезпечити послуги перекладача.• Не намагайтеся здійснювати технічне обслуговування даного обладнання, якщо ви не читали, або не зрозуміли інформацію, надану в керівництві з сервісного обслуговування.• 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.
<p>CẢNH BÁO (VI)</p>	<p>Tài Liệu Hướng Dẫn Sửa Chữa chỉ có bản tiếng Anh.</p> <ul style="list-style-type: none">• 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.• Không được sửa chữa thiết bị trừ khi đã tham khảo và hiểu Tài liệu Hướng dẫn Sửa chữa.• 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.

Contents

1	Introduction	
	Manual Purpose	17
	Related Documents.....	17
2	CASE to MUSE Communication	
	Theory of Operation	19
	Information Transmission.....	19
	Communication Levels	20
	Configuration Requirements.....	20
	Customer Requirements	20
	Communication Level Requirements	20
	Considerations When Using Multiple CASE Systems	21
	Process Overview	21
	Adding the Stress Exercise Option to the MUSE System	22
	MUSE User and Shared Acquisition Folder	23
	Creating the MUSE Acq Users Local Windows Group.....	23
	Creating the CASE8000 Windows User.....	24
	Creating the CASE8000 Windows Share	24
	Adding the User to the MUSE Web Users Group	25
	Creating a MUSE User	25
	Configuring the CASE System Network Settings	26
	Configuring MUSE System Settings on the CASE System	27
	Configuring CASE Reports on the MUSE File Server	31
	System Checkout	33
	Verifying Record Transfer	33
	Verifying Requests for Data.....	34
	Verifying the Retrieval of Patient Demographics	34
	Verifying the Retrieval of Orders	34
	Troubleshooting	35
3	MARS to MUSE Communication	
	Theory of Operation	37
	MUSE Services	37

	Information Transmission.....	38
	Customer Requirements	38
	Configuring MARS to MUSE Communication.....	38
	Configuring the MARS System Network Settings	39
	Verifying the MARS Software Version	39
	Recording the IP Address or Host Name of the MARS System	39
	Verifying the MARS Reports Share.....	39
	Activating the MARS to MUSE Option on the MARS System(s).....	40
	Setting Up the Site Information on the MARS System(s).....	40
	Adding the Holter Data Storage Option to the MUSE System	41
	Adding the MARS System to the MUSE Generacq Configuration	42
	Installing the MARS Print Formatter.....	43
	Creating site.ini for the MARS Print Formatter.....	45
	Copying the rusty.ini Configuration File from the MARS System to the MUSE System.....	46
	System Checkout	46
	Saving a Report on the MARS System	46
	Sending a MARS Holter Report to the MUSE System	47
	Viewing a MARS Holter Report in the MUSE Editor	47
	Printing MARS Holter Reports from the MUSE System.....	48
	Troubleshooting	48
4	MUSE Monitoring Gateway	
	Theory of Operation.....	51
	Information Transmission.....	52
	Installing the MUSE Monitoring Gateway	52
	Preparing for the Installation of the MUSE Monitoring Gateway.....	53
	Verifying and Configuring Network Connections	53
	Firewall Considerations.....	54
	Creating a Share on the MUSE Monitoring Gateway.....	54
	Installing the MUSE Monitoring Gateway Software	55
	Configuring the MUSE Monitoring Gateway Software	55
	Configuring the MUSE Application Server.....	56
	Configuring Bedside Monitors.....	57
	System Checkout	57
	Troubleshooting	58
	Uninstalling MUSE Monitoring Gateway v1.1.....	59
5	MAC ECG Systems to MUSE Communication	
	Theory of Operation.....	61
	Customer Requirements	62
	Configuring MAC ECG to MUSE Communication	62
	Setting Up Modems	63
	Adding the Wireless/LAN Communication Option to the MUSE System.....	63
	Verifying/Installing the MUSE Modem Service	64

	Setting Up a Modem Device	67
	Restarting Modems	68
	Setting Up DCP Inbound Communication	69
	Verifying/Installing the DCP Inbound Service and DCP Communication Option	69
	Setting Up the DCP Server Configuration in the MUSE System.....	70
	System Checkout	71
	CSI Transmission to the MUSE System	71
	MUSE Order Download via CSI.....	72
	DCP Transmission to the MUSE System	72
	MUSE Order Download via DCP.....	72
6	MUSE eDoc Connect	
	Theory of Operation	73
	Preparing to Configure eDoc Connect	74
	Customer Requirements	74
	Installing and Configuring MUSE eDoc Connect	74
	Installing the eDoc Connect Option in the MUSE System	75
	Adding or Enabling a Test Type in the MUSE System	75
	Setting up the Acquisition Profile in the MUSE System	76
	Setting up the File Share	77
	System Checkout	78
	Troubleshooting	79
7	MUSE XML Import Option	
	Theory of Operation	81
	Customer Requirements	81
	Installing and Configuring the MUSE XML Import Option	81
	Installing the XML Import Option and the MUSE XML Parser Service	82
	Setting up the XML Shared Folder.....	83
	Using XMLCONFIG.EXE to Add, Update, or Delete XML Devices.....	83
	System Checkout	87
	Troubleshooting	87
8	DICOM Communication	
	Theory of Operation	89
	Transmission Flow Charts.....	90
	MUSE Services	91
	Customer Requirements	91
	Configuring DICOM Communication.....	91
	Adding the DICOM Service(s) and Option to the MUSE System.....	92
	Configuring the MUSE System to Receive DICOM Tests	93
	Configuring the System to Send DICOM Tests.....	95

	Configuring the System to Query for DICOM Orders	99
	System Checkout	102
	Receiving DICOM Tests into the MUSE System	102
	Sending DICOM Tests from the MUSE System	102
	Querying for DICOM Orders	102
	Troubleshooting	102
9	MUSEAPI3 Installation	
	Theory of Operation	106
	Pre-Installation Instructions	106
	Determining Whether MUSEAPI3 is Already Installed	106
	Determining the Communication Protocol(s) that MUSEAPI3 Uses	107
	Determining the Port Assignments for MUSEAPI3	107
	Locating the MUSE Application Folder on the MUSE Server	107
	Installing MUSEAPI3	107
	Changing the MUSEAPI3 Service Protocol Configuration	112
	Removing MUSEAPI3	113
	Restoring the MUSEAPI3 Configuration	114
	MUSE API Test Client	114
	Running the MUSE API Test Client	114
	Using the MUSE API Test Client	114
	Configuring SSL Certificate for the MUSEAPI3 Port	115
10	MUSE Web Compatibility Layer	
	Theory of Operation	117
	System Requirements	117
	Required Internet Information Services (IIS) for the MUSE Web Compatibility Layer	118
	Installing the MUSE Web Compatibility Layer	119
	Creating a MUSE User for the MUSE Web Compatibility Layer Website	120
	Installing and Configuring the MUSE Web Compatibility Layer	121
	Adding Users to the MUSEWebCompatibilityLayer Website	124
	System Checkout	124
	Changing the MUSE Web Compatibility Layer Configuration Settings	127
	Manual Corrections for MUSE Web Compatibility Layer Installer	128
	No login prompt or HTTP Error 401.2 when accessing the MUSE Web Compatibility Layer website	128
	HTTP Error 404.0 When Accessing the MUSE Web Compatibility Layer Website	128

Troubleshooting	129
Uninstalling the MUSE Web Compatibility Layer	130
Creating an Additional MUSE Web Compatibility Layer Website.....	131
Disabling Directory Browsing for MUSE Web Compatibility Layer.....	133
IIS Unlisted File Name Extension Configuration for MUSE Web Compatibility Layer	133
Manually Installing and Verifying IIS Related Roles, Role Services, and Features	134
Installing IIS 7 Role Services on Windows Server 2008 or 2008 R2.....	134
Installing IIS 8 Role Services on Windows Server 2012 or 2012 R2.....	136

11 MACCRA Compatibility

Theory of Operation	139
Installation Requirements.....	140
Before You Begin	140
Customer Requirements	140
MACCRA Compatibility with CV Web v1.x and v2.x	140
Creating a MUSE User for MACCRA Compatibility.....	141
Installing MACCRA Compatibility	142
Verifying the MACCRA Compatibility Installation.....	146
System Checkout	146
Changing MACCRA Compatibility Configuration.....	148
MOCKRAConfigWriter.exe	148
MOCKRAServerProvisioner.exe.....	149
Uninstalling MACCRA Compatibility.....	150

12 CardioDay to MUSE System Interface

Theory of Operation	151
CardioDay to MUSE Holter Patient ADT/Order Interface	151
CardioDay Holter Report Export to the MUSE System	152
Determining MUSE eDoc Connect Parameters	153
CardioDay to MUSE Interface Prerequisites	153
Verifying the CardioDay Software Version	154
Verifying the MUSE System Software Version	154
Customer Requirements	155
Additional Resources	155
Configuring CardioDay and MUSE Interface Settings	155
Enabling the Holter Data Storage, eDoc Connect, and HIS Interface Option on the MUSE System.....	155
Enabling MUSE Holter Test Type for Each Site.....	156

Enabling MUSE ADT Orders and Holter Orders for Each Site	156
Creating the CardioDay Acquisition Profile on the MUSE System.....	157
Setting Up the CardioDay Share Folder in the MUSE System.....	157
Creating a Dedicated MUSE User Account for CardioDay Holter Orders Query	158
Configuring the CardioDay System for MUSE Holter Orders.....	159
Configuring the CardioDay System to Export Holter Reports to the MUSE System.....	159
Disabling the eDoc Connect Option.....	159
CardioDay / MUSE System Checkout	160
CardioDay Holter Report Export to MUSE Checkout	160
MUSE Order Option Checkout	160
Troubleshooting	160
Troubleshooting the CardioDay Holter Report Export to the MUSE System	160
Troubleshooting the CardioDay MUSE Order Option and eDoc Connect.....	161

13 MUSE Configuration for VA Vista Imaging

Theory of Operation	163
Information Transmission.....	164
Customer Requirements	164
Process Overview	164
Configuring the VOL000 Share	164
Configuring VA Vista Imaging Formats	165
Installing MUSEAPI3	167
Installing MACCRA Compatibility	167
System Checkout	168
Creating Enhanced Metafile Using MUSE API DCOM Tester	168
Viewing Enhanced Metafile Using MUSE Image Viewer	169

Introduction

Manual Purpose

This document provides information on installing and configuring:

- CASE to MUSE communication
- MARS to MUSE communication
- MUSE Monitoring Gateway
- MAC ECG systems to MUSE communication
- MUSE eDoc Connect
- MUSE XML Import option
- MUSE DICOM Communication
- MUSEAPI3 Installation
- MUSE Web Compatibility Layer
- MACCRA Compatibility
- CardioDay to MUSE System Interface
- MUSE Configuration for VA VistA Imaging

Related Documents

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

Part Number	Document Title
2020299-021	<i>MobileLink Installation Manual</i>
2020299-025	<i>LAN Option for MAC Installation and Troubleshooting</i>
2059568-009	<i>MUSE v9 Cardiology Information System Operator's Manual</i>
2059568-011	<i>MUSE v9 Cardiology Information System Installation and Upgrade Manual</i>
2059568-016	<i>MUSE v9 Cardiology Information System Regulatory and Safety Guide</i>
2059568-017	<i>MUSE v9 Cardiology Information System Service Manual</i>

Part Number	Document Title
2059568-018	<i>MUSE v9 Cardiology Information System Pre-Installation Guide</i>
2059568-023	<i>MUSE v9 Cardiology Information System DICOM Conformance Statement</i>
2059568-025	<i>MUSE v9 Cardiology Information System Transactional XML Developer's Manual</i>
2092513-001	<i>CardioDay V2.5 Pre-Installation Manual</i>
2092513-002	<i>CardioDay V2.5 Installation and Field Service Manual</i>
2107900-003	<i>CV Web v3.0 Installation Manual</i>
2107900-004	<i>MUSE Enterprise Integration Reference Manual</i>

CASE to MUSE Communication

This chapter describes how to configure CASE systems to communicate with MUSE v9 systems. In these instructions, the term **CASE** denotes either CASE, CardioSoft, or CS.

NOTE:

MUSE v9 systems support only Windows Server 2008 and newer operating systems. Windows Server 2008 and newer operating systems are not compatible with Windows NT based CASE systems.

Theory of Operation

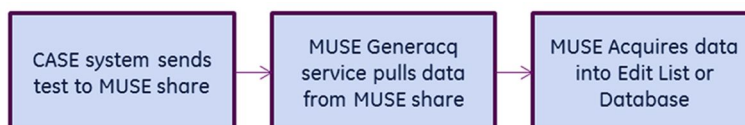
CASE system to MUSE system communication allows you to transfer ECGs and stress exercise tests from the CASE system to the MUSE system for viewing, editing, printing, and storage. CASE system to MUSE system communication also allows for the CASE system to retrieve patient information and orders via the MUSE Web Compatibility Layer.



Example Network Diagram

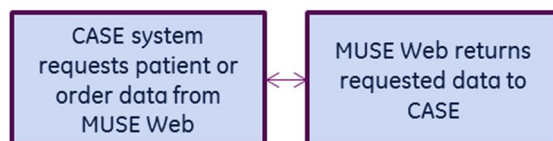
Information Transmission

In CASE system to MUSE system communication, the CASE system transfers tests to a shared folder on the MUSE application server. The **MUSE Generacq** service searches this shared folder for files and pulls them to the MUSE system for processing. Tests are then normalized on the MUSE system and stored in the database.



Transmission Flow Chart

The CASE system also makes requests for patient or order information. In these cases, the MUSE Web Compatibility Layer returns the patient or order information to the CASE system.



MUSE Web Request Flow Chart

Communication Levels

The CASE systems and MUSE systems support three communication levels. Each level builds on the features and requirements of the previous level, as shown in the following table:

Communication Levels

Communication Level		Data Exchanged	Directions		Transfer Method	Required Components
			From	To		
	Record Transfer	CASE Reports	CASE	MUSE	Shared folder	MUSE Exercise Testing Data Storage option
	MUSE Web Compatibility Layer	MUSE Reports Patient Data	MUSE	CASE	Network	MUSEAPI3 and MUSE Web Compatibility Layer
	HIS Orders	Order Data	MUSE	CASE	Network	HIS Orders Interface option

The HIS Orders level includes the features and requirements of the MUSE Web Compatibility Layer level, which in turn includes the features and requirements of the Record Transfer level.

Configuration Requirements

The requirements specified in this section must be satisfied before you begin configuring CASE system to MUSE system communication.

Customer Requirements

The customer is responsible for providing the appropriate network connectivity, including name resolution, between the CASE systems and the MUSE application server.

Communication Level Requirements

If you are using the MUSE Web communication level, you must install the MUSE Web Compatibility Layer before proceeding. For information on installing the MUSE Web Compatibility Layer, see [Chapter 10 “MUSE Web Compatibility Layer” on page 117](#).

If you are using the HIS Orders communication level, you must install and fully configure the HIS Orders Interface option before proceeding. The HIS Orders Interface is configured by a trained HL7 implementation person. Contact the HL7 implementation person to confirm whether the HIS Orders Interface is configured.

Considerations When Using Multiple CASE Systems

If you are using multiple CASE systems, review the items below for additional information.

- When using multiple CASE systems with a single MUSE application server, the same Windows CASE8000 user name and password may be used with every CASE system if desired.
- If you are adding a new CASE system to an existing MUSE system with CASE systems already configured to communicate with it, some of the steps in this chapter may have already been completed.

Process Overview

While the setup process differs depending on the communication level you are configuring, some tasks are performed for more than one level. The following table identifies all setup tasks in the order in which they are performed and which communication levels require them. Use the table to determine which tasks you need to perform to set up the required communication levels.

Setup Tasks

Record Transfer	MUSE Web	HIS Orders	Tasks
√			"Adding the Stress Exercise Option to the MUSE System" on page 22
√			"Creating the MUSE Acq Users Local Windows Group" on page 23
√	√	√	"Creating the CASE8000 Windows User" on page 24
√	√	√	"Creating the CASE8000 Windows Share" on page 24
	√	√	"Adding the User to the MUSE Web Users Group" on page 25
	√	√	"Creating a MUSE User" on page 25
√	√	√	"Configuring the CASE System Network Settings" on page 26
√	√	√	"Configuring MUSE System Settings on the CASE System" on page 27
√	√		"Configuring CASE Reports on the MUSE File Server" on page 31

In addition, at the beginning of each task, a table (similar to the following) indicates which communication levels require the completion of that task. If the communication

level you are setting up is checked, you need to perform the task. If the communication level you are setting up is not checked, skip the task.

Example of Tasks to be Completed

Record Transfer	√
MUSE Web	√
HIS Orders	√

Adding the Stress Exercise Option to the MUSE System

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Add Stress Exercise Option to the MUSE System

Record Transfer	√
MUSE Web	
HIS Orders	

Use the following procedure to add the stress exercise option to the MUSE system. This procedure may only be performed by a qualified GE Healthcare service representative.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full or partial shutdown of the MUSE system following the auto shutdown procedures described in the "System Administration" chapter of the *MUSE v9 Cardiology Information System Service Manual*.

NOTE:

If you are just checking to see if the option is already enabled, a shutdown is not required. If, however, you have to enable or disable the option, the MUSE services will be restarted and a shutdown is required.

3. Go to **Control Panel > Programs and Features**.
4. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
5. Choose **Modify** and click **Next**.
The **Select Feature** window opens.
6. Continue to click **Next** on each window until you reach the **Choose MUSE Options** window.
7. Verify that **Exercise Testing Data Storage** is checked.
If it is not, check it now.
8. Click **Next**.
The **MUSE Serial Number** window opens.

9. If you added the **Exercise Testing Data Storage** option in step 7, enter the **Options Configuration Password**.
NOTE:
 Only qualified GE Healthcare service representatives have access to this password. This password cannot be provided to customers.
10. Click **Next** until your changes are applied and the **Maintenance Complete** window opens.
11. Click **Finish**.
12. If you performed a full or partial shutdown of the MUSE system in step 2, cancel the shutdown following the procedures described in the "System Administration" chapter of the *MUSE v9 Cardiology Information System Service Manual*.

MUSE User and Shared Acquisition Folder

The MUSE v9 InstallShield may have been configured to complete the following actions when the MUSE system was first installed:

- Creating the **MUSE Acq Users** local Windows group
- Creating the **CASE8000** Windows user
- Creating the **CASE8000** Windows share

Refer to the *MUSE v9 Cardiology Information System Installation and Upgrade Manual* for details on the MUSE v9 InstallShield configuration.

If the MUSE v9 Installer was not configured to create the CASE configuration items, they must now be completed manually.

NOTE:

If the CASE configuration items were created when the MUSE system was initially installed, proceed to the next task for your selected communication level. The CASE configuration items do not need to be recreated.

Creating the MUSE Acq Users Local Windows Group

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Create MUSE Acq Users Local Windows Group

Record Transfer	√
MUSE Web	
HIS Orders	

To transfer MUSE reports from a CASE system to the MUSE system, you need to give CASE users access to the MUSE system. The first part of this access is the creation of the **MUSE Acq Users** local Windows group.

If one does not already exist, create a local group on the MUSE Application server named **MUSE Acq Users**.

Creating the CASE8000 Windows User

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Create CASE8000 Windows User

Record Transfer	√
MUSE Web	√
HIS Orders	√

To transfer MUSE reports from a CASE system to the MUSE system, in addition to giving CASE users access to the MUSE system, you also need to create a **CASE8000** Windows user.

1. If a **CASE8000** user does not already exist on the MUSE system, create a local user named **CASE8000** on the MUSE Application server and assign this user a password of **case!8000**.

It is recommended that the Windows user be configured with the following options or equivalent:

- **User cannot change password**
- **Password never expires**

NOTE:

You may use a different password if desired, however, the password specified on the CASE system must match the password used here.

2. If not already done, add the newly created **CASE8000** user to the local **MUSE Acq Users** group created on the MUSE Application server in the [“Creating the MUSE Acq Users Local Windows Group”](#) on page 23 section.

Creating the CASE8000 Windows Share

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Create CASE8000 Windows Share

Record Transfer	√
MUSE Web	√
HIS Orders	√

Lastly, to transfer MUSE reports from a CASE system to the MUSE system, you need to create a CASE8000 share.

By default, the **MUSE Generacq** service on the MUSE Application server is configured to check the **acq** folder (default is **d:\muse\acq**) for incoming files to process. In order to transfer records from a CASE system to the MUSE system, this location must be shared.

1. If it is not already shared, share the **acq** folder (default is **d:\muse\acq**) with a share name of **CASE8000**.
2. Provide **Change** and **Read Share Permissions** to the **MUSE Acq Users** group.
3. If the **Everyone** group is listed with share permissions, remove it.

Adding the User to the MUSE Web Users Group

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Add User to MUSE Web Users Group

Record Transfer	
MUSE Web	√
HIS Orders	√

To access MUSE reports through MUSE Web, you must add the **CASE8000** user to the **MUSE Web Users** group on the MUSE application server.

NOTE:

You must have the MUSE Web Compatibility Layer installed on the MUSE Application server before proceeding with this step. See [Chapter 10 "MUSE Web Compatibility Layer" on page 117](#) for instructions.

If not already done, add the previously created local **CASE8000** user to the local **MUSE Web Users** group on the MUSE Application server.

Creating a MUSE User

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Create MUSE User

Record Transfer	
MUSE Web	√
HIS Orders	√

To request data from the MUSE system via MUSE Web, you must set up a CASE user account in the MUSE application.

If one has not already been created, create a new user account in MUSE **User Setup** with the following values.

MUSE User Properties	Field	Value
General	Last Name	8000
General	First Name	CASE
General	Windows User Name	<servername_or_domain>\CASE8000 NOTE: Replace <servername_or_domain> with the actual name of the MUSE file server for local accounts or the domain for domain accounts.
General	Account is Enabled	Check the box.
General	Active Sites	Select the sites to which the user needs access. NOTE: The CASE user can only request data for the sites to which the user account is granted access. Therefore it is important that you select all the sites for which the CASE system may request data.
Advanced	User ID	Enter an available User ID for the MUSE system on which you are working.
Advanced	Role	View Only
Advanced	Job Titles	Uncheck any boxes.
Advanced	Display User in Personnel Lists	Uncheck the box.

If necessary, refer to the *MUSE v9 Cardiology Information System Operator Manual* for information on creating users in the MUSE system.

Configuring the CASE System Network Settings

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Configure CASE System Network Settings

Record Transfer	√
MUSE Web	√
HIS Orders	√

For the CASE systems and MUSE system to communicate, the CASE systems must conform to the networking settings in effect at the installation site. Contact the site's system administrator to obtain required information or to assist in configuring the system.

Ensure that networking is enabled on all CASE systems that need to communicate with the MUSE system. Additionally, confirm that Windows network settings on these CASE systems are appropriately configured to communicate with the MUSE application and the MUSE website via TCP/IP.

Configuring MUSE System Settings on the CASE System

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Configure MUSE Settings on the CASE System

Record Transfer	√
MUSE Web	√
HIS Orders	√

Before you can fully integrate CASE systems with the MUSE system, you must complete the MUSE configuration on the CASE systems.

NOTE:

Not all of the MUSE configuration must be completed for all installations. Refer to the following table to determine which sections to complete.

CASE System Configuration Window — MUSE tab	Section Completion Requirements
Setup for MUSE section	Required for MUSE Web and HIS Orders
Store procedure for MUSE section	Required for Record Transfer
Everything else	Required for Record Transfer

1. Start the CASE application.
2. Select **System Configuration**. Once the **System Configuration** window opens, select the **MUSE** tab.

System Configuration

General | Devices | Modem | **MUSE** | Option Code | Country Settings | DICOM

Setup for MUSE

☒ Request MUSE Data MUSE Site 1

MUSE Web Server MUSESYS0001

MUSE User Name case8000

MUSE Password *****

Port number 88 SSL Connection ☐ 443

Internet Browser C:\Program Files\Internet Explorer\iexplore.exe

☐ Use MUSE Enumeration Lists Synchronize Lists

Store procedure for MUSE

☐ No data transfer to MUSE

☐ Save MUSE data to medium Drive A:

☐ Data transfer to MUSE via the network

MUSE FTP Server

MUSE FTP User Name

MUSE FTP Password

MUSE FTP Proxy Server

☒ Data transfer to MUSE via Shared Directory

Shared Directory \\MUSESYS001\case8000

Directory User Name case8000

Directory Password *****

Location Number 5 Location Name List * 5 *

Cart/Device Number 5

MUSE Software Version 7.2 and above

Timeout in sec. 10 Sending data upon connection to MUSE...

☒ Limit Text Entry to MUSE Length

☐ Medication, Interpretation Text Blocks are "Select Only"

☐ Automatic transfer to MUSE

☐ Physicians and Technicians are "Select Only"

☐ Delete local test data after transfer to MUSE

☒ Tests are "View Only" after transfer to MUSE

☐ Start modem connection before transfer

Print Help OK Cancel

3. Complete the **Setup for MUSE** section by performing the tasks in the table following the screen capture.

System Configuration

General | Devices | Modem | **MUSE** | Option Code | Country Settings | DICOM

Setup for MUSE

☒ Request MUSE Data MUSE Site 1

MUSE Web Server MUSESYS0001

MUSE User Name case8000

MUSE Password *****

Port number 88 SSL Connection ☐ 443

Internet Browser C:\Program Files\Internet Explorer\iexplore.exe

☐ Use MUSE Enumeration Lists Synchronize Lists

Field	Task
Request MUSE Data	Check this box.
MUSE Web Server	Enter the name or IP address of the MUSE application server.

Field	Task
MUSE User Name	Enter the username of the user with access to MUSE Web. This is typically case8000 . NOTE: If the MUSE website is configured with a default domain, and a local case8000 user is being used, you may need to specify the MUSE User Name as <muse_server_name>\case8000 where <muse_server_name> is the computer name of the MUSE application server.
MUSE Password	Enter the password for the user defined previously. This is typically case!8000 .
Port number	Enter the port for the website on the MUSE system. This is typically 80 .
Port number and SSL Connection	If an SSL connection to the MUSE Web Server is used, enter the SSL Port number and check the SSL Connection box. The SSL port is typically 443 .
Internet Browser	Use the browse button to find the executable for Internet Explorer. Internet Explorer is typically located in the following path: C:\Program Files\Internet Explorer\explore.exe . Adjust the path accordingly for non-English operating systems.

4. Complete the **Store procedure for MUSE** section by performing the tasks in the table following the screen capture.

Store procedure for MUSE

☐ No data transfer to MUSE

☐ Save MUSE data to medium

Drive: A: [v]

☐ Data transfer to MUSE via the network

MUSE FTP Server: []

MUSE FTP User Name: []

MUSE FTP Password: []

MUSE FTP Proxy Server: []

☒ Data transfer to MUSE via Shared Directory

Shared Directory: \\MUSESYS001\case8000

Directory User Name: case8000

Directory Password: []

Field	Task
Data transfer to MUSE via Shared Directory	Select this radio button.
Shared Directory	Enter the UNC path of the shared folder on the MUSE application server. This is typically \\<muse_server_name>\case8000 where <muse_server_name> is the computer name of the MUSE application server.

Field	Task
Directory User Name	Enter the username of the user with access to the shared directory. This is typically case8000 .
MUSE Password	Enter the password for the user defined above. This is typically case!8000 .

5. Populate the **Location Number**, **Cart/Device Number**, and **MUSE Software Version** fields as specified in the table following the screen capture.

Location Number
5 * 5 * Location Name List

Cart/Device Number
5

MUSE Software Version
7.2 and above

Timeout in sec.
10 Sending data upon connection to MUSE...

Field	Task
Location Number	Enter or select the desired MUSE location for the CASE system. This location should match the appropriate location defined in the MUSE system.
Cart/Device Number	Choose a unique device number for this CASE system (and all future CASE systems), to ensure that all records sent to the MUSE system have unique file names.
MUSE Software Version	Select 7.2 and above from the drop-down list.

6. Click **OK**.

NOTE:

For information regarding all other options on the **MUSE** tab of the **System Configuration** window, please refer to the appropriate CASE system documentation.

Configuring CASE Reports on the MUSE File Server

Complete this task only if the following table has a check mark next to the communication level you are setting up. If the communication level you are setting up is not checked, skip this task.

Configure Case Reports

Record Transfer	√
MUSE Web	√
HIS Orders	

In order for the MUSE system to correctly format CASE reports sent to the MUSE share, the MUSE system must use the same report templates. CASE report templates are created on the CASE systems and then copied to the MUSE system.

Refer to your CASE system documentation for instructions on creating the report templates.

1. After creating the templates on the CASE system, copy the **NARRATIV** folder from the CASE system to removable media or a network share.
The default location is **C:\CASE\NARRATIV** or **C:\CARDIO\NARRATIV**.
2. Log on to the MUSE Application server as the MUSE Administrator user.
3. On the MUSE system, copy the **NARRATIV** folder from the removable media or network share to a temporary location on the MUSE application server such as **C:\CASE1\NARRATIV**.

NOTE:

If you are copying report templates from multiple CASE systems, create a separate temporary location for each system, such as **C:\CASE1\NARRATIV**, **C:\CASE2\NARRATIV**, and so on.

4. On the MUSE system, open a Command Prompt.
5. Change to the location of the MUSE application files (default is **C:\Program Files (x86)\MUSE**).
6. Type the following command:

```
loadtemplate -path:"<path to narrativ folder>" -test:4 -lang:<language> -db:<dbname>
```

Where <path to narrativ folder>, <language>, and <dbname> are appropriately populated. Use the following tables to determine the values of these items.

Example command line for an English language CASE system with a local MUSE database:

loadtemplate -path:"C:\CASE1\NARRATIV" -test:4

NOTE:

Notice that in this example neither the language nor the database name was specified. Because the default language is English and the database is local with a default prefix of MUSE, it was not necessary to specify either of these in the command.

Example command line for a Spanish language CASE system, a remote MUSE database named **SQLSERVER1**, and a default prefix of MUSE:

***loadtemplate -path:"C:\CASE1\NARRATIV" -test:4 -lang:es
-db:SQLSERVER1\MUSE***

Example command line for a Swedish language CASE system, a remote MUSE database, an instance name of **SQLSERVER1\MUSE**, and a default prefix of MUSE:

loadtemplate -path:"C:\CASE1\NARRATIV" -test:4 -lang:sv -db:SQLSERVER1\MUSE.MUSE

Command Options

Command Option	Description
-path	Required. The path to the CASE report templates. For example: C:\CASE1\NARRATIV .
-lang	Optional. The report language. If you do not include this switch, the language defaults to en (English). The language you enter should match the language of the CASE system. See the following table for other language codes.
-db	Optional. Database Name and prefix (for example Server\Instance.Prefix). The default is \.MUSE .

Language Codes

Code	Language
da	Danish
de	German
en	English
es	Spanish
fi	Finnish
fr	French
it	Italian

Language Codes (cont'd.)

Code	Language
ja	Japanese
nl	Dutch
no	Norwegian
ru	Russian
sv	Swedish
zh-chs	Simplified Chinese
zh-cht	Traditional Chinese

7. Press **Enter**.
The templates are loaded into the MUSE database.
8. Repeat this procedure to load templates from each CASE system as desired.
NOTE:
If more than one CASE system has the same **Report Template** name, the last **Report Template** with that name loaded into the MUSE database will be the **Report Template** used in the MUSE database. Use unique **Report Template** names at the CASE systems to avoid overwriting report templates already loaded into the MUSE database.
9. Verify the report templates are loaded into the MUSE database.
 - a. Open a stress exercise test in the MUSE Editor.
 - b. Go to the **Clerical** tab and click the down arrow in the **Report Template** drop-down list.
 - c. Verify the report templates loaded from the CASE systems are listed there.

System Checkout

After setting up the MUSE system and all connected CASE systems, complete the following verification procedures to ensure the CASE system to MUSE system communication is set up properly.

Verifying Record Transfer

Use the following procedure to verify that the CASE systems transfer reports to the MUSE share and that the MUSE system imports the CASE reports.

1. From the initial window of the CASE application, click **Local Database**.
2. Highlight a patient name and click **Select**.
The **Select Test** window opens.
3. Select a test record and click **Transfer to MUSE**.
4. Click **Save**.

5. Log on to the MUSE system.
6. Verify the test record is displayed in the MUSE system **Edit List**.

Verifying Requests for Data

Use the following procedure to verify that the Web connection between the CASE system and the MUSE system functions properly and successfully supports data requests.

1. From the initial window of the CASE application, click **MUSE Browser**.
The CASE system launches the **Microsoft Internet Explorer** and connects to the MUSE home page. If you are using the default configuration, you are prompted to enter a user name and password.
2. Enter the user name and password.
NOTE:
If you change the default password for the **case8000** account on the CASE system, you must also change it on the MUSE system.
3. Submit a request query and view the results to verify that the Web connection functions properly.

Verifying the Retrieval of Patient Demographics

Use the following procedure to verify that the CASE system is able to view the patient list from the MUSE system database.

1. From the initial window of the CASE application, click **New Test**.
A list of available patients is displayed.
2. Verify that the patient list is from the MUSE system database and not the local CASE system database.

Verifying the Retrieval of Orders

Use the following procedure to verify that the CASE system is able to view the open orders that exist on the MUSE system.

1. From the initial window of the CASE application, click **New Test**.
2. From the **New Test** screen, click **Order List**.
3. Verify that open orders on the MUSE system are displayed.

Troubleshooting

Use the following troubleshooting tips to help resolve issues you may encounter with CASE system to MUSE system communication.

Troubleshooting Tips

Symptom	Possible Cause	Recommendations
Unable to view patients or orders on the MUSE system from the CASE system.	The MUSE User Name and/or MUSE Password specified in the Setup for MUSE on the CASE system is incorrect.	Ensure the MUSE User Name and/or MUSE Password are entered correctly in the CASE System Configuration .
	The MUSEAPI3 service is stopped on the MUSE application server.	Ensure the MUSEAPI3 service is started on the MUSE application server.
	The MUSE system is in an AutoShutdown state.	Cancel the AutoShutdown .
Unable to transfer tests from a CASE system to the MUSE system.	The Exercise Testing Data Storage option is not enabled on the MUSE system.	Enable the Exercise Testing Data Storage option on the MUSE system.
	The Directory User Name and/or Directory Password defined in the Store procedure for MUSE on the CASE system is incorrect.	Ensure the Directory User Name and/or Directory Password are entered correctly in the CASE System Configuration .
	The Shared Directory defined in the Store procedure for MUSE on the CASE system is incorrect.	Ensure the Shared Directory is entered correctly in the CASE System Configuration .
	The Directory User Name defined in the Store procedure for MUSE on the CASE system does not have access to the MUSE share.	Ensure the Directory User Name defined on the CASE system is a member of the MUSE Acq Users group on the MUSE application server.
	The share on the MUSE application server is not defined correctly.	Ensure the acq folder (default is d:\muse\acq) is correctly shared on the MUSE application server.

3

MARS to MUSE Communication

This chapter describes how to configure MARS systems and MUSE systems in order to send Holter reports from the MARS system to the MUSE v9 system.

Theory of Operation

MARS system to MUSE system communication allows you to transfer stored MARS reports from the MARS system to the MUSE system for viewing, editing, printing, and storage. The MARS system transfers the complete Holter report. At the MUSE system, you can view the strip pages and edit patient demographics, diagnosis statements, and findings.

NOTE:

MARS stored reports do not contain full disclosure information.



Example Network Diagram

MUSE Services

MARS system to MUSE system communication uses the following two MUSE services:

MUSE Generacq and MUSE Format Services

Service	Description
MUSE Generacq Service	The MUSE Generacq Service handles acquisitions from other systems or devices. In MARS system to MUSE system communication, it searches the reports share on the MARS system for stored reports (files with the *.mrs file extension) and pulls the reports to the MUSE system for processing.
MUSE Format Service(s)	The MUSE Format service(s) launch the MARS Formatter program. The MARS Formatter program formats the output to match the format from the MARS system.

Information Transmission

In MARS system to MUSE system communication, a Holter test is stored in the reports folder on the MARS system with a **.mrs** extension. The **MUSE Generacq** service searches that folder for ***.mrs** files.

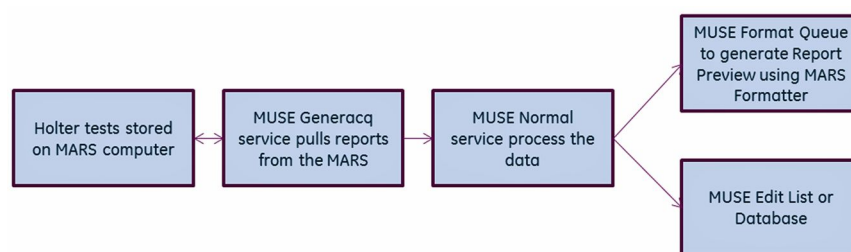
Tests are then normalized on the MUSE system and stored in the database.

Tests are also processed through the MARS Formatter during acquisition to generate a PDF that can be viewed in the MUSE Editor.

NOTE:

While tests are being processed by the MARS Formatter during acquisition, you cannot view or edit them in the test editor. The following message is displayed while the Holter report is being formatted after normalization:

The Holter record acquired for patient is currently checked out by Admin.



Acquisition Flow Chart

Customer Requirements

The customer is responsible for supplying appropriate network connectivity, including name resolution, between the MARS systems and the MUSE application server.

Configuring MARS to MUSE Communication

Adding MARS system to MUSE system communication requires changes to both the MARS workstation and the MUSE application server and includes:

- [“Configuring the MARS System Network Settings” on page 39](#)
- [“Verifying the MARS Software Version” on page 39](#)
- [“Recording the IP Address or Host Name of the MARS System” on page 39](#)
- [“Verifying the MARS Reports Share” on page 39](#)
- [“Activating the MARS to MUSE Option on the MARS System\(s\)” on page 40](#)
- [“Setting Up the Site Information on the MARS System\(s\)” on page 40](#)
- [“Adding the Holter Data Storage Option to the MUSE System” on page 41](#)
- [“Adding the MARS System to the MUSE Generacq Configuration” on page 42](#)
- [“Installing the MARS Print Formatter” on page 43](#)
- [“Creating site.ini for the MARS Print Formatter” on page 45](#)

- “Copying the rusty.ini Configuration File from the MARS System to the MUSE System” on page 46
- “System Checkout” on page 46

Configuring the MARS System Network Settings

For the MARS and MUSE systems to communicate, the MARS system must conform to the network settings in effect at the installation site. Contact the site’s system administrator to obtain required information or to assist in configuring the system.

Ensure that networking is enabled on all MARS systems that need to communicate with the MUSE system. Additionally, confirm that Windows network settings on the MARS systems are appropriately configured to communicate with the MUSE application server.

Verifying the MARS Software Version

To determine your MARS software version:

1. From the MARS system menu bar, select **Help > About**.
The **About** window opens.
2. Record the software version listed on the **About** window.
3. Find your version in the following table to determine your next step.

If the current MARS software version is...	Then...
5.x or 6.x	Upgrade to version 7.0 or later.
7.0 or later	Continue the MARS to MUSE communication configuration. Go to “Recording the IP Address or Host Name of the MARS System” on page 39.

Recording the IP Address or Host Name of the MARS System

Record the computer name or IP address of each MARS system you wish to configure for communication with the MUSE system.

If you want to use the IP address, it must be static.

Verifying the MARS Reports Share

Ensure that the MARS reports folder (default is **c:\gemsit\reports**) is shared and has a share name of **Reports**. You must establish and give file and share permissions of **Full Control** to the user account that is configured to start the **MUSE Generacq** service on the MUSE application server.

Activating the MARS to MUSE Option on the MARS System(s)

Use the following procedure to activate the **MARS to MUSE** option on the MARS system.

1. Locate the MARS software activator sheet.
2. From the MARS application menu bar, select **System > System Setup > Software Activators**.
A list of task names opens along with their corresponding modes and statuses.
3. If the **MARS to MUSE** task name is disabled, click **MARS to MUSE**.
A list of available modes is displayed in the **Change Mode To** list box.
4. Click **Activate**.
5. Type the access code from the activator sheet into the **Enter Activator Code Here** text box.
6. Click **Save Changes**.
If the code is incorrect or incomplete, an error message is displayed.
7. Select **OK**.
8. Click **Quit** to close the window.
9. Repeat steps 2 through 8 on all systems requiring MARS system to MUSE system communication.

Setting Up the Site Information on the MARS System(s)

Site setup is necessary to transfer Holter data to a MUSE system. The sites and locations entered in each MARS system must match the sites and locations used on the MUSE system.

NOTE:

Contact the MUSE system owner for the site and location information you need to use for the MARS system.

Repeat the following steps for each MARS system that is communicating with the MUSE system.

1. From the MARS main window, select **System > System Setup > Site**.
The **System: Site and Locations Setup** window opens.
2. Select the appropriate **Site #**.
3. Enter the corresponding **Site Name**.
4. Select the appropriate **Location #**.
5. Enter the corresponding **Location Name**.
6. Click **Add**.
7. Repeat steps 2 through 6 as necessary.
8. Click **OK**.
9. At the **Changes made. Save them?** prompt, click **Yes** to save your changes.

Adding the Holter Data Storage Option to the MUSE System

Use the following procedure to add the **Holter Data Storage** option to the MUSE system.

NOTE:

This procedure may only be performed by a qualified GE Healthcare service representative.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full or partial shutdown of the MUSE system following the auto shutdown procedures described in the “System Administration” chapter of the *MUSE v9 Cardiology Information System Service Manual*.

NOTE:

If you are just checking to see if the option is already enabled, a shutdown is not required. If, however, you have to enable or disable the option, the MUSE services will be restarted and a shutdown is required.

3. In the Windows **Control Panel**, select **Programs and Features**.
4. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
5. Choose **Modify** and click **Next**.
The **Select Feature** window opens.
6. Continue to click **Next** on each window until you reach the **Choose MUSE Options** window.
7. Verify that **Holter Data Storage** is checked.
If it is not, check it now.
8. Click **Next**.
The **MUSE Serial Number** window opens.
9. If you added the **Holter Data Storage** option in step 7, you need to enter the **Options Configuration Password**.

NOTE:

Only qualified GE Healthcare service representatives have access to this password. This password cannot be provided to customers.

10. Click **Next** until your changes are applied and the **Maintenance Complete** window opens.
11. Click **Finish**.
12. If you performed a full or partial shutdown of the MUSE system in step 2, cancel the shutdown following the procedures described in the “System Administration” chapter of the *MUSE v9 Cardiology Information System Service Manual*.

Adding the MARS System to the MUSE Generacq Configuration

To ensure the MUSE system can locate and communicate with the MARS system(s), use the following procedures to add, modify, or remove paths to the MARS system(s) as needed.

Adding the Path of Each MARS System to the MUSE Database

Complete the following procedure to add the path of each MARS system to the MUSE database.

1. From within the MUSE application, go to **Setup**.
2. Select **Share Folder**.

The list of existing **Share Folders** is displayed.

The **Share Folder** option within MUSE is where **MUSE Generacq** folders and file name filters are configured.

3. Select **Action > New**.

The **Share Folder Properties** dialog opens.

4. Complete the fields as described in the following table:

Field	Task
Entry	Enter the UNC path of the MARS reports share on the MARS system, for example \\MARS001\reports .
File Name Filter	Enter *.MRS .
Profile Name	Select None .

5. Click **OK**.

Modifying an Existing Share Folder Entry

The following procedure can be used to modify an existing **Share Folder** entry.

1. From within the MUSE application, go to **Setup**.
2. Select **Share Folder**.

The list of existing share folders is displayed.

3. Right-click on the **Share Folder** you want to modify and choose **Properties**.

The **Share Folder Properties** window opens.

4. Complete the fields as described in the following table:

Field	Value
Entry	Enter the UNC path of the MARS reports share on the MARS system, for example \\MARS001\reports .
File Name Filter	Enter *.MRS .
Profile Name	Select None .

5. Click **OK**.

Removing an Existing Share Folder Entry

The following procedure can be used to delete an existing **Share Folder** entry if necessary.

1. From within the MUSE application, go to **Setup**.
2. Select **Share Folder**.
The list of existing Share Folders is displayed.
3. Right-click on the Share Folder you want to remove and choose **Delete**.

Installing the MARS Print Formatter

The MARS Print Formatter allows Holter reports that are viewed and printed from the MUSE system to look the same as when they are printed from the MARS system. Starting with the MUSE v9 system, the MARS Print Formatter is automatically installed when the MUSE application is installed on the MUSE application server.

The version of the MARS Print Formatter installed with the MUSE v9 system is MARS v8.0 SP4. The print formatter is backward compatible with previous versions of MARS, however it may not be forward compatible. If the MARS Print Formatter version is later than v8.0 SP4, you may need to install it to ensure compatibility with MARS Holter reports from MARS versions newer than MARS v8.0 SP4.

The following steps describe how to install and uninstall the print formatter software.

NOTE:

Do not perform these steps unless you are installing a version of the MARS Print Formatter that is later than MARS v8.0 SP4.

Uninstalling an Older MARS Print Formatter

1. Log on to the MUSE application server as an administrator.
2. Go to Windows **Control Panel>Programs and Features**.
3. Select **MUSE-MARS** and choose **Uninstall**.
The MARS InstallShield Wizard is displayed and prompts you to confirm the uninstall.
4. Click **OK**.
5. At the **InstallShield Wizard Complete** screen, click **Finish**.
6. Confirm that the **<drive>:\gemsit** folder no longer exists, where <drive> is the letter of the drive on which the MARS Print Formatter software was previously installed.
If the **<drive>:\gemsit** folder still exists, rename or delete it.

Installing a Newer MARS Print Formatter

1. Log on to the MUSE application server as an administrator.
2. Ensure all antivirus software is turned off during the installation; it can be turned on again after the installation is completed.

3. Insert or mount the MARS Print Formatter installation media into the optical drive.
The **InstallShield Wizard** window may open. If necessary, browse to the optical drive and run **setup.exe**.
If a **User Account Control** prompt appears, choose **Yes** or **Allow**.
4. Choose your desired installer language and click **Next**.
NOTE:
The installer language selection only sets the language of the InstallShield Wizard.
5. At the **Welcome to the InstallShield Wizard for MUSE-MARS** screen, click **Next**.
6. At the **License Agreement** screen, click **Yes**.
7. At the **Destination Disk** screen, ensure the **C:** drive is selected and click **Next**.
8. At the **Ready to Install the Program** screen, click **Install**.
9. At the **InstallShield Wizard Complete** screen, click **Finish**.

Reinstalling the MARS Print Formatter Software that Comes with the MUSE v9 System

If for some reason you need to reinstall the MARS Formatter software that comes with the MUSE v9 system, complete the following procedure.

1. Perform the steps in [“Uninstalling an Older MARS Print Formatter” on page 43](#) to remove the existing MARS Print Formatter software.
2. Ensure all antivirus software is turned off during the installation; it can be turned on again after the installation is completed.
3. Insert or mount the MUSE v9 installation media into the optical drive.
If the MUSE v9 installation options window opens, close it.
4. Browse to the **\MUSESetup\MARS-MUSE_Formatter** folder on the MUSE v9 installation media.
5. Run **setup.exe**.
If a **User Account Control** prompt appears, choose **Yes** or **Allow**.
The InstallShield Wizard opens.
6. Choose your desired installer language and click **Next**.
NOTE:
The installer language selection only sets the language of the InstallShield Wizard.
7. At the **Welcome to the InstallShield Wizard for MUSE-MARS** screen, click **Next**.
8. At the **License Agreement** screen, click **Yes**.
9. At the **Destination Disk** screen, ensure the **C** drive is selected and click **Next**.
10. At the **Ready to Install the Program** screen, click **Install**.
11. At the **InstallShield Wizard Complete** screen, click **Finish**.

Creating site.ini for the MARS Print Formatter

Use the following instructions to create the **site.ini** file on the MUSE Application server. The **site.ini** file is used by the MARS Print Formatter for outputting the MUSE site and location name on MARS formatted reports. If these steps are not performed, the MARS formatted reports viewed and printed from the MUSE system will show **Unknown** for site names and locations.

NOTE:

This process will need to be repeated each time a MUSE site or location that is used by a MARS formatted Holter report is added to MUSE system.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Insert the MUSE v9 installation media into the optical drive of the system.
If any **Autorun** or **AutoPlay** screens appear, close or cancel them.
3. Browse the optical drive in Windows Explorer and perform one of the following:
 - If the MUSE v9 Application and Support DVD is inserted, navigate to the **\MUSE Support\MARS Site INI Update** folder.
 - If the MUSE v9 Support ISO is being used, navigate to the **\MARS Site INI Update** folder.
4. Copy **SiteIniUpdate.exe** from the MUSE v9 support media to the location where the MUSE application is installed. The default location of the MUSE application is: **C:\Program Files (x86)\MUSE**.
5. Run **Siteiniupdate.exe** from the MUSE installation folder using **Run as Administrator**.
When **Siteiniupdate.exe** runs, a command prompt window will open and close. There will be no on-screen messages if it completes successfully.
6. Verify the **C:\gemsit\var\MarsNT\system\site.ini** is created or updated.
The contents of the file will reflect the MUSE site and location configuration of the MUSE system. See the following **site.ini** file basics.

site.ini File Basics

The **site.ini** file is made up of at least three sections.

- The **[Site List]** section lists all of the site numbers.
- Each site will have a **[Site]** section that lists the location numbers and the site name. If there are multiple sites, there will be multiple **[Site]** sections.
- Each site and location combination will have its own **[Site Location]** section containing the location name. If there are multiple locations for each site, there will be multiple **[Site Location]** sections.

Following is an example of a **site.ini** file:

```
[Site List]
Site Numbers= 1 2
[Site 1]
Location Numbers= 1 2
Site Name= "Memorial Hospital"
[Site 1 Location 1]
```

Location Name= "Holter Scanning"
[Site 1 Location 2]
Location Name= "ECG Department"
[Site 2]
Location Numbers= 1 2
Site Name= "General Hospital"
[Site 2 Location 1]
Location Name= "Mary's Office"
[Site 2 Location 2]
Location Name= "John's Office"

Copying the rusty.ini Configuration File from the MARS System to the MUSE System

To maintain proper MARS Holter report formatting on the MUSE v9 system, you must copy the **Rusty.ini** configuration file from the primary MARS Server (or standalone workstation) to the MUSE system.

This file is located in the following default installation folder on the MARS system:

C:\gemsit\var\MarsNT\system

NOTE:

Repeat this step if changes are made to the MARS system configuration.

System Checkout

To ensure that the MARS system to MUSE system communication is functioning properly, you need to save a report on each MARS workstation, send those reports to the MUSE application server, and then retrieve and print those reports on the MUSE application server.

Saving a Report on the MARS System

Complete the following steps to save a report on the MARS system. These steps are performed on the MARS system.

1. Click the **Patient Select** icon.
2. In the **Patient Select** window, select **Holter** from the **Data Type** list.
3. Select a patient in the list.
4. Click the **Patient Information** icon.
5. Verify that the **Site** and **Location** information is filled in for this patient.
6. Click the **Report Review** icon.
7. Click **Save Report**.

The following message is displayed: **Report successfully stored.**

8. Click **OK**.
9. Click **Close**.

The **Report Review** tool closes.

Sending a MARS Holter Report to the MUSE System

Complete the following steps to send a MARS report to the MUSE system. These steps are performed on the MARS system.

1. Click the **Patient Select** icon.
2. In the **Patient Select** window, select **Stored Reports** from the **Data Type** list.
3. Select the stored report you saved using the steps in [“Saving a Report on the MARS System” on page 46](#).
4. Click **Tools**.
5. Click **Store to MUSE**.

The following message is displayed: **You have selected 1 file(s) for MUSE storage. Are you sure you want to store the selected file(s) to MUSE?**

6. Click **Yes**.

The following message is displayed: **1 report(s) queued for storage to MUSE.**

7. Click **OK**.
8. After a brief delay, verify that the report is listed as **Stored to MUSE**.

NOTE:

If the **Delete Reports After Transfer to MUSE** option is enabled on the MARS system, the patient report will automatically be removed from the **Stored Reports** list.

9. Click **Close**.

Viewing a MARS Holter Report in the MUSE Editor

With the MUSE v9 system there is a **Report Preview** tab available within the MUSE Editor. This **Report Preview** displays the Holter Report as it would look if printed from the MARS system.

1. Open the Holter report stored to the MUSE system using the steps in [“Sending a MARS Holter Report to the MUSE System” on page 47](#).
2. Verify the **Report Preview** tab displays the MARS Holter report.

NOTE:

Be aware of the following when viewing Holter reports on the MUSE system:

- Created reports are not displayed in the **Report Preview** tab until the associated electronic document data is manually imported.
- Holter reports acquired by earlier versions of the MUSE system cannot be previewed until they have been opened in the MUSE Editor at least once. The following message displays the first time you open a Holter report in the MUSE system that does not have a **Report Preview**: **The Full Report is currently not present for this test, but will be available the next time the study is opened in the editor.**

Printing MARS Holter Reports from the MUSE System

1. Select the **Holter** report from the **MUSE Edit** List.
2. On the tool bar, click **Print Test**.
3. From the **Available Printers** list, select a **Laser** printer or **PDF Folder** device.
4. Click **OK**.
5. Verify that the report was generated, then confirm that it is formatted properly based on the configuration:
 - If the MARS Format Holter specific format setting is enabled, the report should look like a MARS report.
 - If the MARS Format Holter specific format setting is not enabled, the report should look like a MUSE report.

Troubleshooting

Use the following troubleshooting tips to help resolve issues you may encounter with MARS system to MUSE system communication.

Troubleshooting Tips

Symptom	Possible Cause	Recommendations
Unable to store tests from the MARS system to the MUSE system.	The Holter Data Storage option is not enabled on the MUSE system.	Enable the Holter Data Storage option on the MUSE system.
	The MARS to MUSE option is not activated on the MARS system.	Activate the MARS to MUSE option on the MARS system. The MARS to MUSE option must be activated on each MARS system that needs to store data to the MUSE system.
	The user account configured to start the MUSE Generacq service on the MUSE application server does not have access to the reports share on the MARS system.	Ensure the user account configured to start the MUSE Generacq service on the MUSE application server has access to the reports share on the MARS system.
	The reports share on the MARS system is not defined correctly.	Ensure the reports share on the MARS system is set up correctly.
	The Share Folder is not set up correctly for the MARS system in the MUSE System Setup .	Ensure the Share Folder setup in MUSE System Setup is correctly defined.
The Site and/or Location on MARS reports display as Unknown when viewed on the MUSE system.	The site.ini has not been correctly configured on the MUSE system for the MARS Print Formatter.	Ensure the site.ini exists and is correctly defined on the MUSE system.

Troubleshooting Tips (cont'd.)

Symptom	Possible Cause	Recommendations
The following message appears when attempting to view a recently acquired Holter report in the MUSE application: <i>The Holter record acquired for patient is currently checked out by Admin.</i>	The Holter report is being processed by the MARS Print Formatter.	Wait for the test to be processed by the MUSE system and MARS Print Formatter and then open the test in the MUSE application.
The following message appears when attempting to view a Holter report that was acquired before the MUSE system was upgraded to v9: <i>The Full Report is currently not present for this test, but will be available the next time the study is opened in the editor.</i>	The Holter report has not been processed by the MARS Print Formatter yet.	Wait for the test to be processed by the MARS Print Formatter and then open it again in the MUSE application.

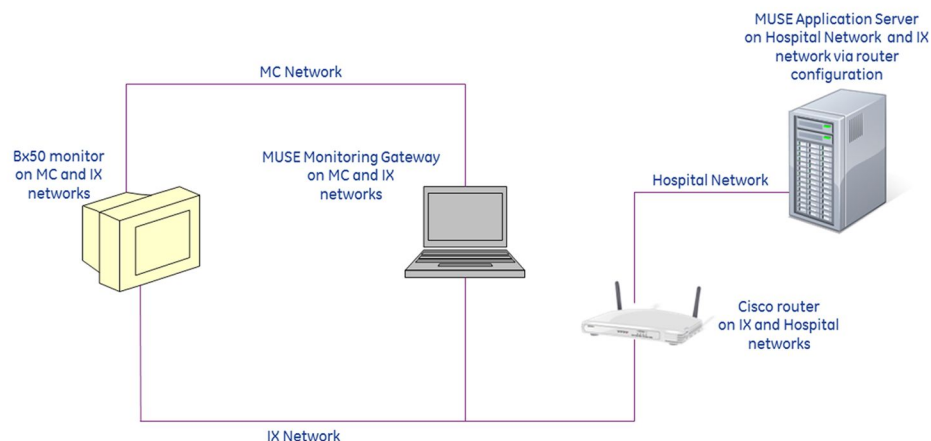
MUSE Monitoring Gateway

This chapter describes how to Install the MUSE Monitoring Gateway to allow bedside monitors to transmit ECG tests to the MUSE v9 system.

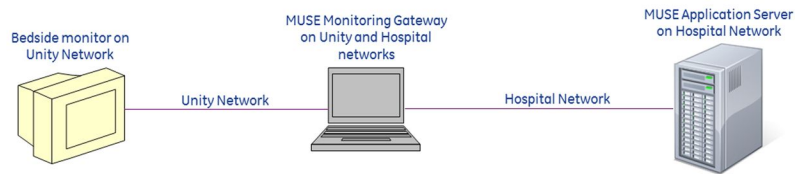
Theory of Operation

The MUSE Monitoring Gateway computer allows bedside monitors on a real-time monitoring network to transmit ECGs to the MUSE system. This is facilitated by the MUSE Monitoring Gateway having two Network Interface Cards (NICs), each on a different network. In many cases there is also a GE Healthcare configured router which will allow some bedside monitors to retrieve ECGs back from MUSE system.

When an ECG is transmitted from the bedside monitor, the test is received by the MUSE Monitoring Gateway. The MUSE application then retrieves the test from the MUSE Monitoring Gateway and acquires it into the MUSE database.



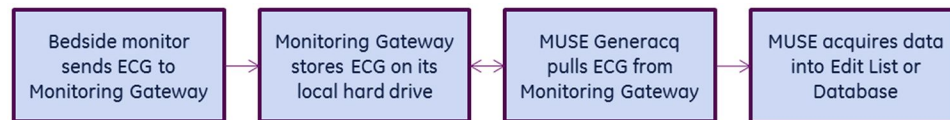
Example Network Diagram — MUSE Monitoring Gateway on the Mission Control and Information Exchange Networks



Example Network Diagram — MUSE Monitoring Gateway on the Unity and Hospital Networks

Information Transmission

In MUSE Monitoring Gateway to MUSE system communication, an ECG is transmitted from the bedside monitor to the MUSE Monitoring Gateway. The **MUSE Generacq** service searches the ACQMON share on the MUSE Monitoring Gateway for files and pulls them to the MUSE system for processing. Tests are then normalized on the MUSE system and stored in the database.



Acquisition Flow Chart

Installing the MUSE Monitoring Gateway

Follow the instructions in this chapter to complete the installation of the MUSE Monitoring Gateway. This chapter covers:

- “Preparing for the Installation of the MUSE Monitoring Gateway” on page 53
- “Verifying and Configuring Network Connections” on page 53
- “Firewall Considerations” on page 54
- “Creating a Share on the MUSE Monitoring Gateway” on page 54
- “Installing the MUSE Monitoring Gateway Software” on page 55
- “Configuring the MUSE Monitoring Gateway Software” on page 55
- “Configuring the MUSE Application Server” on page 56
- “Configuring Bedside Monitors” on page 57
- “System Checkout” on page 57
- “Troubleshooting” on page 58
- “Uninstalling MUSE Monitoring Gateway v1.1” on page 59

NOTE:

The MUSE Monitoring Gateway software version (v1.1) has not changed between the MUSE v8 and MUSE v9 releases. Therefore, this procedure should not need to be performed for MUSE v8 to MUSE v9 system upgrades, if the Monitoring Gateway existed prior to the upgrade.

Preparing for the Installation of the MUSE Monitoring Gateway

In order to ensure a successful installation, the person installing a new MUSE Monitoring Gateway system must be aware of the following items prior to beginning the installation.

Item	Action
Is the monitoring network configured by GE Healthcare or the customer?	Work with the Project Manager and/or the customer to determine this.
Router configuration, IP Addresses of the NICs, NAT Address of the NIC, and physical network connections	<p>If it is a GE Healthcare configured network, the GE Healthcare ND&I (Network Design and Implementation) team configures everything. The GE Healthcare ND&I engineer performing the configuration provides information to the FE (Field Engineer) installer and to the Project Manager (if applicable).</p> <p>If it is a customer configured network, the FE installer must work with the customer to determine appropriate configuration information.</p>

Ensure you meet the following requirements before continuing with the installation:

System	Requirements
Monitoring Gateway	<ul style="list-style-type: none"> Windows 7 Professional, Enterprise, or Ultimate <p>NOTE: Only 32-bit English-language versions of Windows 7 are supported.</p> <ul style="list-style-type: none"> C: drive partition Two network interface cards (NICs) No previous MUSE client installations (that is, the system should have no leftover traces of a previous MUSE installation, such as MUSE specific entries in the <i>win.ini</i> file)
MUSE Application Server	A user starting the MUSE Generacq service on the MUSE Application is able to connect to shares on the Monitoring Gateway.

Verifying and Configuring Network Connections

Configure and verify that the Monitoring Gateway has two Network Interface Cards (NICs) with the following network connections:

Typical New Installations on GE Healthcare-supplied Monitoring Networks

Network	IP Address	Subnet Mask
GE Healthcare Monitoring MC (Mission Critical) Network	172.16.0.1	255.255.0.0
GE Healthcare IX (Information Exchange) Network	Appropriate IP address and appropriate subnet mask	

Legacy or Customer-installed Monitoring Networks

Network	IP Address	Subnet Mask
Unity Network	126.8.8.1	255.0.0.0
LAN on which the MUSE application server resides	Appropriate IP address and appropriate subnet mask	

NOTE:

The network settings listed in the previous tables are defaults. The IP address and subnet mask may be different for customer configured networks.

After configuring the NICs it is a good practice to rename the Local Network Connections in Windows to match the networks to which they are connected.

Firewall Considerations

If the MUSE Monitoring Gateway has a firewall in place, you must make the following exceptions:

- TFTP (UDP port 69): allows communication from the Bedside Monitors to the MUSE Monitoring Gateway.
- Windows File Sharing: allows the MUSE system to access the folder share on the MUSE Monitoring Gateway.

Creating a Share on the MUSE Monitoring Gateway

Use the following procedure to set up a folder on the Monitoring Gateway that the MUSE application server can access.

1. On the MUSE application server, determine what user account is running the **MUSE Generacq** service.
Typically, this is the MUSE Background account. However, for security reasons the customer may be using a different account.
2. Create a **C:\ACQMON** folder on the Monitoring Gateway system.
3. Share the folder created in step 2, giving the account determined in step 1, full permissions to the share.
If a local account is being used to start the **MUSE Generacq** service, create an identical user account locally on the Monitoring Gateway, using the same password.

The key requirement here is that the account configured to start the **MUSE Generacq** service on the MUSE application server must have full access to the **ACQMON** share on the MUSE Monitoring Gateway.

NOTE:

Do not change the account used to start the **MUSE Generacq** service on the MUSE application server. Changing this account could impact other **MUSE Generacq Share Folder** configurations.

Installing the MUSE Monitoring Gateway Software

1. Insert the MUSE Monitoring Gateway CD into the optical drive.
2. Browse to the optical drive and run **setup.exe**.
3. Follow the prompts until the installer completes.
If a **User Account Control** prompt to run **MuseGatewaySetup.msi** is displayed, choose **Yes** or **Allow**.
4. When the **Installation Complete** screen displays, click **Close**.
5. Verify that the following Windows services are installed and started:
 - **MUSE Gateway RWHAT**
 - **MUSE Gateway TFTP**
6. Right-click on the **MUSE Gateway RWHAT** service and choose **Properties**. The **MUSE Gateway RWHAT Properties** window opens.
7. Select the **Log On** tab.
8. Verify the **Allow service to interact with desktop** box is checked. If it is not checked, check it.
9. Click **OK**.
10. If you enabled the **Allow service to interact with desktop** option in step 8, restart the **MUSE Gateway RWHAT** service.

Configuring the MUSE Monitoring Gateway Software

If the IP address used by the Network Interface Card (NIC) connected to the MC/Unity network is not the default of 126.8.8.1, the **MUSE Gateway RWHAT** service configuration needs to be modified. Perform the following steps to modify the **MUSE Gateway RWHAT** service configuration.

1. Using Notepad, open **c:\program files\monitorgateway\monitorgateway.ini**.

NOTE:

You may need to use **Run as Administrator** when opening Notepad to ensure you can save the file after making changes.

2. Delete the semicolon in the **RWhat=** line.
3. Change the IP address in the **RWhat=** line to the IP address of the Monitoring Gateway NIC connected to the MC/Unity network.
For example, if the IP address of the Monitoring Gateway NIC connected to the MC/Unity network is 172.16.0.1, the line should be **RWhat=172.16.0.1**.
4. Delete the semicolon in the **RWhat_Subnet=** line.
5. Change the subnet address in the **RWhat_Subnet=** line to the subnet address of the Monitoring Gateway NIC connected to the MC/Unity network.
For example, if the subnet address of the Monitoring Gateway NIC connected to the MC/Unity network is 255.255.0.0, the line should be **RWhat_Subnet=255.255.0.0**.
6. Save your changes and exit Notepad.

7. Restart the Monitoring Gateway computer.
8. Verify that both **MUSE Gateway RWHAT** and **MUSE Gateway TFTP** services are started.

Configuring the MUSE Application Server

To ensure the MUSE system can locate and communicate with the MUSE Monitoring Gateway systems, use the following procedures to add, modify, or remove the paths to the MUSE Monitoring Gateway system(s) as needed.

Adding the Path of Each MUSE Monitoring Gateway System to the MUSE Database

Complete the following procedure to add the path of each MUSE Monitoring Gateway system to the MUSE database.

1. From within the MUSE application, go to **Setup**.
2. Select **Share Folder**.

The list of existing Share Folders is displayed.

The **Share Folder** option within MUSE is where **MUSE Generacq** folders and file name filters are configured.

3. Select **Action > New**.

The **Share Folder Properties** window opens.

4. Complete the fields as described in the following table:

Field	Task
Entry	Enter the UNC path of the ACQMON share on the MUSE Monitoring Gateway system, for example \\MMG001\ACQMON.
File Name Filter	Enter *.*.
Profile Name	Select None .

5. Click **OK**.

Modifying an Existing Share Folder Entry

The following procedure can be used to modify an existing **Share Folder** entry if necessary.

1. From within the MUSE application, go to **Setup**.
2. Select **Share Folder**.

The list of existing share folders is displayed.

3. Right-click on the share folder you want to modify and choose **Properties**.

The **Share Folder Properties** window opens.

- Complete the fields as described in the following table:

Field	Task
Entry	Enter the UNC path of the ACQMON share on the MUSE Monitoring Gateway system, for example \\MMG001\ACQMON.
File Name Filter	Enter *.*.
Profile Name	Select None .

- Click **OK**.

Removing an Existing Share Folder Entry

The following procedure can be used to delete an existing **Share Folder** entry if necessary.

- From within the MUSE application, go to **Setup**.
- Select **Share Folder**.
The list of existing share folders is displayed.
- Right-click on the share folder you want to remove and choose **Delete**.

Configuring Bedside Monitors

The bedside monitors may require additional configuration or options to successfully transmit ECGs to the MUSE system through the MUSE Monitoring Gateway. Use the following information as a high-level reference, and refer to the appropriate bedside monitor service documentation for complete details.

- All bedside monitors: **Site** and **Location** need to be defined appropriately to ensure the tests are associated with the correct MUSE site and location.
- Bx50 Monitors: In addition to **Site** and **Location** configuration, Bx50 monitors need to have a **MUSE Web URL** configured in **Webmin**. A valid URL would be in the following format: **http://<ip_or_name_of_muse_app_server>:<port>/musescripts/museweb.dll**

System Checkout

This verification is only for transmitting ECGs from bedside monitors to the MUSE system via the MUSE Monitoring Gateway.

NOTE:

This procedure does not test the retrieval of ECGs from the MUSE system via MUSE Web. The configuration and verification of MUSE Web are outside the scope of this document.

- From a bedside monitor, transmit a 12SL ECG to the MUSE system.
- In the MUSE system, select **System Status**.
- Select the **Acquisition Log**.
- Confirm that the ECG was acquired successfully into the MUSE system by locating the **PID/Name** of the transmitted ECG in the **Acquisition Log**.

Troubleshooting

Use the following troubleshooting tips if the Monitoring Gateway was installed and configured correctly, but the bedside monitor is unable to send data to it.

Troubleshooting Tips

Symptom	Condition	Action
Monitoring Gateway is not available on the bedside monitor.	Some bedside monitors may not see a new Monitoring Gateway on the network. This is especially common when the Monitoring Gateway has recently changed IP addresses.	Restarting the bedside monitor should resolve this issue.
Monitoring Gateway is available from the bedside monitor but cannot receive data.	The Monitoring Gateway system has a firewall in place.	<p>You need to add the following exceptions to the firewall:</p> <ul style="list-style-type: none"> • TFTP (UDP port 69): Allows communication from the monitors to the Monitoring Gateway. • Windows File Sharing: Allows communication from the MUSE system to the Monitoring Gateway. Depending on how the router and networks are configured, you may need to specify the MUSE IP address in the exceptions.
ECG tests sent from bedside monitors are not showing up in the MUSE system.	The user account configured to start the MUSE Generacq service on the MUSE application server does not have access to the ACQMON share on the Monitoring Gateway system.	Ensure the user account configured to start the MUSE Generacq service on the MUSE application server has access to the ACQMON share on the Monitoring Gateway system.
	The ACQMON share on the Monitoring Gateway system is not defined correctly.	Ensure the ACQMON share on the Monitoring Gateway system is set up correctly.
	The Share Folder is not set up correctly for the Monitoring Gateway system in the MUSE System Setup.	Ensure the Share Folder set up in MUSE System Setup is correctly defined.
	The ECG test has an invalid site.	Ensure the bedside monitor is configured with a valid MUSE site number. Check the MUSE Discarded Data List for the missing test(s).

Uninstalling MUSE Monitoring Gateway v1.1

Use the following procedure to uninstall Monitoring Gateway v1.1 should it need to be uninstalled for any reason.

1. Save a copy of the **c:\program files\monitorgateway\monitorgateway.ini** file to a different location for future reference.
2. Go to **Control Panel>Programs and Features**.
3. Select **Monitoring Gateway 1.1** and choose **Uninstall**.
4. Choose **Yes** when you receive the following prompt: **"Are you sure you want to uninstall MUSE Monitoring Gateway 1.1?"**

If you receive a prompt for the **User Account Control** to confirm the removal of the **Monitoring Gateway 1.1**, choose **Yes** or **Allow**.

This removes the **MUSE Gateway RWHAT** and **MUSE Gateway TFTP** services and deletes the **C:\Program Files\monitorgateway** folder.

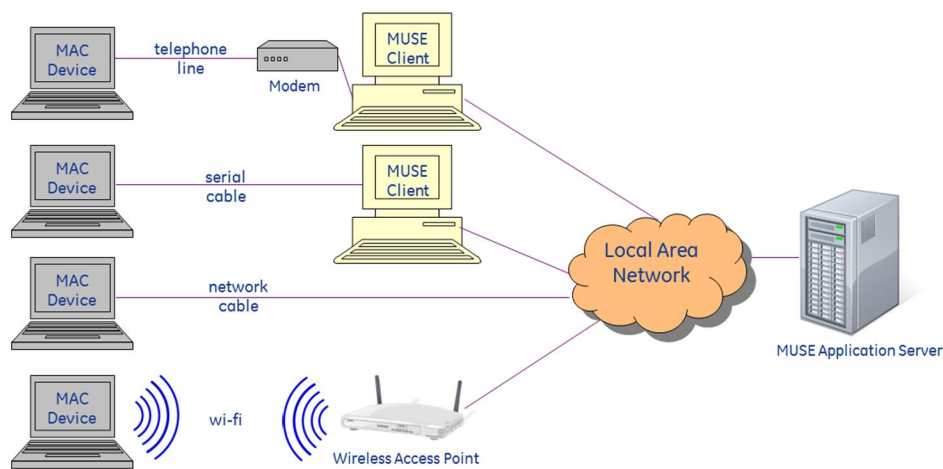
5

MAC ECG Systems to MUSE Communication

This chapter describes how to configure MAC ECG systems to send tests to MUSE v9 systems.

Theory of Operation

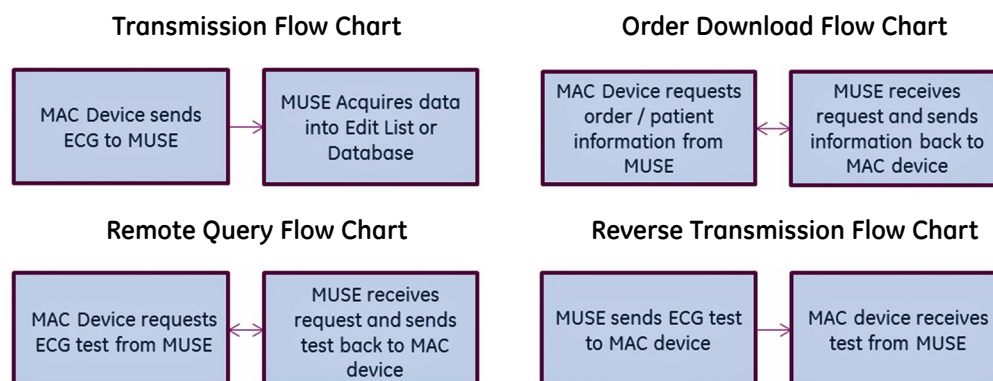
MAC ECG to MUSE communication allows you to transfer tests from MAC ECG systems to the MUSE system for viewing, editing, printing, and storage. It also allows MAC ECG systems to receive orders and/or patient demographics information from the MUSE system. Additionally, remote query allows a MAC ECG system to query for and receive tests from the MUSE system, while reverse transmission allows MUSE to send data to a MAC ECG system.



Example Network Diagram

MAC ECG devices can communicate with the MUSE system via direct serial cable, modem, wireless network, or local area network.

Data Flow Between MAC ECG Systems and the MUSE System



Customer Requirements

The customer is responsible for appropriate serial, telephony, or network connectivity between the MAC ECG systems and the MUSE systems that have been configured for MAC system to MUSE system communication.

Configuring MAC ECG to MUSE Communication

Use the following sections for configuring MAC ECG to MUSE system communication.

- Direct Serial Cable and Modem
See ["Setting Up Modems" on page 63](#) for details on setting up modems in the MUSE system.
- Wireless Network via CSI
See ["Setting Up Modems" on page 63](#) for information on setting up the CSI Network type of modem required for wireless network communication. For more detailed information on configuring MAC ECG systems to communicate with MUSE wirelessly, refer to the *MobileLink Installation Manual*.
- Local Area Network via CSI
See ["Setting Up Modems" on page 63](#) for information on setting up the CSI Network type of modem required for local area network communication. For detailed information on configuring MAC ECG systems to communicate with MUSE via local area network, refer to the *LAN Option for MAC Installation and Troubleshooting Guide*.
- Wireless or Local Area Network via DCP (DCAR Communication Protocol)
Some GE Healthcare MAC ECG systems can use DCP to communicate with the MUSE system. See ["Setting Up DCP Inbound Communication" on page 69](#) for information on setting up the MUSE DCP Server. For detailed information on configuring MAC ECG systems to communicate with the MUSE system via local area network, refer to the *LAN Option for MAC Installation and Troubleshooting Guide*.

Setting Up Modems

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

MUSE Modem Types

Modem Type	Description
FAX Modem	Supports outgoing fax transmission. Requires physical modem.
CSI Modem	Supports Plain Old Telephone Service (POTS) modem communication to compatible MAC systems. Requires physical modem.
CSI Direct	Supports direct serial cable communication with compatible MAC systems. Requires physical serial cable.
CSI Network	Supports wireless and/or LAN cart connections with compatible MAC systems.

To support any of the available modem types on MUSE v9, the MUSE **Modem** feature must be installed and the **MUSE Modem** service must be running.

NOTE:

During an upgrade from MUSE v7.x, all CSI Wireless modems are converted to CSI Network modems. If you see a CSI Wireless entry in the **Modem Setup** list, the modem server for that modem was not upgraded or is missing. Refer to the *MUSE v9 Cardiology System Installation and Upgrade Manual* for information on performing a wireless modem migration during a MUSE v7 upgrade.

Adding the Wireless/LAN Communication Option to the MUSE System

The Wireless/LAN Communication option is required for Wireless/LAN CSI Communication. Use the following procedure to add the Wireless/LAN Communication option to the MUSE system. This procedure may only be performed by a qualified GE Healthcare service representative.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full or partial shutdown of the MUSE system following the auto shutdown procedures described in the "System Administration" chapter of the *MUSE v9 Cardiology Information System Service Manual*.

NOTE:

If you are just checking to see if the option is already enabled, a shutdown is not required. If, however, you have to enable or disable the option, the MUSE services will be restarted and a shutdown is required.

3. Go to **Control Panel>Programs and Features**.
4. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
5. Choose **Modify** and click **Next**.
The **Select Features** window opens.

6. Continue to click **Next** on each window until you reach the **Choose MUSE Options** window.
7. Verify that **Wireless/LAN Communication** is checked.
If it is not, check it now.
8. Click **Next**.
The **MUSE Serial Number** window opens.
9. If you added the **Wireless/LAN Communication** option in step 7, enter the **Options Configuration Password**.
NOTE:
Only qualified GE Healthcare service representatives have access to this password. This password cannot be provided to customers.
10. Click **Next** until your changes are applied and the **Maintenance Complete** window opens.
11. Click **Finish**.
12. If you performed a full or partial shutdown of the MUSE system in step 2, cancel the shutdown following the procedures described in the "System Administration" chapter of the *MUSE v9 Cardiology Information System Service Manual*.

Verifying/Installing the MUSE Modem Service

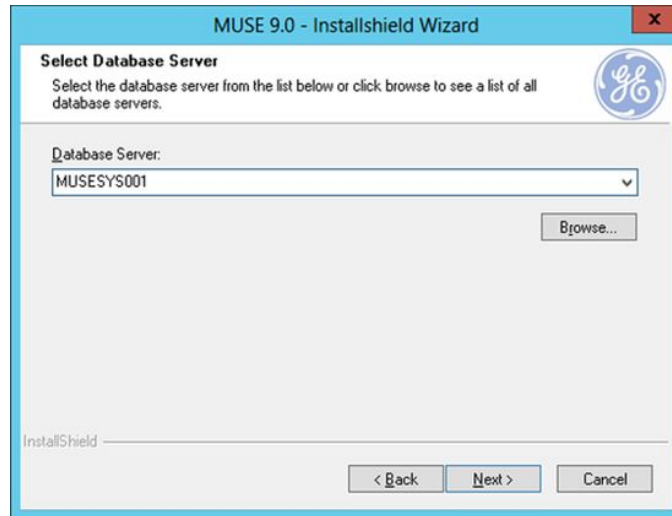
The MUSE **Modem** feature and service are typically installed during the initial installation of the MUSE client. Use the following instructions to verify whether the MUSE **Modem** feature and service are installed on the MUSE system and to install them if they are not. These steps can be performed on the MUSE application server or MUSE workstation.

1. Log on to the MUSE system you want to configure as the MUSE Administrator user.
2. Go to **Control Panel>Programs and Features**.
3. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
4. Choose **Modify** and click **Next**.
The **Select Features** window opens.
5. In the **Select Features** window, perform one of the following:
 - If the check box next to **Modem** is already checked, click **Cancel**. The **Modem** feature is already installed.
Proceed to "[Setting Up a Modem Device](#)" on page 67".
 - If the check box next to **Modem** is not checked, check the box and click **Next**.

NOTE:

On the MUSE application server the **Modem** feature will be a sub-item of **Server>Services**. On the MUSE client workstation, the **Modem** feature will be a sub-item of **MUSE Client**.

6. Click **Next** until the **Select Database Server** window opens.



7. In the **Database Server** field, click **Browse** or type the name of the SQL Server where the MUSE databases are installed. Be sure to include the instance name if a non-default SQL Server instance is being used.

The following is a default instance example:

SQLSERVER

Named instance example:

SQLSERVER\INSTANCE

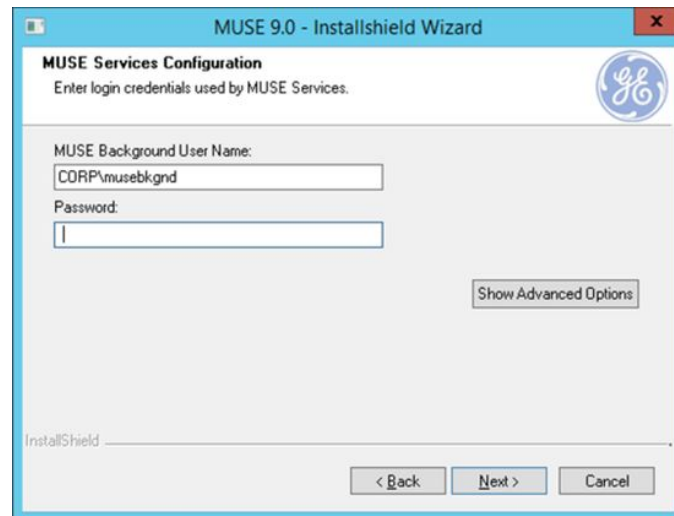
NOTE:

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

8. Click **Next**.

The installer validates that the database is available. If the database cannot be found, the following SQL Server Validation warning message will be 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 still want to continue?** Click **No** and verify the name and instance of the SQL Server before proceeding.

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



9. Enter the **MUSE Background User Name** and **Password** for the MUSE Background account.
 - The default user name for the MUSE Background account is **MUSEBknd**.
 - If you are using a domain account, enter the name in <domain name>\<user name> format.
 - If you are using a local account, enter the user name in .\<user name> format.

The MUSE services will be installed using the specified MUSE Service Manager account and password.

NOTE:

The **Show Advanced Options** button can be used to specify Service Command Line Arguments. Do not use this button unless specifically directed to do so by GE Healthcare's MUSE Engineering or MUSE Technical Support.

10. Click **Next**.
 The installer validates that the user account you chose exists on the system.
 If you receive a warning message that the account was not found or user validation failed, choose **No** to the prompt to return to the **MUSE Services Configuration** and check the following:
 - The user account and password are correct
 - The account exists
 If the user account is validated, the **Maintenance Complete** window opens.
11. Click **Finish**.
12. Verify that the **MUSE** and **MUSE Modem** services are started.

Setting Up a Modem Device

Use the following instructions to set up a modem device.

1. Log on to the MUSE system as a user with privileges to modify settings in **MUSE Setup**.
2. Go to **System>Setup**.
3. In the **Navigation** pane, select **Modems**.
4. Perform one of the following:
 - a. To create a new modem, go to **Action>New** and select one of the following:

Modem	Description
Fax Modem	Used for physical FAX modems
CSI Modem	Used for physical CSI modems
CSI Direct	Used for direct serial cable at a MUSE client
CSI Network	Used for CSI LAN or Wireless Carts

The appropriate **Modem Properties** window opens.

- b. To modify an existing modem, right-click on an existing entry and choose **Properties**.

The appropriate **Modem Properties** window opens.

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

FAX, CSI, or CSI Direct Modem Properties

Field	Description
Computer Name	Name of the computer where the modem is physically installed.
Port	For FAX modems and CSI modems, this is the port where the modem is physically connected. For CSI Direct, this is the port where the serial cable is physically connected.
Baud	115.2K (CSI Direct), 9600 (CSI, FAX) ¹
¹ If the FAX modem encounters problems at 9600 baud, use 4800 baud.	

CSI Network Modem Properties

Field	Description
Computer Name	Name of the computer where the connection is supported.
IP Address or Hostname	The IP address or hostname assigned to the device.

CSI Network Modem Properties (cont'd.)

Field	Description
Port	Port this connection is using.
Retry Interval in Seconds	Defines the upper limit of the time delay between the cart's attempts to communicate with the MUSE system. The default is 30 seconds.

NOTE:

Refer to the appropriate document referenced below for detailed installation and configuration information for the CSI Network modem types when used with compatible MAC ECG systems:

- *MobileLink Wireless Communication Installation Manual*
- *LAN Option for MAC Resting ECG Systems Installation and Troubleshooting Guide*

- Click **OK** to save your changes or **Close/Cancel** to ignore your changes.

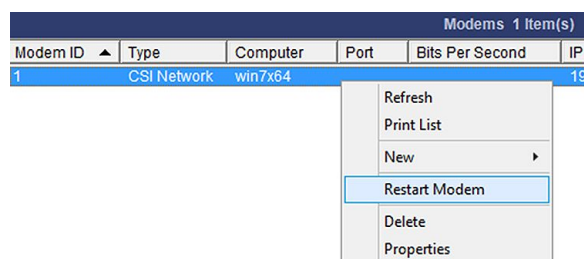
NOTE:

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

Restarting Modems

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

- Log on to the MUSE application.
- Select **Setup>Modems**.
- Select the modem(s) that you want to restart, right-click on it/them, and select **Restart Modem**.



NOTE:

There is also a **Restart Modem** icon on the toolbar that can be used to restart a modem.



A message displays that the modems were successfully restarted.

NOTE:

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

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

For more information about the modems, including when they start or restart, refer to the **MUSE Application** log.

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

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

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

Setting Up DCP Inbound Communication

The MUSE system can receive inbound tests and requests for orders via DCP Inbound communication. Compatible GE Healthcare MAC ECG systems can use the protocol to communicate directly with the MUSE application server wirelessly or via LAN.

Verifying/Installing the DCP Inbound Service and DCP Communication Option

The MUSE **DCP Inbound** service and **DCP Communication** option are typically installed during the initial installation of the MUSE system. Use the following instructions to verify whether the MUSE **DCP Inbound** service and **DCP Communication** option are installed on the MUSE system and to install them if they are not. This procedure is performed on the MUSE application server. It may only be performed by a qualified GE Healthcare service representative.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full or partial shutdown of the MUSE system following the auto shutdown procedures described in the "System Administration" chapter of the *MUSE v9 Cardiology Information System Service Manual*.

NOTE:

If you are just checking to see if the option is already enabled, a shutdown is not required. If, however, you have to enable or disable the option, the MUSE services will be restarted and a shutdown is required.

3. Go to **Control Panel > Programs and Features**.

4. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
5. Choose **Modify** and click **Next**.
The **Select Features** window opens.
6. In the **Select Features** window, go to **Server>Services>DCP** and verify that **DCP Inbound** is checked.
If it is not, check it now and click **Next**.
7. Continue to click **Next** on each window until you reach the **Choose MUSE Options** window.
8. Verify that **DCP Communication** is checked.
If it is not, check it now.
9. Click **Next**.
The **MUSE Serial Number** window opens.
10. If you added the **DCP communication** option in step 8, enter the **Options Configuration Password**.
NOTE:
Only qualified GE Healthcare service representatives have access to this password. This password cannot be provided to customers.
11. Click **Next** until your changes are applied and the **Maintenance Complete** window opens.
12. Click **Finish**.
13. If you performed a full or partial shutdown of the MUSE system in step 2, cancel the shutdown following the procedures described in the “System Administration” chapter of the *MUSE v9 Cardiology Information System Service Manual*.
14. Verify that the **MUSE DCP Inbound** service is started.

Setting Up the DCP Server Configuration in the MUSE System

By default, the **DCP Inbound** service has a **Device Friendly Name** of MUSE and listens on port 9240 of all network interfaces on the MUSE application server.

Perform the following steps to modify these defaults:

1. Log on to the MUSE system as a user with privileges to modify settings in **MUSE Setup**.
2. Go to **System>Setup**.
3. In the **Navigation** pane, select **System**.
4. Right-click on the MUSE entry and choose **Properties**.
The **System Properties** window opens.
5. Select **DCP Configuration**.

6. Modify the fields using the information in the following table.

Field	Description/Action
Device Friendly Name	This is the name the compatible device will see when finding DCP servers. The default is MUSE. Change this if desired.
Server Port	This is the port on which the DCP Inbound service is listening for inbound connections. The default is 9240. Change this if necessary.
Network Interfaces	This is where you can specify which network interface the DCP Server should listen on. This field is blank by default so it will listen on all network interfaces on the MUSE application server. To configure the DCP Server to listen only on a single network interface, for example IPv4, you can type the IPv4 IP address into this field.
Server Addresses	This is a read-only output indicating the Server Address(es) that the DCP Inbound service is currently listening on. This is the full DCP URL that can be used to define this MUSE system on a compatible DCP client device such as a MAC 2000. Multiple server addresses may be listed if the Network Interfaces field is blank.

7. Click **OK** to save your changes or **Close/Cancel** to ignore your changes.

NOTE:

Refer to the *LAN Option for MAC Installation and Troubleshooting Guide* for detailed installation and configuration information regarding the use of the DCP Protocol on compatible MAC ECG systems.

8. If any configuration changes were made, restart the MUSE **DCP Inbound** service on the MUSE Application server.

System Checkout

Complete the following verification procedures to ensure the MAC ECG devices can successfully transmit tests to the MUSE system and download orders from the MUSE system.

CSI Transmission to the MUSE System

1. Transmit an ECG test from the MAC ECG device to the MUSE system using the CSI protocol.
2. Verify the test is successfully acquired into the MUSE system.

MUSE Order Download via CSI

1. From the MAC ECG device, download an order from the MUSE system using the CSI protocol.
2. Verify the order is successfully downloaded to the MAC ECG device.

DCP Transmission to the MUSE System

1. Transmit an ECG test from the MAC ECG device to the MUSE system using the DCP protocol.
2. Verify the test is successfully acquired into the MUSE system.

MUSE Order Download via DCP

1. From the MAC ECG device, download an order from the MUSE system using the DCP protocol.
2. Verify the order is successfully downloaded to the MAC ECG device.

MUSE eDoc Connect

This chapter describes how to configure the MUSE **eDoc Connect** option used to process incoming electronic document files on the MUSE v9 system.

Theory of Operation

The MUSE **eDoc Connect** option allows the MUSE system to acquire electronic documents. Once the electronic device types and shared folders are appropriately defined in the MUSE system, devices transfer electronic documents to a shared folder. The **MUSE Generacq** service searches this shared folder for files and stores them in the MUSE database. Electronic document tests may also be acquired via the MUSE Acquisition module. Refer to the *MUSE v9 Cardiology Information System Operator Manual* for instructions on how to acquire electronic documents via the MUSE Acquisition module.



eDoc Connect Acquisition Flow Chart

The MUSE system can acquire the following types of electronic documents:

- PDF – Portable Document Format File
- PDF/A – Portable Document Format File/Archive
- JPG – JPEG Image
- DOC – Microsoft Word Document
- DOCX – Microsoft Word Open XML Document
- TIFF – Tagged Image File Format
- PNG – Portable Network Graphic
- TXT – Plain Text File

Preparing to Configure eDoc Connect

The following steps are performed by GE Healthcare personnel to prepare for the installation and configuration of the eDoc Connect option:

1. A MUSE system customer contacts GE Healthcare to configure their MUSE system to receive and store electronic document test files.
2. A GE Healthcare representative asks for several examples of the documents the customer wants to import and inquires about the ability of the devices to export these documents. The GE Healthcare representative also gathers information regarding the test type and target MUSE site and location for these test results.
3. GE Healthcare creates and tests an **Acquisition Profile** that allows the electronic documents to be automatically imported into the target MUSE site and location, with the correct **Test Type** and **Patient/Test** demographics.

NOTE:

The Acquisition Profile is created using the Acquisition Profile Tool. Use of the Acquisition Profile Tool to create the Acquisition Profile is outside the scope of this document.

After GE Healthcare collects the necessary information and creates the Acquisition Profiles, the eDoc Connect option can be installed and configured, as described in the remainder of this chapter.

Customer Requirements

The customer is responsible for the following:

- Supplying electronic documents that meet the configured **eDoc Connect** profile(s).
- Establishing network connectivity between the device that outputs the electronic documents and the MUSE system.
- Granting the user account configured to start the **MUSE Generacq** service with **Read** and **Delete** permissions to the files and share location of the electronic documents.

Installing and Configuring MUSE eDoc Connect

Installing and configuring **eDoc Connect** consists of the following tasks:

- [“Installing the eDoc Connect Option in the MUSE System” on page 75](#)
- [“Adding or Enabling a Test Type in the MUSE System” on page 75](#)
- [“Setting up the Acquisition Profile in the MUSE System” on page 76](#)
- [“Setting up the File Share” on page 77](#)

Installing the eDoc Connect Option in the MUSE System

Use the following procedure to add the **eDoc Connect** option to the MUSE system.

NOTE:

This procedure may only be performed by a qualified GE Healthcare service representative.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full or partial shutdown of the MUSE system following the auto shutdown procedures described in the “System Administration” chapter of the *MUSE v9 Cardiology Information System Service Manual*.

NOTE:

If you are just checking to see if the option is already enabled, a shutdown is not required. If, however, you have to enable or disable the option, the MUSE services will be restarted and a shutdown is required.

3. From the Windows **Control Panel**, go to **Programs and Features**.
4. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
5. Choose **Modify** and click **Next**.
The **Select Feature** window opens.
6. Continue to click **Next** on each window until you reach the **Choose MUSE Options** window.
7. Verify that **eDoc Connect** is checked.
If it is not, check it now.
8. Click **Next**.
The **MUSE Serial Number** window opens.
9. If you added the **eDoc Connect** option in step 7, you need to enter the **Options Configuration Password**.

NOTE:

Only qualified GE Healthcare service representatives have access to this password. This password cannot be provided to customers.

10. Click **Next** until your changes are applied and the **Maintenance Complete** window opens.
11. Click **Finish**.
12. If you performed a full or partial shutdown of the MUSE system in step 2, cancel the shutdown following the procedures described in the “System Administration” chapter of the *MUSE v9 Cardiology Information System Service Manual*.

Adding or Enabling a Test Type in the MUSE System

Use the following two procedures to create a new test type or to enable, disable, or modify an existing test type, as needed.

Creating a New Test Type

1. From within the MUSE application, go to **Setup**.
2. Select **Test Types**.
The list of existing test types is displayed.
3. Select **Action** and click **New**.
4. Complete the fields as indicated in the following table:

Field	Task
Test Type Name	Enter the name of the test type.
Test Type Abbreviation	Enter the three character abbreviation for the test type.
Enabled for Sites	Put a check in the box next to sites for which this test type should be enabled.

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

Enabling, Disabling, or Modifying an Existing Test Type

1. From within the MUSE application, go to **Setup**.
2. Select **Test Types**.
A list of existing test types is displayed.
3. Right-click on the test type you want to modify and choose **Properties**.
The **Test Type Properties** window opens.
4. Check the check box next to each site you want to enable for this test type.
If the box is unchecked for a site, it means the test type is disabled for that site.
If the test type is not a system-defined test type, then the **Test Type Name** and **Test Type Abbreviation** may also be changed at this time.
5. Click **OK** to save your changes.
If no changes were made, click **Close** to close the **Test Type Properties**.

Setting up the Acquisition Profile in the MUSE System

Use the following two procedures to create a new acquisition profile or to modify an existing one, as needed.

Creating a New Acquisition Profile

To create a new acquisition profile:

1. From within the MUSE application, go to **Setup**.
2. Select **Acquisition Profile**.
The list of existing acquisition profiles is displayed.
If this is the first acquisition profile, the list is empty.
3. Select **Action** and click **New**.

4. Complete the fields as indicated in the following table.

Field	Value
Name	Enter the name of the profile. It is recommended that the name reflect the test type, site and location. For example: CATH - SITE 1 - LOC 50
Test Type	Choose the test type from the drop-down list.
Site	Choose the MUSE site from the drop-down list.
Location	Choose the MUSE site location from the drop-down list.
Profile	Click Import , browse to the file created in the Acquisition Profile Tool , and click Open .

5. Click **OK**.

Modifying an Existing Acquisition Profile

1. From within the MUSE application, go to **Setup**.
2. Select **Acquisition Profile**.
The list of existing acquisition profiles is displayed.
3. Right-click on the acquisition profile you want to modify and choose **Properties**.
4. Modify the fields as needed.
5. Click **OK**.

Setting up the File Share

To transfer electronic documents from a device to the MUSE system, you need to create a share. Use the following instructions to create a share.

Creating the Windows File Share

The share can be a local folder on the MUSE file server that is shared to the device, or a share on a device that the MUSE application server can access. The share can also be a gateway-type computer to which both the MUSE application server and the device have access. In any case, the user account configured to start the **MUSE Generacq** service must have access to the location through **Full Control** file and share permissions.

Setting up the Share Folder in MUSE

Use the following two procedures to create a new share folder or to modify an existing one, as needed.

Creating a New Share Folder

1. From within the MUSE application, go to **Setup**.
2. Select **Share Folder**.
The list of existing share folders is displayed.
3. Select **Action** and click **New**.

4. Complete the fields as indicated in the following table:

Field	Value
Entry	Enter the UNC or Local Path from which the electronic documents are parsed.
File Name Filter	Enter the file mask to filter on. For example *.PDF ensures that only files with an extension of .PDF are processed.
Profile Name	Choose the appropriate MUSE profile name from the drop-down list. All eDoc Connect Share Folders must have a profile name selected.

5. Click **OK**.

Modifying an Existing Share Folder

1. From within the MUSE application, go to **Setup**.
2. Select **Share Folder**.
The list of existing share folders is displayed.
3. Right-click on the share folder you want to modify and choose **Properties**.
4. Modify the fields as needed.
5. Click **OK**.

System Checkout

Complete the following procedure to ensure that the MUSE system can successfully acquire electronic documents.

1. From a device capable of transferring electronic documents, transfer an electronic document to the appropriate shared folder on the MUSE system.
2. Log on to the MUSE system.
3. Verify the test is displayed in the MUSE system **Edit List**.
4. Verify the test can be opened in the **MUSE Editor**.

Troubleshooting

Symptom	Condition	Action
Document imported with incorrect acquisition profile.	An electronic document was copied to an incorrect folder or bulk acquired using the wrong acquisition profile. If this happens then it is most likely acquired with incorrect attributes (test type, site, location, etc.)	To correct this, discard the test. Once on the Discarded Data List , you can reacquire the electronic document using the correct acquisition profile. Right-click on the test on the Discarded Data List , choose Correct Acquisition Profile , and choose the correct acquisition profile with which to reimport the test.
Cannot acquire electronic documents.	The user account that is configured to start the MUSE Generacq service on the MUSE application server does not have access to the folder or share defined for the Share Folder in the MUSE system.	Ensure the user account configured to start the MUSE Generacq service on the MUSE application server has access to the folder or share defined for the Share Folder in the MUSE system.
	The Share Folder is not set up correctly for the location of the electronic document files in MUSE System Setup .	Ensure the Share Folder set up in MUSE System Setup is correctly defined.

MUSE XML Import Option

This chapter describes how to configure the **MUSE XML Import** option to process incoming XML files on the MUSE v9 system.

Theory of Operation

The **XML Import** option allows the MUSE system to acquire XML files that meet the MUSE Transactional XML specification. Devices that are able to output the appropriately structured XML files send their XML files into a shared folder on the MUSE system. The **MUSE XML Parser** service searches this shared folder, acquires the XML files from the shared folder, and moves them into the MUSE system for processing. The test is normalized and stored in the MUSE database.



XML Acquisition Flow Chart

Customer Requirements

The customer is responsible for supplying the following:

- XML files that meet the MUSE Transactional XML specification. Refer to the *MUSE Cardiology Information System Transactional XML Developer's Guide* for details.
- Network connectivity between the device that can output XML files and the MUSE application server.

Installing and Configuring the MUSE XML Import Option

Adding the **XML Import** option consists of the following tasks:

- [“Installing the XML Import Option and the MUSE XML Parser Service” on page 82](#)
- [“Setting up the XML Shared Folder” on page 83](#)
- [“Using XMLCONFIG.EXE to Add, Update, or Delete XML Devices” on page 83](#)

Installing the XML Import Option and the MUSE XML Parser Service

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

NOTE:

This procedure may only be performed by a qualified GE Healthcare service representative.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full or partial shutdown of the MUSE system following the auto shutdown procedures described in the "System Administration" chapter of the *MUSE v9 Cardiology Information System Service Manual*.

NOTE:

If you are just checking to see if the option is already enabled, a shutdown is not required. If, however, you have to enable or disable the option, the MUSE services will be restarted and a shutdown is required.

3. From the Windows **Control Panel**, go to **Programs and Features**.
4. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
5. Choose **Modify** and click **Next**.
The **Select Feature** window opens.
6. In the **Select Features** window, go to **Server>Services** and verify that **XML** is checked.
This installs the **MUSE XML Parser** service.
7. Continue to click **Next** on each window until you reach the **Choose MUSE Options** window.
8. Verify that **XML Import** is checked.
If it is not, check it now.
9. Click **Next**.
The **MUSE Serial Number** window opens.
10. If you added the **XML Import** option in step 8, you need to enter the **Options Configuration Password**.

NOTE:

Only qualified GE Healthcare service representatives have access to this password. This password cannot be provided to customers.

11. Click **Next** until your changes are applied and the **Maintenance Complete** window opens.
12. Click **Finish**.
13. If you performed a full or partial shutdown of the MUSE system in step 2, cancel the shutdown following the procedures described in the "System Administration" chapter of the *MUSE v9 Cardiology Information System Service Manual*.

Setting up the XML Shared Folder

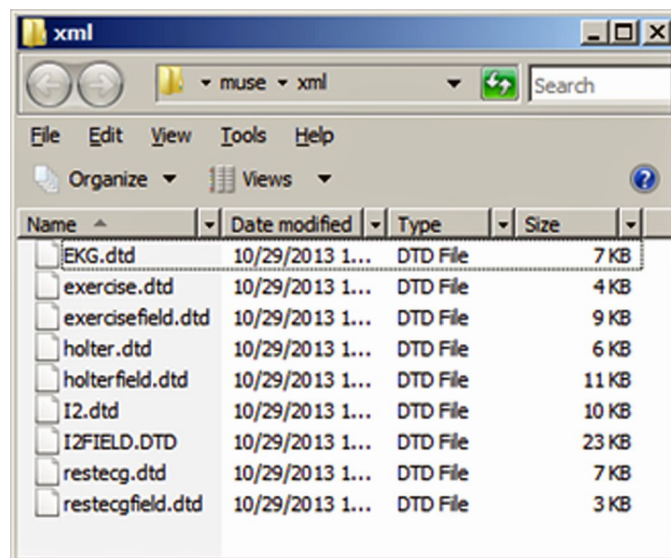
To transfer XML tests from an XML-capable device to the MUSE system, you need to create a shared folder on the MUSE system.

The **MUSE XML Parser** service on the MUSE application server is only configured to check the MUSE XML folder (default is **d:\muse\xml**) for incoming XML files to process.

This folder may need to be shared to allow XML-capable devices to transfer records into it. If this folder is shared, the XML-capable device that will be writing data to the share must have access to it. Customers are responsible for ensuring this connectivity between the XML device and the MUSE system.

NOTE:

There are nine DTD files in the MUSE XML folder. These .DTD files are required for the MUSE system to acquire XML records. These files must not be altered or deleted.



Using XMLCONFIG.EXE to Add, Update, or Delete XML Devices

Use the following two procedures to add XML devices or to update or delete XML devices as needed. Settings for known XML devices are provided after these procedures.

Using XMLCONFIG.EXE to Add a New XML Device

The **XMLCONFIG** utility inserts entries into the **cfgXmlInput** table in the **MUSE_System** database.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Run the **xmlconfig.exe** utility located in the folder where the MUSE application is installed (default is **c:\Program Files(x86)\MUSE**).

The **XML Input Devices** window opens.

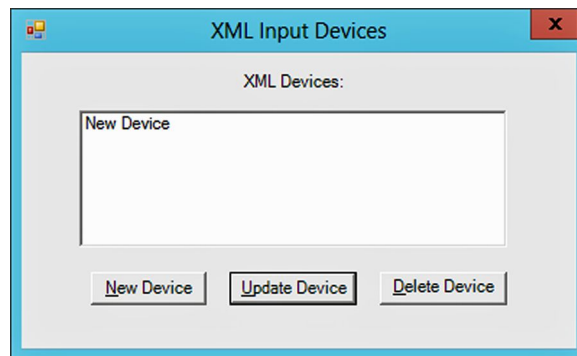
3. Click **New Device**.

The **Add a New XML Device** window opens.

4. Enter the device configuration using the following table.

Field	Value
Device Name	Enter a unique name for each device. The value entered here must match the <AcquisitionDevice> value in the incoming XML file.
Device Type	Select ECG . No other data types are supported at this time.
Manufacturer	Select the appropriate manufacturer. Anyone other than Physio Controls or Getemed is acceptable unless the device is actually a Physio Controls (except for LP15-GL) or Getemed device. The specific configurations for the Physio Control LP12 and Getemed devices are documented in "Known XML Device Configurations" on page 85. When in doubt, choose Other .
Image Type	Always set this to Image as Waveform Data Points .
Analysis Function	Always set this to XML_AnalyzeWaveform . This is case sensitive and is auto-populated in the XMLCONFIG utility; do not change this value.

5. Click **OK**.
6. Verify the **Device Name** has been added to the list of **XML Devices** in the **XMLCONFIG** utility.



7. Close the **XMLCONFIG** utility.
8. Restart the **MUSE XML Parser** service.

Using XMLCONFIG.EXE to Update or Delete a Device

1. Log in to the MUSE application server as the MUSE Administrator user.
2. Run the **xmlconfig.exe** utility located in the folder where the MUSE application is installed (default is **c:\Program Files (x86)\MUSE**).

The **XML Input Devices** window opens.

3. To update a device, select the device and click **Update Device** and use the information in step 4 of the ["Using XMLCONFIG.EXE to Add a New XML Device" on page 83](#).

NOTE:

When updating a device, the device name cannot be changed. To change the name of a device, the device must first be deleted and then recreated with a new name.

To delete a device, click **Delete Device**.

4. Click **OK**.
5. Close the **XMLCONFIG** utility.
6. Restart the **MUSE XML Parser** service.

Known XML Device Configurations

The following windows display the XML device configurations you must use to configure the following specific devices:

- Physio Controls LifePak 12
- Physio Controls LifePak 15
- Getemed CM3012

- DataMed Format Translator
- Zoll RescueNet

Physio Controls LifePak 12

A screenshot of the 'Add a New XML Device' dialog box. The title bar reads 'Add a New XML Device'. The form contains the following fields: 'Device Name' with the value 'LP12', 'Device Type' set to 'ECG', 'Manufacturer' set to 'Physio Controls', 'Image Type' set to 'Image as Waveform Data Points', and 'Analysis Function' set to 'XML_AnalyzeWaveform'. At the bottom are three buttons: 'Ok', 'Close', and 'Apply'.

Getemed CM3012

A screenshot of the 'Add a New XML Device' dialog box. The title bar reads 'Add a New XML Device'. The form contains the following fields: 'Device Name' with the value 'CM3012', 'Device Type' set to 'ECG', 'Manufacturer' set to 'Getemed', 'Image Type' set to 'Image as Waveform Data Points', and 'Analysis Function' set to 'XML_AnalyzeWaveform'. At the bottom are three buttons: 'Ok', 'Close', and 'Apply'.

Physio Controls LifePak 15

A screenshot of the 'Add a New XML Device' dialog box. The title bar reads 'Add a New XML Device'. The form contains the following fields: 'Device Name' with the value 'LP15-GL', 'Device Type' set to 'ECG', 'Manufacturer' set to 'DataMed', 'Image Type' set to 'Image as Waveform Data Points', and 'Analysis Function' set to 'XML_AnalyzeWaveform'. At the bottom are three buttons: 'Ok', 'Close', and 'Apply'.

DataMed Format Translator

A screenshot of the 'Add a New XML Device' dialog box. The title bar reads 'Add a New XML Device'. The form contains the following fields: 'Device Name' with the value 'DataMedFT', 'Device Type' set to 'ECG', 'Manufacturer' set to 'DataMed', 'Image Type' set to 'Image as Waveform Data Points', and 'Analysis Function' set to 'XML_AnalyzeWaveform'. At the bottom are three buttons: 'Ok', 'Close', and 'Apply'.

Zoll RescueNet

Device Name: ZOLLRN

Device Type: ECG

Manufacturer: Zoll Medical

Image Type: Image as Waveform Data Points

Analysis Function: XML_AnalyzeWaveform

Ok Close Apply

System Checkout

Complete the following procedure to ensure that the MUSE **XML Import** option is setup properly.

1. Transfer an XML file to the XML folder on the MUSE system.
2. Log on to the MUSE system.
3. Verify the test is displayed in the MUSE system **Edit List**.
4. Verify the test can be opened in the MUSE **Editor**.

Troubleshooting

Use the following troubleshooting tips if something is not working correctly.

Symptom	Condition	Action
The XML file is not processed from the XML folder.	The MUSE XML Parser service is not started.	Start the MUSE XML Parser service.
XML is renamed to BAD in the MUSE XML folder.	The XMLCONFIG.EXE configuration is incorrect.	Ensure the XMLCONFIG.EXE configuration is correct.
	MUSE XML Parser is unable to process the XML file.	Check the MUSE application log for details.

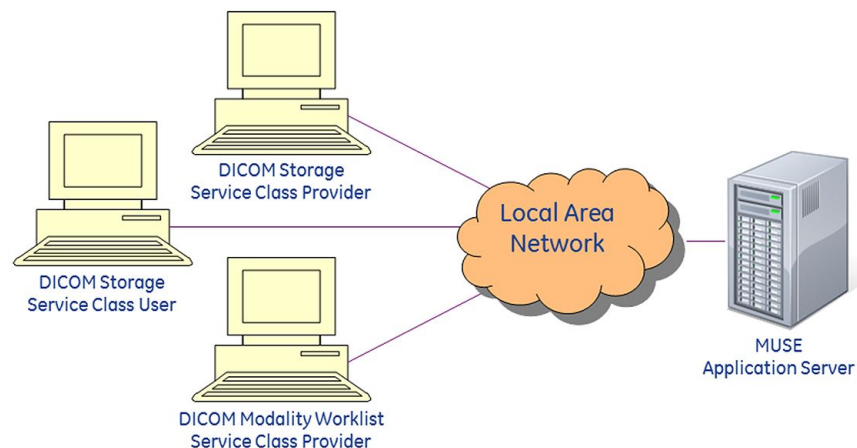
DICOM Communication

This chapter describes how to configure the system for DICOM communication. For detailed information on DICOM conformance, refer to the *MUSE v9 Cardiology Information System DICOM Conformance Statement*.

Theory of Operation

The MUSE system supports DICOM functionality in three different ways. The following table provides a description of each.

Feature	Description
DICOM Storage Service Class Provider (SCP)	Allows DICOM ECG tests to be received by the MUSE system. Storage Commitment is supported. The MUSE system acts as a DICOM Storage Service Class Provider. NOTE: Inbound DICOM tests can only be acquired into MUSE Site 1 and will be acquired without any MUSE location information. This means that tests acquired via DICOM and intended for a MUSE Site other than 1 must be discarded and recovered to the correct site. Furthermore, non-default report distribution locations cannot be used for routing the test when it is acquired. The location of the test, however, can be changed in the MUSE Editor.
DICOM Storage Service Class User (SCU)	Allows tests to be sent from the MUSE system to DICOM devices. Storage Commitment is supported. The system acts as a DICOM Storage Service Class User.
DICOM Modality Worklist (MWL) Service Class User (SCU)	Allows the system to receive orders from DICOM Modality Worklist Service Class Providers. The system queries Modality Worklist Service Class Provider (SCP) for Modality Worklist orders and updates the system orders database. The system acts as a DICOM Modality Worklist Service Class User.



Example Network Diagram

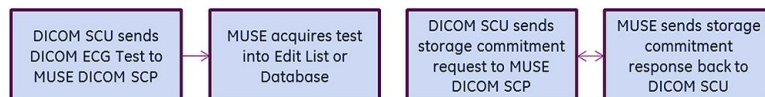
Transmission Flow Charts

The following descriptions and flow charts explain the flow of data between:

- Sending DICOM SCU and the receiving MUSE DICOM SCP
- Sending MUSE DICOM SCU and the receiving DICOM SCP
- MUSE MWL SCU and DICOM MWL SCP

DICOM SCU to MUSE DICOM SCP

The DICOM device Storage Service Class User transmits a DICOM test across the network to the MUSE DICOM Storage Service Class Provider service. The test is then normalized on the MUSE system and stored in the database. If storage commitment is enabled, a DICOM SCU sends a storage commitment request to the MUSE system and the MUSE system returns a storage commitment response to the DICOM SCU.



MUSE DICOM SCU to DICOM SCP

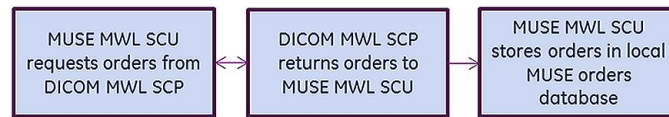
The MUSE DICOM device Storage Service Class User transmits a DICOM test across the network to a receiving DICOM Storage Service Class Provider. If storage commitment is enabled, the MUSE system sends a storage commitment request to the DICOM SCP, and the DICOM SCP returns a storage commitment response to the system.



MUSE Modality Worklist SCU

The DICOM Modality Worklist Service Class User service queries the DICOM Modality Worklist Service Class Provider for orders. Orders that are returned are

created/updated in the system orders database. These orders behave the same as orders received via the MUSE HL7 Parser.



MUSE Services

Each system DICOM function has its own MUSE service on the system application server, as described in the following table.

MUSE Service Name	DICOM Function
<i>MUSE DICOM Modality Worklist Client</i>	DICOM Modality Worklist (MWL) Service Class User (SCU)
<i>MUSE DICOM Storage Provider</i>	DICOM Storage Service Class Provider (SCP)
<i>MUSE DICOM Storage User</i>	DICOM Storage Service Class User (SCU)

In addition to these services, the **MUSE Normal** service is used to normalize all inbound test data, including DICOM, and the **MUSE Format** service is used to format all outbound data, including DICOM IOD and DICOM Encapsulated PDF.

Customer Requirements

The customer is responsible for supplying the following:

- Network connectivity between the system and the non-system DICOM services and devices.
- AE titles, IP addresses, and ports for all non-system DICOM services and devices.

Configuring DICOM Communication

Follow the instructions in this section to complete the configuration of MUSE DICOM Communication.

- [“Adding the DICOM Service\(s\) and Option to the MUSE System” on page 92](#)
- [“Configuring the MUSE System to Receive DICOM Tests” on page 93](#)
- [“Configuring the System to Send DICOM Tests” on page 95](#)
- [“Configuring the System to Query for DICOM Orders” on page 99](#)

Adding the DICOM Service(s) and Option to the MUSE System

There are three DICOM services and one DICOM option. Use the following procedure to add the DICOM service(s) and option to the MUSE system.

NOTE:

This procedure can only be performed by a qualified GE Healthcare service representative.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full or partial shutdown of the MUSE system following the auto shutdown procedures described in the “System Administration” chapter of the *MUSE v9 Cardiology Information System Service Manual*.

NOTE:

If you are just checking to see if the option is already enabled, a shutdown is not required. If, however, you have to enable or disable the option, the MUSE services will be restarted and a shutdown is required.

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 Features** window opens.
6. Go to **Server > Services**.
7. Scroll down to the bottom of the list and select the checkbox next to DICOM.
Selecting DICOM automatically selects all DICOM services.
8. Click **Next**.
The **MUSE Client Configuration** window opens.
9. Continue and click **Next** on each window until you come to the **Choose MUSE Options** window.
10. Scroll to the bottom of the list and verify that **DICOM** is selected.
If **DICOM** is not selected, select it now.
11. Click **Next**.
The **MUSE Serial Number** window opens.
12. If you added the **DICOM** option in step 10, you need to enter the **Options Confirmation Password**.

NOTE:

Only qualified GE Healthcare service representatives have access to this password. This password cannot be provided to customers.

13. Click **Next**.
The **Maintenance Complete** window opens.
14. Click **Finish**.

If you performed a full or partial shutdown of the MUSE system in step 2, cancel the shutdown following the procedures described in the “System Administration” chapter of the *MUSE v9 Cardiology Information System Service Manual*.

Configuring the MUSE System to Receive DICOM Tests

Configuring the MUSE system to receive DICOM tests consists of the following procedures:

- “Configuring the MUSE DICOM Storage Provider Service” on page 93
- “Configuring the Inbound DICOM Device(s) in the MUSE System” on page 94
- “Configuring the Transmitting DICOM Device(s) to Send DICOM Tests to the MUSE System” on page 95

Configuring the MUSE DICOM Storage Provider Service

The **MUSE DICOM Storage Provider** service is a DICOM Storage Service Class Provider and receives inbound DICOM tests from DICOM Storage Service Class Users. The service is configured with a default AE Title and port.

Use the following steps to configure the **MUSE DICOM Storage Provider** service.

1. Log on to the MUSE application.
2. Go to **System > Setup**.
3. Select **DICOM Services**.
4. Right-click on **DICOM STORE SCP** and select **Properties**.
5. Select **General** and complete the following fields as appropriate:

Field	Description	Action
IP Address	The name or IP address of the MUSE application server. The default is localhost .	You should not need to change this.
AE Title	The DICOM Application Entity Title of the MUSE Storage Service Class Provider. The default is MuseStoreSCP .	Type a new title if needed.
Port	The port that the MUSE Storage Provider service will listen on. The default port is 104.	Type a new port value if needed.
Enable Storage Commitment	If this box is checked, the MUSE system will provide storage commitment responses.	Check this box as needed. The MUSE Storage Provider service listens for storage commitment messages on the same IP address and port as DICOM tests.

Field	Description	Action
Retry Interval for sending N-Report (in seconds)	The time between attempts to send a Storage Commitment status to the DICOM Storage Service Class User. The default is 60.	Change this value if needed.
Maximum wait time before failure	The maximum time the MUSE Storage Provider service should wait for a Storage Commitment response. The default is 180.	Change this value if needed.

6. Select **DICOM Association Settings** to configure these settings.
Default values exist for these settings and typically do not need to be changed.
7. Click **OK** to save your changes.
To ignore your changes, click **Close**.

If any changes were made, the **MUSE DICOM Storage Provider** service will need to be restarted on the system application server.

Configuring the Inbound DICOM Device(s) in the MUSE System

Each inbound DICOM Storage Service Class User Device needs to be configured in the MUSE system prior to the device being able to associate with and send DICOM tests to it.

Use the following steps to configure an inbound DICOM Device in the MUSE system. Repeat these steps for each inbound DICOM Device that needs to send tests to the MUSE system.

1. Log on to the MUSE application.
2. Go to **System > Setup**.
3. Select **DICOM Devices**.
4. Perform one of the following steps:
 - a. To create a new device, go to **Action > New**.
 - b. To modify an existing device, right-click on the entry for the device and select **Properties**.
5. Select **General** and complete the following fields as appropriate.

Field	Description	Actions
AE Title	The DICOM Application Entity Title of the MUSE Storage Service Class User device.	Type the AE Title of the DICOM Device that sends tests to the MUSE system.
IP Address	The name or IP address of the DICOM device.	Type the IP address of the DICOM Device that sends tests to the MUSE system.
Description	This field can be used to describe the device.	Type a description of the device into this field.

Field	Description	Actions
Storage Commitment	If storage commitment is enabled, the MUSE system sends storage commitment responses to the DICOM device storage commitment service using information configured here.	If the DICOM device supports storage commitment, select this box to enable it.
AE Title	The DICOM Application Entity Title of the storage commitment service on the DICOM device.	Type the AE Title of the storage commitment service on the DICOM Device.
IP Address	The IP Address of the storage commitment service on the DICOM device.	Type the IP Address of the storage commitment service on the DICOM Device.
Port	The port number of the storage commitment service on the DICOM device.	Type the port number of the storage commitment service on the DICOM Device.

- Click **OK** to save your change.
To ignore your changes, click **Close**.

Configuring the Transmitting DICOM Device(s) to Send DICOM Tests to the MUSE System

To send DICOM tests to the MUSE system, configure the DICOM Storage Service Class User Device to use the MUSE DICOM Storage Service Class Provider AE Title, IP Address, and Port as defined in the DICOM STORE SCP entry in DICOM Services in **MUSE Setup**.

Use this same information for storage commitment, if that option is enabled for the MUSE Storage Provider service.

Configuring the System to Send DICOM Tests

Configuring the system to send DICOM tests consists of the following procedures:

- “Configuring the DICOM Storage User Service” on page 95
- “Configuring the Outbound DICOM Device(s) in the System” on page 96
- “Configuring the Receiving DICOM Device(s) to Receive DICOM Tests from the System” on page 98

Configuring the DICOM Storage User Service

The DICOM Storage Service Class User service sends outbound DICOM tests to DICOM Storage Service Class Providers. The service is configured with a default AE title and storage commitment port.

Use the following steps to configure the DICOM Storage User service.

- Log in to the system application.
- Go to **System>Setup**.

3. Select **DICOM Services**.
4. Right-click on **DICOM STORE SCU** and select **Properties**.
5. Select **General**.

Complete the following fields as appropriate:

Field	Description	Action
AE Title	The DICOM Application Entity Title of the System Storage Service Class User. The default is MuseStoreSCU .	If required, change the default by typing a new title.
Storage commitment port (for receiving responses)	The port that the System Storage User service listens on for storage commitment responses. The default port is 105.	If required, change the default by typing a new port.
Maximum Wait Time	The maximum time in seconds that the system waits for storage commitment responses. Default is 60.	If required, change the default by typing a new wait time.
Maximum retries	The maximum number of storage commitment requests that the system makes if previous requests fail. Default is 3.	If required, change the default by typing a new maximum number of retries.

6. Select **DICOM Association Settings** to configure these settings.
Default values exist for these settings and typically do not need to be changed.
7. Click **OK** to save your changes.
Click **Close** or **Cancel** to ignore your changes.
If any changes were made, the **MUSE DICOM Storage User** service will need to be restarted on the system application server.

Configuring the Outbound DICOM Device(s) in the System

Each outbound DICOM device needs to be configured in the system prior to sending a test from the system to the outbound DICOM device.

Use the following steps to configure an outbound DICOM device in the system. Repeat these steps for each outbound DICOM device that needs to be configured.

1. Log in to the system application.
2. Go to **System>Setup**.
3. Select **Devices**.

4. Perform one of the following:
 - To create a new device, go to **Action>New** and select one of the following device types.
 - **DICOM IOD**
DICOM Information Object Definition. Only ECG test types may be sent to DICOM IOD devices.
 - **DICOM PDF**
DICOM Encapsulated PDF

The device types are based on the compatibility or preference of the receiving DICOM storage service class provider.
 - To modify an existing DICOM device, right-click the entry and select **Properties**.
5. Select **General** and set up the following fields as appropriate:

Field	Description	Action
Device Name	The name of the system device.	Type the name of the device.
Device AE Title	The DICOM Application Entity Title of the receiving DICOM storage service class provider. This is the DICOM storage service class provider that receives tests from the system.	Type the AE Title of the DICOM storage service class provider.
IP Address	The IP address of the receiving DICOM storage service class provider. This is the DICOM storage service class provider that receives tests from the system.	Type the IP address.
Port	The port number of the receiving DICOM storage service class provider. This is the DICOM storage service class provider that receives tests from the system.	Type the port number.
Send Original IOD if available	<p>Flag that determines whether the original unedited data or the edited test is exported.</p> <p>If this option is enabled, the original, initially acquired data is exported.</p> <p>NOTE: This option is only available for DICOM IOD device types.</p>	<p>Check the box to enable this option.</p> <p>Uncheck the box to disable the option.</p>

Field	Description	Action
Supports Storage Commitment	A flag that enables/disables storage commitment on the MUSE system. If the DICOM storage service class provider supports storage commitment, this box can be checked to enable it. When storage commitment is enabled, the system sends storage commitment requests to the DICOM device storage commitment service using information configured here.	Check the box to enable this option. Uncheck the box to disable the option.
Storage Commitment AE Title	The DICOM Application Entity Title of the storage commitment service on the DICOM device.	Type the AE Title of the storage commitment service on the DICOM device.
Storage Commitment IP Address	The IP address of the storage commitment service on the DICOM device.	Type the IP address of the storage commitment service on the DICOM device.
Storage Commitment Port	The port number of the storage commitment service on the DICOM device.	Type the port number of the storage commitment service on the DICOM device.

6. After entering the device AE title, IP address, and port, click **DICOM Echo** to verify an association can be made with the DICOM storage service class provider.

If an association can be established, the following message is displayed: **DICOM ECHO Successful**

If an association cannot be established, the following message is displayed: **DICOM ECHO Failed**. If a failure occurs, check the settings and try again.

7. Select **Hours of Operation** and configure them as desired.
8. Select **Advanced** and configure **Valid Sites** as desired.
9. Click **OK** to save your changes.
Click **Close** or **Cancel** to ignore your changes.

Configuring the Receiving DICOM Device(s) to Receive DICOM Tests from the System

To receive DICOM tests from the system, the receiving DICOM storage service class provider might need to be configured with the DICOM storage service class user AE title and IP address defined in the DICOM STORE SCU entry in DICOM Services in the system setup. If storage commitment is used, specify the MUSE STORE SCU storage commitment port on the receiving DICOM storage service class provider.

Configuring the System to Query for DICOM Orders

Use the following procedures to configure the system to query for DICOM orders.

1. Configure the system DICOM modality worklist client service.
2. Configure the DICOM modality worklist service class provider to receive DICOM order queries from the system.

Configure the System DICOM Modality Worklist Client Service

The system DICOM modality worklist client service queries a DICOM modality worklist service class provider for DICOM orders.

Perform the following to configure the system DICOM modality worklist client service to query for DICOM orders. Repeat these steps for each system site that needs to query for DICOM orders.

1. Log on to the system application.
2. Go to **System > Setup**.
3. Select **DICOM Services**.
4. Perform one of the following steps:
 - a. To create a new DICOM MWL SCU service, go to **Action > New > MWL Server**.
 - b. To modify an existing DICOM MWL SCU service, right-click on the entry and select **Properties**.
5. Select **MWL Config** and set up the following fields as appropriate:

Modality Worklist User Service

Field	Description	Action
AE Title	The DICOM Application Entity Title of the system modality worklist service class user.	Type the AE Title.
Default Site	The system site number.	Orders received via DMWL with a value in the DICOM Institution Name (0008,0080) that matches a configured MUSE Site name are stored under that site. If the DICOM Institution Name is either blank, or does not match a configured MUSE Site name, the Order is stored in this Default Site .
Query Default Site Only	Checkbox to enable	If enabled, queries will be made for only orders that have a DICOM Institution Name that matched the name of the Default MUSE Site.

Modality Worklist Provider Configuration

Field	Description	Action
AE Title	The DICOM Application Entity Title of the DICOM modality worklist service class provider that is to query for orders.	Type the AE Title.
IP Address	The IP Address of the DICOM Modality Worklist Service Class Provider that the system is to query for orders.	Type the IP address of the DICOM Modality Worklist Service Class Provider.
Port	The Port of the DICOM Modality Worklist Service Class Provider that the system is to query for orders.	Type the Port of the DICOM Modality Worklist Service Class Provider.

Default Query

Field	Description	Action
Query Interval (In Minutes)	The frequency the system queries for orders.	Type a number in minutes to specify the frequency.
Days in the Future	The number of days in the future (from current time) to query for Scheduled Procedure Start Date/Time. The default is five.	Enter the number of days in the future (from current time) to query for Scheduled Procedure Start Date/Time.
Days in the Past	The number of days in the past (from current time) to query for Scheduled Procedure Start Date/Time. The default is five.	Enter the number of days in the past (from current time) to query for Scheduled Procedure Start Date/Time

Location Parsing

Field	Description	Action
Location Parsing Field	One of two fields from the Orders received through DMWL can be used to match a configured MUSE HIS Location Full Name . The matched Orders will be stored under that location. The two fields are: <ul style="list-style-type: none"> Scheduled Station AE Title Current Patient Location 	Select the field from the Orders received through DMWL that should be used to match a configured MUSE HIS Location Full Name . The matched Orders will be stored under that location.
Current Patient Location Separator	When parsing Location from the Current Patient Location Field, the Separator to be used for parsing multi-segment Current_Patient_Location strings.	When parsing Location from the Current Patient Location field, orders received through DMWL with a value in the DICOM Current Patient Location (0038,0300) that match a configured MUSE HIS Location Full Name , the order is stored under that location.
Current Patient Location Location Section	When parsing Location from the Current Patient Location Field, the Segment to be used for parsing multi-segment Current_Patient_Location strings.	<p>If both a Location Separator and Location Segment# are configured, the Current Patient Location is parsed prior to matching the MUSE HIS Location Full Name. For example, if the Current Patient Location value contains the string 'General Hospital-Cardiac ICU-204-1' and the Location Separator is configured as '-' and the Location Segment is configured as '2', the parsed result of 'Cardiac ICU' is used for matching to the MUSE HIS Location Full Name.</p> <p>If a match is not made to a MUSE HIS Location Full Name, the order is not associated with any MUSE Location.</p> <p>The Room Section and Bed Section fields are similarly used for parsing out the room number and bed number from the Current Patient Location value. In the above example, the room number would be parsed as "204" and the bed number would be parsed as "1".</p>

- After entering the **Device AE Title**, **IP Address**, and **Port** for the Modality Worklist Provider Configuration, click **DICOM Echo** to verify an association can be made with the DICOM device.

If an association can be established, the following message is displayed: **DICOM ECHO Successful**

If an association cannot be established, the following message is displayed: **DICOM ECHO Failed**. If a failure occurs, check the settings and try again.

- Select **DICOM Association Settings** to configure these settings.
Default values exist for these settings and typically do not need to be changed.

8. Click **OK** to save your changes.
Click **Close** or **Cancel** to ignore your changes.
9. Restart the **MUSE DICOM Gateway DICOM Modality Worklist Client** service on the system application server.

Configure the DICOM Modality Worklist Service Class Provider to receive DICOM Order Queries from the System

To receive DICOM modality worklist queries from the system, the DICOM modality worklist service class provider might need to be configured with the system modality worklist service class user AE Title defined in the DICOM MWL SCU entry in DICOM services in the system setup.

System Checkout

Receiving DICOM Tests into the MUSE System

1. From the DICOM Storage Service Class User device, send a DICOM ECG test to the MUSE system.
2. On the MUSE system, verify the test is visible in the **MUSE Edit List**.

Sending DICOM Tests from the MUSE System

1. From the MUSE system, print an ECG to a DICOM IOD or PDF device.
2. On the DICOM device, verify the test is transmitted successfully.

Querying for DICOM Orders

In the MUSE system, verify orders from the DICOM Modality Worklist Service Class Provider are visible.

Troubleshooting

Use the following troubleshooting table to help with issues encountered with DICOM Communication.

Symptom	Condition	Action
Unable to send tests from a DICOM device to the MUSE system.	The sending DICOM device has not been defined as a DICOM Device in the MUSE system.	Confirm that the DICOM device has been defined in the MUSE system. Each DICOM device that sends DICOM tests to the MUSE system must be defined in MUSE Setup>DICOM Devices with a valid configuration.
	The MUSE DICOM Storage Provider service is not started.	Start the MUSE DICOM Storage Provider service.

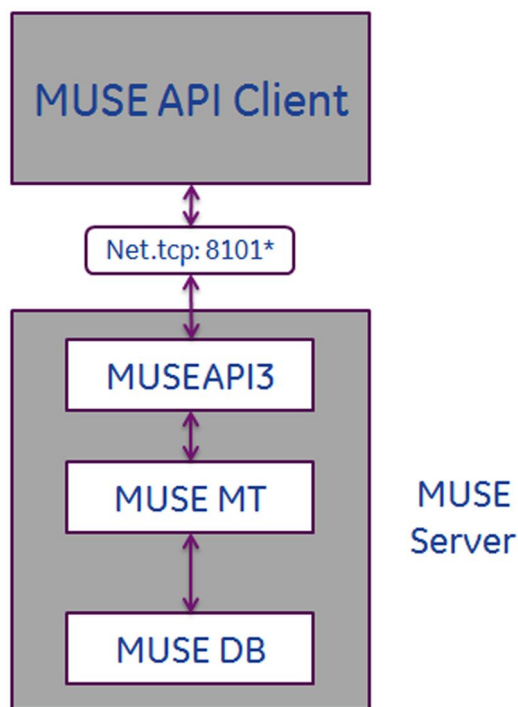
Symptom	Condition	Action
Unable to send tests from the MUSE system to a DICOM Device.	The test is a non-ECG test.	Only ECG tests can be sent to a DICOM IOD device. ECG and non-ECG tests may be sent to a DICOM PDF device.
	The MUSE DICOM Storage User service is not started.	Start the MUSE DICOM Storage User service.
Unable to receive DICOM MWL orders in the MUSE system.	The MUSE DICOM Modality Worklist Client service is not started.	Start the MUSE DICOM Modality Worklist Client service.

MUSEAPI3 Installation

This chapter describes how to install MUSEAPI3 on MUSE v9 servers. MUSE v9.0 ships with MUSE API v3.1. For the purposes of this documentation, all references to MUSEAPI3 refer to MUSE API v3.1.

Theory of Operation

MUSEAPI3 resides on the MUSE v9 server and allows MUSE API clients, including CV Web v3, MUSE Web Compatibility Layer, and MACCRA Compatibility, to communicate with the MUSE system through the MUSE Middle Tier (MUSE MT Host Service).



* Default port setting shown

NOTE:

Third-party developers can use MUSEAPI3 to interface with the MUSE system. Third-party developers require a license and must design their interface following the guidelines described in the *MUSE Enterprise Integration Reference Manual*.

Pre-Installation Instructions

Complete the following pre-installation procedures before installing MUSEAPI3. Information obtained from these procedures is needed to successfully complete your MUSEAPI3 installation.

Determining Whether MUSEAPI3 is Already Installed

The MUSE system may already have MUSEAPI3 installed if you are using CV Web 3 or another MUSEAPI3 client.

Go to Windows Services on the MUSE server and determine whether the **MUSEAPI3** service is already present. If it is, then MUSEAPI3 is already installed. If MUSEAPI3 is already installed, you may run the **MUSEAPIServiceConfig.exe** application located in the MUSE installation folder to determine the communication protocol(s) that MUSEAPI3 is using.

Determining the Communication Protocol(s) that MUSEAPI3 Uses

You can configure MUSEAPI3 to communicate with MUSEAPI3 clients using http, https, or net.tcp protocols. It is possible to configure MUSEAPI3 for more than one protocol.

- HTTP – a non-secure web communication protocol.
- HTTPS – a secure web communication protocol that uses an additional encryption layer. Use of HTTPS requires that the customer configure a secure communication channel, such as SSL, and establish any public key certificates. When using HTTPS, you must obtain a thumbprint of the certificate and use it to configure the port MUSEAPI3 uses. The thumbprint is the hash of the public key.
See [“Configuring SSL Certificate for the MUSEAPI3 Port” on page 115](#) for more information.
- Net.tcp – Unless HTTPS is used, this is the preferred communication protocol for MUSEAPI3. Net.tcp uses domain security and requires that the MUSE API Client and MUSE Server(s) be on the same domain.

Determining the Port Assignments for MUSEAPI3

MUSEAPI3 uses the following default ports. If these ports are already in use, you may enter different ports during installation.

- HTTP — port 8100
- HTTPS — no default assigned (port 443 is typically used for secure websites using SSL)
- net.tcp — port 8101

Locating the MUSE Application Folder on the MUSE Server

You must install MUSEAPI3 files in the MUSE application folder. Following is a list of the default folder locations:

- 32-bit Windows Server Operating Systems: **C:\Program Files\MUSE.**
- 64-bit Windows Server Operating Systems: **C:\Program Files (x86)\MUSE.**

Installing MUSEAPI3

Perform the following steps to install MUSEAPI3 on a MUSE v9 application server.

1. Log on to the MUSE application server using an account that has **administrator** privileges on the MUSE application server.
2. Have the customer disable any antivirus software during the installation. Re-enable the antivirus software after the installation is complete.
3. Insert the MUSE v9 installation media into the optical drive of the system.
If any **Autorun** or **AutoPlay** screens appear, close or cancel them.

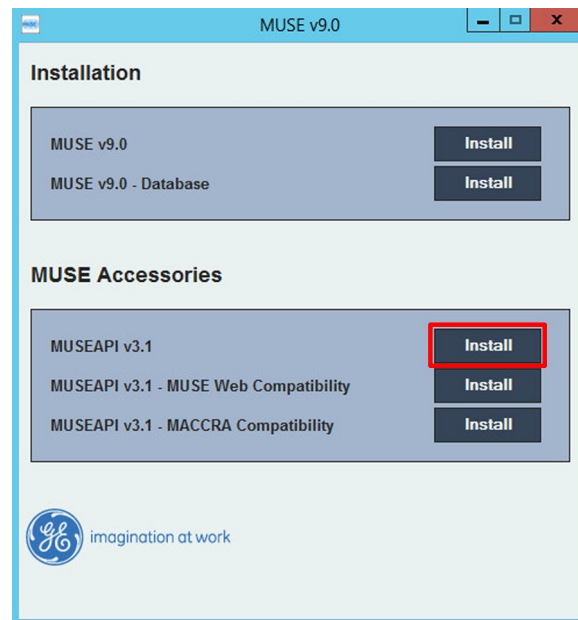
4. Browse the optical drive in Windows Explorer and perform one of the following:
 - If the MUSE v9 Application and Support DVD is inserted, navigate to the **MUSE Application** folder and execute the **Autorun.exe** application.
 - If the MUSE v9 Application ISO is being used, navigate to the root folder and execute the **Autorun.exe** application.

NOTE:

Be sure to execute **Autorun.exe** and not **Autorun.exe.config**.

The **MUSE v9.0 Installation Options** window opens.

5. Click **Install** next to **MUSEAPI v3.1**.

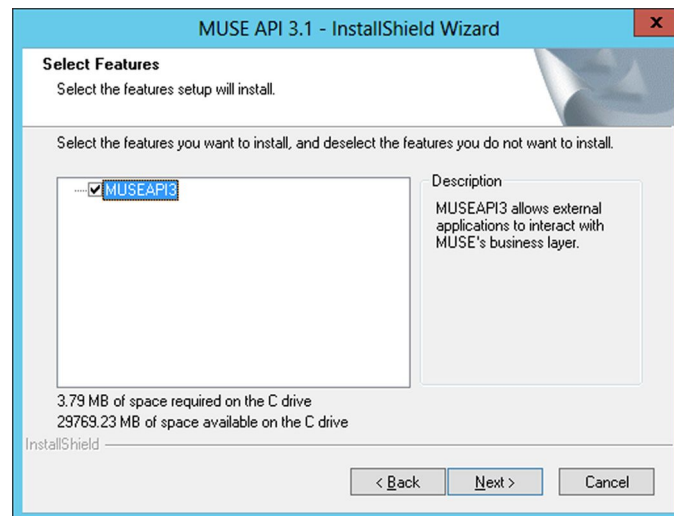


If a **User Account Control** dialog opens, choose **Yes** or **Allow**.

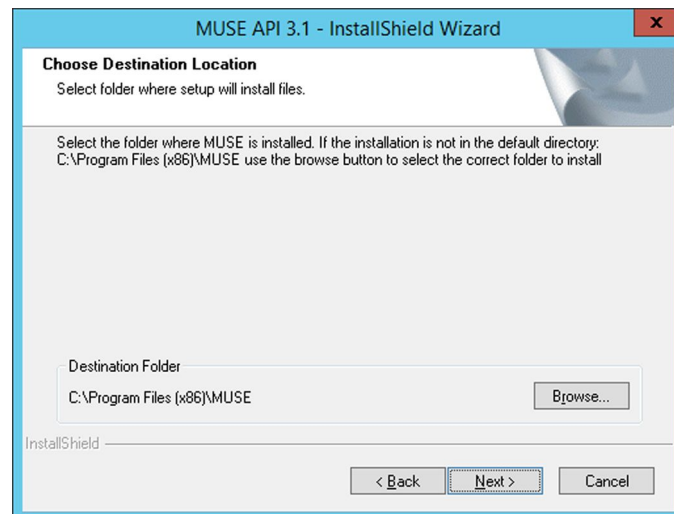
The **MUSE API 3.1- InstallShield Wizard** window opens.

6. Click **Next**.
The **License Agreement** window opens.
7. Read and accept the License Agreement.

8. Click **Next**.
The **Select Features** window opens.

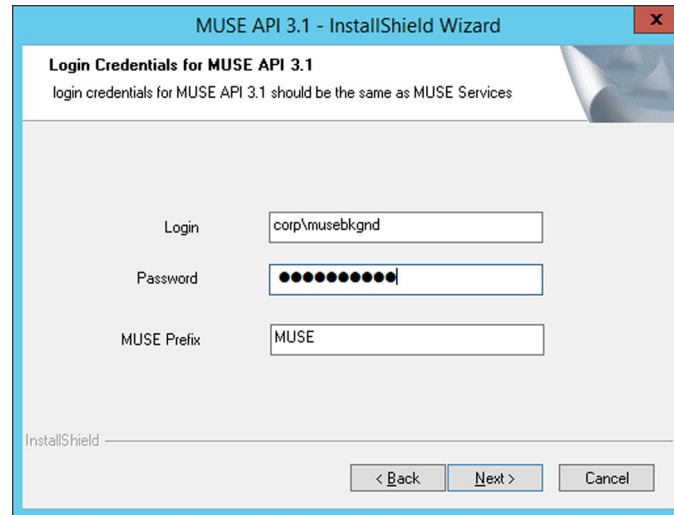


9. Ensure **MUSEAPI3** is selected and click **Next**.
The **Choose Destination Location** window opens.



10. Ensure that the destination folder for MUSEAPI3 is the same folder in which the MUSE program files are installed, then click **Next**.

The **Login Credentials for MUSE API 3.1** window opens.



11. Enter the login and password that the **MUSEAPI3** service uses to communicate with the MUSE Middle Tier.

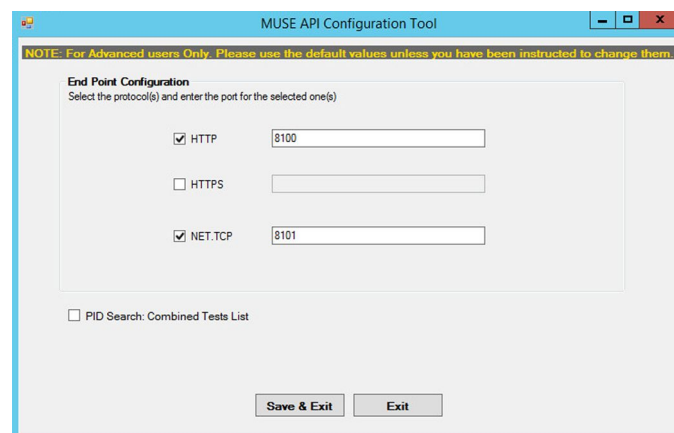
This should be the same account used for the other MUSE services (typically the domain MUSE Background user).

NOTE:

If you are unsure of the account to use for MUSE services, open Windows Services and determine the user account configured to start the other MUSE services. Enter the prefix used by the MUSE services. This is almost always **MUSE**.

12. Click **Next**.

The **MUSE API Configuration Tool** window opens.



13. In the **End Point Configuration** area of the window, select the protocol(s) you are using to communicate with MUSEAPI3 and enter the port value(s).

Note that you must have at least one protocol enabled, and you may have more than one. If any protocols are selected that you do not want, uncheck them.

You are advised to use the following values for the ports:

Protocol	Recommended Port Values
HTTP	8100
HTTPS	The port for SSL, as configured by the customer.
net.tcp	8101

NOTE:

For more information on the available communication protocols, see [“Determining the Communication Protocol\(s\) that MUSEAPI3 Uses” on page 107.](#)

14. Determine whether you want to check the box next to **PID Search: Combined Test Lists** to change the Patient Conflict behavior of the MUSEAPI3 and do one of the following:

- To enable the **PID Search: Combined Test List**, check the box. When performing a Patient ID search while this option is enabled, MUSEAPI3 automatically combines all tests for that Patient ID for the same MUSE site even if there is a Patient ID/Last Name mismatch.
- To disable the **PID Search: Combined Test List**, leave the box unchecked. When performing a Patient ID search while this option is disabled, MUSEAPI3 includes patient conflicts if there is a Patient ID/Last Name mismatch within the same site.

This setting can always be changed later.

NOTE:

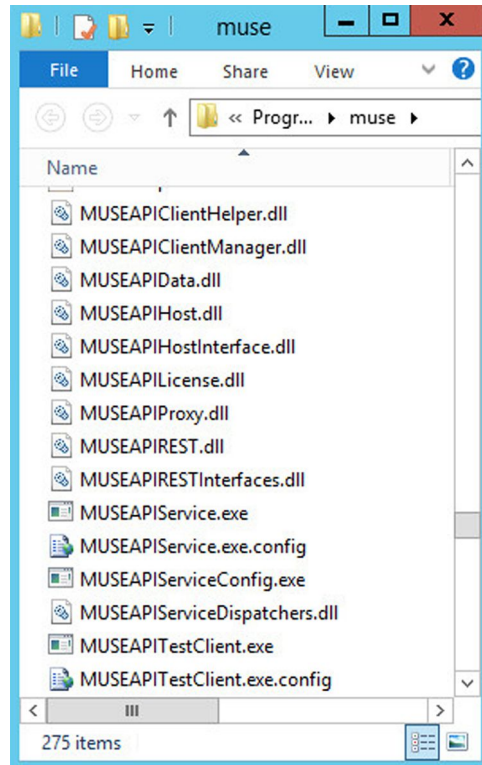
MUSE API 3.1 handles patient conflicts within the same MUSE site differently than MUSE API 3.0 did. MUSE API 3.1 only provides a response that includes patient conflicts if there is a Patient ID / Last Name mismatch, and that conflict response can be disabled by enabling this option. MUSE API 3.1 handles patient ID conflicts across different servers or at different sites the same as MUSE API 3.0 did.

15. Click **Save & Exit** to save the changes to the **End Point Configuration**.
16. Click **Finish** to end the installation of MUSEAPI3.
17. Open the install log located in **C:\MUSEAPI3_Installer_Log_xxx.log** and verify that the installation completed successfully without any errors.

A new log is created each time the installer is launched. Look at the log file with the highest number in the sequence to make sure you are looking at the most recent installation. Verify the following are installed:

- **MUSEAPI3 service**
Verify that the MUSEAPI3 service has started. If the service has not started, manually start it.
- **MUSEAPI3 program files**

Verify the MUSEAPI3 program files were added to the MUSE installation folder.



Changing the MUSEAPI3 Service Protocol Configuration

1. Run the **MUSEAPIServiceConfig.exe** application located in the MUSE installation folder.

NOTE:

To make changes to the configuration you may need to use **Run as Administrator**.

2. Review the protocol(s) that you are using to communicate with MUSEAPI3 and modify as appropriate.

If you want additional protocol(s), check the corresponding box. You can select more than one protocol.

If you do not want any of the selected protocol(s), uncheck the appropriate box(es).

You are advised to use the following values for the ports:

Protocol	Recommended Port Values
HTTP	8100
HTTPS	The port for SSL, as configured by the customer.
net.tcp	8101

NOTE:

For more information on the available communication protocols, see [“Determining the Communication Protocol\(s\) that MUSEAPI3 Uses” on page 107.](#)

3. Determine whether you want to check the box next to **PID Search: Combined Test Lists** to change the Patient Conflict behavior of the MUSEAPI3 and do one of the following:
 - To enable the **PID Search: Combined Test List**, check the box. When performing a Patient ID search while this option is enabled, MUSEAPI3 automatically combines all tests for that Patient ID for the same MUSE site even if there is a Patient ID/Last Name mismatch.
 - To disable the **PID Search: Combined Test List**, leave the box unchecked. When performing a Patient ID search while this option is disabled, MUSEAPI3 includes patient conflicts if there is a Patient ID/Last Name mismatch within the same site.

This setting can always be changed later.

NOTE:

MUSE API 3.1 handles patient conflicts within the same MUSE site differently than MUSE API 3.0 did. MUSE API 3.1 only provides a response that includes patient conflicts if there is a Patient ID / Last Name mismatch, and that conflict response can be disabled by enabling this option. MUSE API 3.1 handles patient ID conflicts across different servers or at different sites the same as MUSE API 3.0 did.

4. If any changes were made, restart the **MUSEAPI3** service.

Removing MUSEAPI3

NOTE:

If you are going to reinstall MUSEAPI3 at a later date, it is recommended that you copy the **MUSEAPIService.exe.config** file located in the MUSE installation folder and save it to a location outside of the MUSE installation folder. This file contains the current settings for MUSEAPI3 and you can use it as reference during the reinstallation or to restore the MUSEAPI3 settings to their original values. Uninstalling MUSEAPI3 removes the MUSEAPI3 service and MUSEAPI files from the MUSE installation folder.

1. Log on to the MUSE application server as an administrator user.
2. Stop the **MUSEAPI3** service.
3. Go to Windows **Control Panel>Programs and Features**.

4. Right-click on **MUSE API 3.1** and select **Uninstall**.
The **MUSE API 3.1 - InstallShield Wizard** window opens.
5. Ensure **Remove** is selected and click **Next**.
6. Click **Yes** when you receive the following prompt: **Do you want to completely remove the selected application and all its features?**
7. When the **Uninstall Complete** window opens, click **Finish**.

Restoring the MUSEAPI3 Configuration

If you saved the MUSEAPI3 configuration file **MUSEAPIService.exe.config** as part of the uninstallation process, you can reinstall it and use it to restore the MUSEAPI3 settings.

1. Copy the file **MUSEAPIService.exe.config** from the saved location to the MUSE installation folder.
2. Restart the **MUSEAPI3** service.

MUSE API Test Client

The MUSE API Test Client is installed with MUSEAPI3 and can be used to test and troubleshoot MUSEAPI3.

Running the MUSE API Test Client

To run the MUSE API Test Client, execute **MUSEAPITestClient.exe** from the MUSE installation folder (default is **C:\Program Files (x86)\MUSE**).

Using the MUSE API Test Client

The following steps provide a high-level example of how to use the MUSE API Test Client. This procedure can also be used as a system checkout to verify MUSEAPI3 is installed correctly.

1. Run the MUSE API Test Client.
The **MainWindow** screen opens.
2. Use the following table to complete the configuration of the MUSE API Test client.

NOTE:

This configuration will need to be repeated each time the test client is used unless the settings are manually entered in the **MUSEAPITestClient.exe.config** file.

Item	Description
MUSE Username	The username of a MUSE user whose role includes all privileges in the MUSE system. The default is museadmin .
Password	The password of the MUSE user defined above. The default is maclink .

Item	Description
License Key	The license key to access MUSEAPI3. A unique key is provided to MUSEAPI3 licensees. GE Healthcare Service has their own license key that they can use here. NOTE: GE Healthcare Service must not permanently save the license key in the config file.
Site Number	The MUSE Site Number . The default is 1.
Base URI	The Endpoint URI for MUSEAPI3. The default is http://localhost:8100/ .

3. Click **Login**.
4. Select the **Patient** tab.
5. Select **PatientRetrieve.GetTestPatientsByPatientId**.
6. Enter the **Patient Id** of a patient in the MUSE database and click **OK**.
7. Verify the patient is found.
8. Click **Logout**.
9. Close the MUSE API Test Client application.

Configuring SSL Certificate for the MUSEAPI3 Port

This section provides the steps to obtain the thumbprint of the new certificate and use it to configure the port.

NOTE:

Prior to completing these steps, the customer must obtain a certificate from a Certificate Authority and have it installed on the MUSE application server.

1. To get the thumbprint of your certificate, you need the MMC dialog box open and configured to deal with Certificates:
 - a. Run Microsoft Management Console (**mmc.exe**).
 - b. When the Microsoft Management Console (MMC) opens, press **Ctrl+M** to add a snap-in.
 - c. In the **Add or Remove Snap-ins** dialog box, do the following:
 - i. In the **Available snap-ins** list, select **Certificates**.
 - ii. Click **Add**.
 - d. In the **Certificates snap-in** dialog box do the following:
 - i. Select **Computer account**.
 - ii. Click **Next**.
 - e. Select **Local computer** and click **Finish**.
 - f. To close the **Add or Remove Snap-ins** dialog box, click **OK**.
2. Expand the **Certificates** node in the left panel.

3. Expand the **Personal** node in the left panel and click the **Certificates** node.
The certificate that the customer obtained and installed is listed here.
4. Double-click on the certificate the customer obtained and installed to open it.
5. Select the **Details** tab.
6. In the list box, click **Thumbprint**.
The bottom window lists the hex values.
7. Select and copy the list of hex values from 6 into a text editor such as Notepad.
8. Remove all the spaces between the values to make one long string.
When you are done, it will look similar to the following:
a237052b1a2d52f72c576c5702136802a7bf8804
This is your certificate thumbprint.
9. Use **Run as Administrator** to obtain a command-prompt, then run the following two commands:

```
netsh http add sslcert iport=0.0.0.0:(port
assigned for MUSEAPI3 HTTPS protocol
goes here) certhash=[your thumbprint]
appid={3df9aba0-cbd8-4dbe-b3c7-daf47b8a015b}

netsh http add sslcert iport=[:]:(port
assigned for MUSEAPI3 HTTPS protocol
goes here) certhash=[your thumbprint]
appid={3df9aba0-cbd8-4dbe-b3c7-daf47b8a015b}
```
10. Run the following command to show the SSL Certificate bindings and verify that the IP:port, Certificate Hash, and Application ID match those entered in step 9:
netsh http show sslcert

NOTE:

IF the SSL Certificate bindings were entered incorrectly, the SSL Certificate bindings must be deleted and recreated using the following commands:

```
netsh http delete sslcert iport=0.0.0.0:(port assigned for MUSEAPI3 HTTPS
protocol)
```

```
netsh http delete sslcert iport=[:]:(port assigned for MUSEAPI3 HTTPS
protocol)
```

After deleting the bindings they can be re-created using the information in step 9.

10

MUSE Web Compatibility Layer

With the MUSE v9 system, MUSE Web is no longer a component of the MUSE system installation. MUSE Web has been replaced by the MUSE Web Compatibility Layer, which is a separate installation and uses MUSEAPI3 with the MUSE v9 system. This chapter provides information about the installation, configuration, and maintenance of the MUSE Web Compatibility Layer on a MUSE v9 server.

Theory of Operation

The MUSE Web Compatibility Layer provides a web interface to the MUSE patient database. This interface allows you to search for tests and view them as PDFs in a web browser. The MUSE Web Compatibility Layer uses MUSEAPI3 to communicate with the MUSE Middle Tier, which in turn communicates with the MUSE database.



The MUSE Web Compatibility Layer

System Requirements

Verify that MUSEAPI3 is installed. The MUSE Web Compatibility Layer requires MUSEAPI3 to function. Refer to [Chapter 9 "MUSEAPI3 Installation" on page 105](#) for information on installing MUSEAPI3.

Verify or install the necessary Windows Internet Information Services (IIS) components on the MUSE application server. The following table and instructions provide information on how to verify Windows IIS components.

Required Internet Information Services (IIS) for the MUSE Web Compatibility Layer

The following Internet Information Services (IIS) components are required for the MUSE Web Compatibility Layer. The following table identifies the Internet Information Services (IIS) components that are required by each supported operating system.

NOTE:

These are the minimum Roles, Role Services, and Features required. If additional Roles, Role Services, and Features are installed, it should not have any impact on the MUSE Web Compatibility Layer functionality.

Required Components

Windows Feature / Role / Role Service	Windows Server 2008	Windows Server 2008 R2	Windows Server 2012 / 2012 R2
Role			
<i>Web Server (IIS) Role</i>			
Web Server (IIS)	X	X	X
Web Server (IIS) Role Services			
<i>Application Development</i>			
ASP.NET	X	X	
.NET Extensibility	X	X	
ASP.NET 4.5			X
.NET Extensibility 4.5			X
ISAPI Extensions	X	X	X
ISAPI Filters	X	X	X
<i>Common HTTP Features</i>			
Static Content	X	X	X
Default Document	X	X	X
Directory Browsing	X	X	X
HTTP Errors	X	X	X
<i>Health and Diagnostics</i>			
HTTP Logging	X	X	X
Request Monitor	X	X	X
<i>Security</i>			
Basic Authentication	X	X	X
Windows Authentication	X	X	X
Request Filtering	X	X	X

Required Components (cont'd.)

Windows Feature / Role / Role Service	Windows Server 2008	Windows Server 2008 R2	Windows Server 2012 / 2012 R2
<i>Management Tools</i>			
IIS Management Console	X	X	X
Feature			
<i>Windows Process Activation Service</i>			
Process Model	X		
.NET Environment	X		
Configuration APIs	X		
<i>.NET Framework 4.5 Features</i>			
ASP .NET 4.5			X

Perform the following procedure to automatically install the required Windows features, roles, and role services.

Completing this procedure automatically installs all required components for the MUSE Web Compatibility Layer, with the exception of any components that are already installed. Components that are already installed are ignored.

1. Insert the MUSE v9 installation media into the optical drive of the system.
If any **Autorun** or **AutoPlay** screens appear, close or cancel them.
2. Browse the optical drive in Windows Explorer and perform one of the following:
 - If the MUSE v9 Application and Support DVD is inserted, navigate to the **\MUSE Support\Pre Install Scripts** folder.
 - If the MUSE v9 Support ISO is being used, navigate to the **\Pre Install Scripts** folder.
3. Right-click on **Install_IIS.cmd** and choose **Run as administrator**.
The batch file runs and installs any required components.
4. Using **Windows Server Manager**, verify that the Windows components listed in the previous table were installed as appropriate for the Windows operating system you are using. The [“Manually Installing and Verifying IIS Related Roles, Role Services, and Features”](#) section on [page 134](#) can be used to manually install or verify the appropriate Windows components.

Installing the MUSE Web Compatibility Layer

Use the following instructions to install the MUSE Web Compatibility Layer on the MUSE application server.

Installing the MUSE Web Compatibility Layer requires that you complete the following tasks:

- “Creating a MUSE User for the MUSE Web Compatibility Layer Website” on page 120
- “Installing and Configuring the MUSE Web Compatibility Layer” on page 121
- “Adding Users to the MUSEWebCompatibilityLayer Website” on page 124

NOTE:

When using Internet Information Services (IIS) anonymous authentication with a MUSE Web Compatibility Layer website, only specific RetrieveTestList, GeneratePatientList, and RetrieveTestByDateTime URLs can be used. Refer to the *MUSE Enterprise Integration Reference Manual* for supporting information for these URLs.

Creating a MUSE User for the MUSE Web Compatibility Layer Website

The MUSE v9 system includes patient access logging. All use of the MUSE Web Compatibility Layer website using **IIS Basic Authentication** or **IIS Windows Authentication** is logged in the MUSE audit logs as the MUSE user that logs into the MUSE Web Compatibility Layer website, however if **IIS Anonymous Authentication** is used with MUSE Web Compatibility Layer, all use of the MUSE Web Compatibility Layer website will be logged as the user configured for the MUSE Web Compatibility Layer website when it was installed.

It is recommended that you create and use a new MUSE user for each MUSE Web Compatibility Layer website configured with **IIS Anonymous Authentication** to allow for MUSE patient access logging details to reflect this specific MUSE user. If **IIS Anonymous Authentication** will not be used with MUSE Web Compatibility Layer, this step is optional and the existing MuseBkgnd user may be used when installing MUSE Web Compatibility Layer.

Perform the following steps to create a new MUSE user:

1. From within the MUSE application, go to **Setup**.
2. Select **Users**.
The list of users is displayed.
3. Select **Action>New**.
4. Select the **General** page and complete the fields as indicated in the following table:

NOTE:

You may accept the default value for all fields, with the exception of those specified in the following table.

MUSE User Creation – General Page Field Requirements

Field	Action
Last Name	Enter a last name for the MUSE web user, for example, AnonymousMUSEWeb.
First Name	Enter a first name for the MUSE web user, for example, AnonymousMUSEWeb.

MUSE User Creation – General Page Field Requirements (cont'd.)

Field	Action
MUSE User name	Enter a MUSE User Name for the MUSE web user, for example, AnonymousMUSEWeb.
MUSE Password	Enter a password for the Anonymous MUSE web user. Make a note of this password as it will be needed later when installing and configuring the MUSE Web Compatibility Layer.
Re-enter MUSE Password	Re-enter the password you entered in the MUSE Password field. The password you enter here and the password entered in the MUSE Password field must be identical.
Active Sites	Put a check in the box next to each site to which this user needs access.

- Select the **Advanced** page and complete the fields in the following table.

NOTE:

You may accept the default value for all fields, with the exception of those specified in the following table:

MUSE User Creation – Advanced Page Field Requirements

Field	Action
User ID	Enter a user ID. This ID must be unique and may not be used by any other MUSE users.
Role	Set this to All Privileges .
Job Titles	Clear all boxes in the list.
Display User in Personnel Lists	Clear this box.

- Click **OK**.

Installing and Configuring the MUSE Web Compatibility Layer

- Log on to the MUSE application server using an account that has **administrator** privileges on the MUSE application server.
- Have the customer disable any antivirus software before beginning the installation. Re-enable the antivirus software after the installation is complete.
- Insert the MUSE v9 installation media into the optical drive of the system.
If any **Autorun** or **AutoPlay** screens appear, close or cancel them.

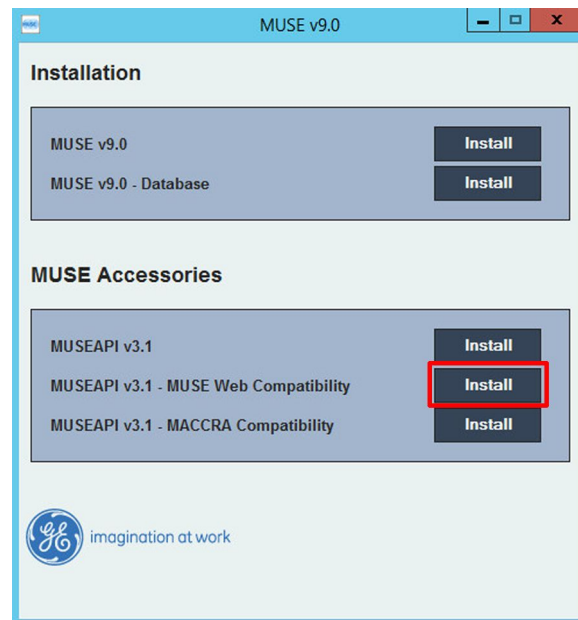
4. Browse the optical drive in Windows Explorer and perform one of the following:
 - If the MUSE v9 Application and Support DVD is inserted, navigate to the **MUSE Application** folder and execute the **Autorun.exe** application.
 - If the MUSE v9 Application ISO is being used, navigate to the root folder and execute the **Autorun.exe** application.

NOTE:

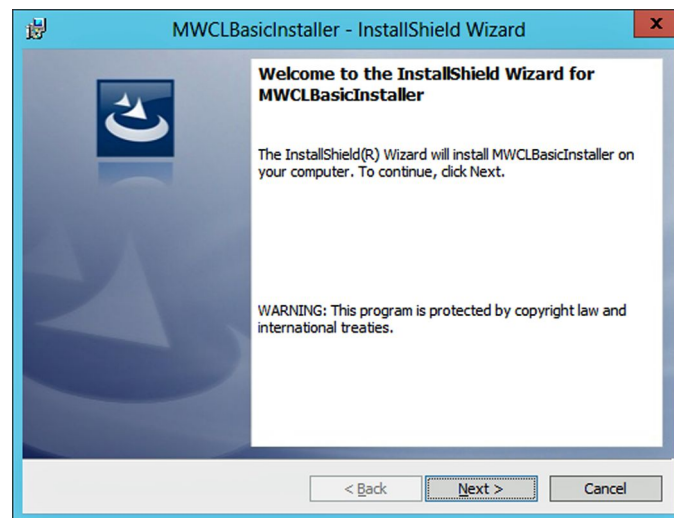
Be sure to execute **Autorun.exe** and not **Autorun.exe.config**.

The **MUSE v9.0 Installation** options window opens.

5. Click **Install** next to **MUSEAPI v3.1 – MUSE Web Compatibility**.



The **MWCLBasicInstaller** welcome screen opens.



6. Click **Next**.

The **Ready to Install MUSEWebCompatibilityLayer** window opens.

7. Click **Install**.

The **Configure MUSE Web Compatibility Layer** window opens.

8. Enter the appropriate values in the **Configuration** screen as described in the following table.

Field Descriptions for the Configure MUSE Web Compatibility Window

Field	Description
Port	The port number the MUSE Web Compatibility website uses. The default is port 88.
Language	The language you want the website to display.
MUSE User	A MUSE user (not Windows user) who is assigned all MUSE privileges and has access to all MUSE sites. If IIS Anonymous Authentication will be used for the MUSE Web Compatibility Layer website, it is recommended that a new MUSE user be created. Refer to “Creating a MUSE User for the MUSE Web Compatibility Layer Website” on page 120 for details. If IIS Anonymous Authentication will not be used for the MUSE Web Compatibility Layer website, you may use the MuseBkgnd user that already exists in MUSE.
Password	The password for the MUSE User .
MUSEAPI3 Web Service End Point	The Uniform Resource Identifier (URI) to the MUSEAPI3 installed on the server. This field is pre-populated with a drop-down list that includes the current MUSEAPI3 endpoint configurations. The default recommendation is net.tcp .

9. Click **Next** when complete.
10. When the **InstallShield Wizard Completed** window opens, click **Finish**.

11. Review the log file.

Log files are located in **C:\MWCLMergeMod3_Installer_Log_xxx.log** where xxx is a sequential number. Review the file with the highest number in the sequence to make sure you are looking at the most recent installation, and verify that the installation completed without errors.

The installation creates the following:

- **MuseWebCompatibilityLayer** website
- **MuseWebCompatibilityLayer** folder in **c:\inetpub\wwwroot**
- **MuseWebCompatibilityLayerPool** in **Application Pools**
- **MUSE Web Users** local Windows group if one does not already exist

12. If users must be set up for the **MUSE Web Compatibility Layer** website, see [“Adding Users to the MUSEWebCompatibilityLayer Website” on page 124.](#)

Adding Users to the MUSEWebCompatibilityLayer Website

Installation of the **MUSE Web Compatibility Layer** creates a **MUSE Web Users** group on the MUSE application server. By default this group has permissions to the **MuseWebCompatibilityLayer** website.

Use the following instructions to add a user to the MUSE Web Users group and thus, by default, gain access to the **MuseWebCompatibilityLayer** website.

1. Create a MUSE account for the user.
 - Be sure to include the user’s Windows user name in the MUSE account. The Windows user name is in **domain\username** format.
 - Ensure the user has **View Only** role or equivalent privileges in MUSE.

Refer to the *MUSE v9 Cardiology Information System Operator Manual* for instructions on how to set up MUSE users.

2. Add the user to the **MUSE Web Users** group on the MUSE application server.

System Checkout

After installing the web server and adding users, use the following instructions to verify that the installation was successful.

1. Log on to a MUSE workstation.
2. Open **Internet Explorer**.
3. Type **http://<servername>/** in the address field.

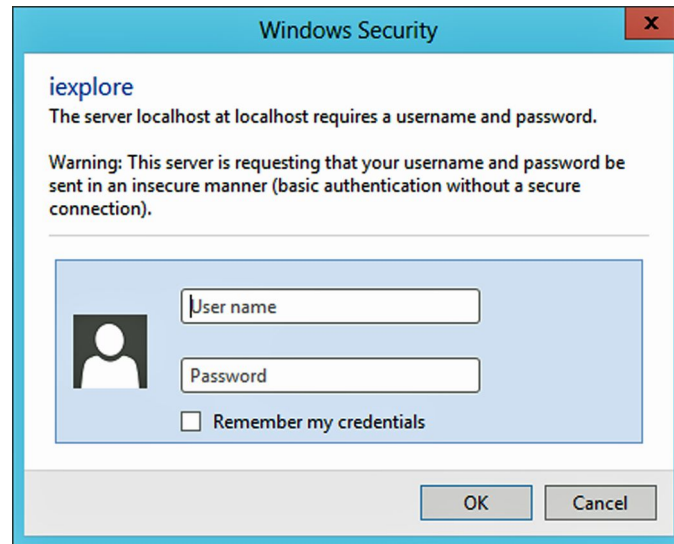
For example, if the server name is MUSEAppServer, you would enter **http://MUSEAppServer/** in the address field.

NOTE:

If MUSE Web Compatibility Layer is not using the port 80, you need to include the port number in the URL.

For example, if you are using port 81, you enter: **http://MUSEAppServer:81.**

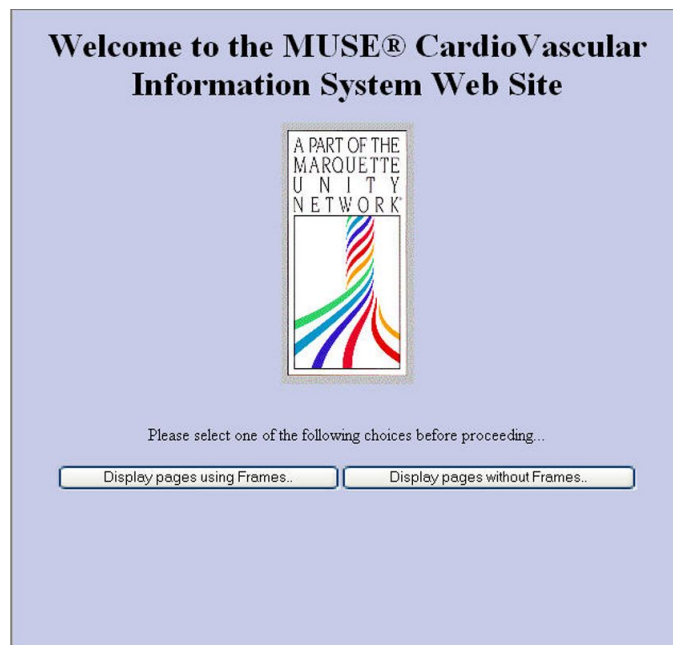
4. Press **Enter**.
A credentials dialog box opens.

**NOTE:**

If this window does not open, there was a problem with the installation, the server configuration, or the IIS services. Refer to ["Troubleshooting" on page 129](#) for more information.

5. Enter the **User name** and **Password** of a MUSE user who is set up in the **MUSE Web User** group and click **OK**.

The **MUSE Web** home page opens.



NOTE:

If this page does not open, verify that the user you entered is a member of the **MUSE Web User** group and that you entered the correct password.

6. Click either **Display pages with Frames** or **Display pages without Frames**.

If the following window opens, the installation is complete.

Enter Patient ID or Patient Name, then Click the "Submit Query" Button

Patient ID:

Patient Last Name:

Patient First Name:

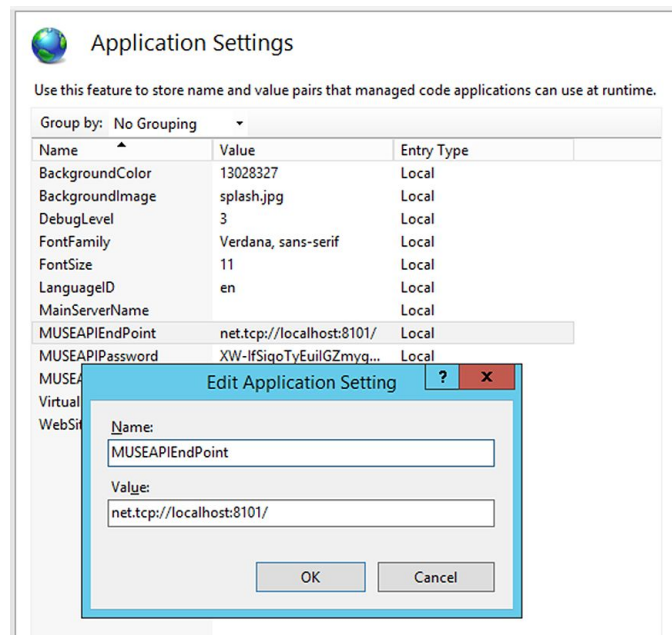
Site: ▼

If you get an error message instead, refer to ["Troubleshooting" on page 129](#).

Changing the MUSE Web Compatibility Layer Configuration Settings

The following information can be used to modify the existing MUSE Web Compatibility Layer Endpoint configuration.

1. Open Internet Information Service (IIS) Manager (*inetmgr.exe*).
2. Navigate to and select the **MuseWebCompatibilityLayer** website to be configured.
3. From the **ASP.NET** section, double-click on **Application Settings**.
The **Application Settings** screen appears.
4. Double-click on **MUSEAPIEndPoint**.
The **Edit Application Setting** dialog is displayed.



5. In the **Value** field, type the desired URI Endpoint that the MUSE Web Compatibility Layer website should use to communicate with MUSEAPI3.
6. Click **OK**.

NOTE:

The **MUSEAPIPassword** is encrypted and stored here. If the password of the website's assigned user has changed, you must uninstall and reinstall the MUSE Web Compatibility Layer with the user's new password. If you also need to change the password of an additional MUSE Web Compatibility Layer website, you must repeat the steps for creating the additional website after you reinstall the MUSE Web Compatibility layer with the new password.

Manual Corrections for MUSE Web Compatibility Layer Installer

Sometimes the custom actions which the MWCL installer uses do not completely configure the MUSE Web Compatibility Layer website for use. If the MUSE Web Compatibility Layer exhibits one or both of the following symptoms, perform the manual steps in the following sections to correct the configuration.

- No login prompt and/or HTTP Error 401.2 when accessing the MUSE Web Compatibility Layer website
- HTTP Error 404.0 when accessing the MUSE Web Compatibility Layer website

No login prompt or HTTP Error 401.2 when accessing the MUSE Web Compatibility Layer website

If the IIS authentication is not set for the MUSE Web Compatibility Layer website by the MWCL installer, no login prompt appears and/or **HTTP Error 401.2 - Unauthorized** message is displayed when attempting to access the MUSE Web Compatibility Layer website.

Perform the following steps to manually set the authentication for the MUSE Web Compatibility Layer website in IIS.

1. Open **Internet Information Services (IIS) Manager (inetmgr.exe)**.
2. Navigate to and select the MuseWebCompatibilityLayer website.
The **MuseWebCompatibilityLayer Home** screen opens.
3. Under the **IIS** heading, select the **Authentication** feature.
4. Enable either **Windows Authentication** or **Basic Authentication**.

HTTP Error 404.0 When Accessing the MUSE Web Compatibility Layer Website

If the ***musewebMap*** handler mapping is not created by the MWCL installer, an **HTTP Error 404.0 - Not Found** message is displayed when attempting to access the MUSE Web Compatibility Layer website.

Perform the following steps to manually create the ***musewebMap*** handler mapping.

1. Open **Internet Information Services (IIS) Manager (inetmgr.exe)**.
2. Navigate to and select the MuseWebCompatibilityLayer website.
The **MuseWebCompatibilityLayer Home** screen opens.
3. Under the **IIS** heading, open the **Handler Mappings** feature.
4. Verify that ***musewebMap*** does not appear on the list of mappings.
5. From the **Actions** menu, click **Add Script Map...**
The **Add Script Map** window opens.

6. Complete the **Add Script Map** fields using the information in the following table.

Field Name	Value
Request path	*.dll
Executable	Enter the path to the aspnet_isapi.dll file. This path is typically C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll The path and file may be manually entered or the ... button may be used to browse to and the file.
Name	musewebMap

7. Click the **Request Restrictions** button.
The **Request Restrictions...** window opens.
8. Select the **Mapping** tab.
9. Clear the box next to **Invoke handler only if request is mapped to**.
10. Select the **Verbs** tab.
11. Verify that the **All verbs** radio button is selected.
12. Select the **Access** tab.
13. Verify that the **Script** radio button is selected.
14. Click **OK** to close the **Request Restrictions** window.
15. Click **OK** to close the **Add Script Map** window.
16. Click **Yes** to the **Do you want to allow this ISAPI extension?** prompt.
17. Verify that the **musewebMap** handler mapping was created and added to the list of mappings.

Troubleshooting

Use the following troubleshooting table to help resolve issues encountered with the MUSE Web Compatibility Layer.

Symptom	Condition	Action
There are no MUSE sites configured for the following user: domain\user.	The domain\user specified in the message is not a valid MUSE user.	Ensure the user attempting to access the MUSE Web Compatibility Layer site is a MUSE user whose Windows User Name matches the domain\user in the message.
	The MUSE system is in an AutoShutdown state.	Cancel the AutoShutdown .
User cannot log in to the MUSE Web Compatibility Layer.	User is not a member of the local MUSE Web Users group on the MUSE application server.	Add user to the MUSE Web Users group on the MUSE application server.

Symptom	Condition	Action
The MUSE Web Compatibility Layer website will not display on the MUSE application server, but will work from other systems or browsers other than Internet Explorer.	IE Enhanced Security Configuration is enabled on the MUSE application server.	Disable IE Enhanced Security Configuration on the MUSE application server.
There are no MUSE sites configured for the following user: .	IIS Authentication used for the website is Anonymous and a URL other than RetrieveTestList, GeneratePatientList, and RetrieveTestByDateTime was used.	When Anonymous Authentication is used for the website, only specific RetrieveTestList, GeneratePatientList, and RetrieveTestByDateTime URLs can be used. Refer to the <i>MUSE Enterprise Integration Reference Manual</i> for supporting information for these URLs.
404 error when browsing the MUSE Web Compatibility Layer website.	Allow unlisted file name extensions option is disabled in IIS.	Extra configuration steps must be taken if Allow unlisted file name extensions option is disabled in IIS. For more information, see "IIS Unlisted File Name Extension Configuration for MUSE Web Compatibility Layer" on page 133.

Uninstalling the MUSE Web Compatibility Layer

Uninstalling the MUSE Web Compatibility Layer removes the following:

- **MuseWebCompatibilityLayer** website
- **MuseWebCompatibilityLayer** folder in **c:\inetpub\wwwroot**
- **MuseWebCompatibilityLayerPool** in **Application Pools**

Uninstalling the MUSE Web Compatibility Layer does NOT remove:

- **MUSE Web Users** group
- Any secondary/additional MUSE Web Compatibility Layer websites that were created

1. Log on to the MUSE application server as administrator.
2. Go to the Windows **Control Panel** and select **Programs and Features**.
3. Right-click on **MWCLBasicInstaller** and choose **Uninstall**.
A message asking you to confirm the removal is displayed.
4. Click **Yes**.
5. If a **User Account Control** dialog box appears, choose **Yes** or **Allow**.

Creating an Additional MUSE Web Compatibility Layer Website

The MUSE Web Compatibility Layer installer only installs a single instance of the MUSE Web Compatibility Layer website in the default installation folder. A customer may want to add one or more additional instances of the MUSE Web Compatibility Layer website on a different port with a different authentication scheme.

These steps can only be performed after the default MUSE Web Compatibility Layer website is installed.

Perform the following steps to create an additional MUSE Web Compatibility Layer website:

1. Go to **C:\inetpub\wwwroot** and make a copy of the **MUSEWebCompatibilityLayer** folder in the same directory.
2. Rename the copied folder, for example **MUSEWebCompatibilityLayer2**.
3. Go to the security settings for the folder you just created and add the appropriate group(s) that need access to the website, such as **MUSE Web Users**, with the following permissions:
 - **Read & execute**
 - **List folder contents**
 - **Read**
4. Open Internet Information Services (IIS) Manager (inetmgr.exe).
5. Right-click on **Application Pools** and choose **Add Application Pool...**
6. Complete the required fields as indicated in the following table and click **OK**.

Application Pool Field Values

Field	Value
Name	Enter the name of the folder you created in step 2, such as MUSEWebCompatibilityLayerPool2 .
.NET Framework version	.NET CLR or Framework v4.0.30319
Managed pipeline mode	Classic
Start application pool immediately	Select this box

7. Right-click the application pool you created in steps 5 and 6, and choose **Advanced Settings...**
8. Verify/Change the fields as indicated in the following table and click **OK**.

Field Values for Application Pool - Advanced Settings

Field	Value
Enable 32-bit Applications	True
Queue Length	4000

Field Values for Application Pool - Advanced Settings (cont'd.)

Field	Value
Limit Interval (minutes)	0
Identity	NetworkService

9. Right-click on **Sites** and choose **Add Website...**
10. Complete the required fields as indicated in the following table and click **OK**.

Field Values for Sites - Add Website... Screen

Field	Value
Site Name	Type the name of the folder you created in steps 1 and 2, such as MUSEWebCompatibilityLayer2 .
Application Pool	Click Select and choose the Application Pool you created in steps 5 and 6.
Physical Path	Click Browse and navigate to the copied folder created in steps 1 and 2, then click OK .
Binding	<ul style="list-style-type: none"> • Type = http • IP address = All Unassigned • Port = Set to the port number you are using. The port must be unique and not be used by any other applications or websites.
Host Name	Leave blank.
Start Website immediately	Select this box.

11. Select the website that you created in steps 9 and 10.
12. Open **Authentication** and enable the authentication method you are using.
If you are using Anonymous Authentication, you must edit the properties and enter the credentials for a Windows user that is also a MUSE user who has access to the MUSE system.
13. Verify the new website works as expected.

NOTE:

When using Internet Information Services (IIS) anonymous authentication with a MUSE Web Compatibility Layer website, only specific RetrieveTestList, GeneratePatientList, and RetrieveTestByDateTime URLs can be used. Refer to the *MUSE Enterprise Integration Reference Manual* for supporting information for these URLs.

Disabling Directory Browsing for MUSE Web Compatibility Layer

By default, the **MUSEWebCompatibilityLayer** website allows for **Directory Browsing**. This may be undesirable default behavior as it allows for manually browsing folders on the website that would not normally be exposed to users of the website.

The following steps can be used to verify whether the **Directory Browsing** is enabled for the **MUSEWebCompatibilityLayer** website and disable it if it is

1. Go to the Internet Information Services (IIS) Manager.
2. Select **MUSEWebCompatibilityLayer** website.
3. Open **Directory Browsing**.

NOTE:

If **Directory Browsing** is not an option, then the **Directory Browsing Role Service** is not installed at all which means that **Directory Browsing** is not possible which has the equivalent effect as disabling it and no further action is required

4. Under **Actions**, verify whether the available action is **Enable** or **Disable** and perform one of the following action:
 - If the available action is **Enable**, **Directory Browsing** has already been disabled for the website and no further action is required.
 - If the available action is **Disable**, click **Disable** and verify the action changes to **Enable**.

IIS Unlisted File Name Extension Configuration for MUSE Web Compatibility Layer

Internet Information Services (IIS) has a **Request Filtering** configuration that can allow it be configured to disallow unlisted file name extensions. By default, IIS allows unlisted file name extensions. If the **Allow unlisted file name extensions** option is disabled for the **MUSEWebCompatibilityLayer** website, a **404** error occurs when accessing the website.

The following steps can be used to verify whether the **Allow unlisted file name extensions** option is disabled for the **MUSEWebCompatibilityLayer** website.

Verify Option is Disabled

1. Go to the Internet Information Services (IIS) Manager.
2. Select **MUSEWebCompatibilityLayer** website.
3. Open **Request Filtering**.
4. Go to **Actions > Edit Feature Settings...**

An **Edit Request Filtering Settings** window opens.

If the box next to the **Allow unlisted file name extensions** option is not selected, the option is disabled.

Change Configuration to Enable Allow Unlisted File Name Extensions Option

The following configuration changes are necessary if the **Allow unlisted file name extensions option** is disabled for the **MuseWebCompatibilityLayer** website.

1. Go to the Internet Information Services (IIS) Manager.
2. Select **MuseWebCompatibilityLayer** website.
3. Open **Request Filtering**.
4. Go to **Actions > Allow File Name Extension...**
An **Allow File Name Extension** prompt opens.
5. In the **File name extension** field, type an extension as appropriate using the information in the following table and click **OK**.

File Name Extension	Reason
.	This is a single period or dot. This allows you to browse to the Select MuseWebCompatibilityLayer website.
.htm	This allows access to the museweb.htm file.
.dll	This allows access to the museweb.dll function.
.gif	This allows access to the unity.gif image.

6. Repeat steps 4 and 5 for each extension listed in the table,
7. Restart the **MuseWebCompatibilityLayer** website.

Manually Installing and Verifying IIS Related Roles, Role Services, and Features

Installing IIS 7 Role Services on Windows Server 2008 or 2008 R2

Use the following steps to install or verify that the required IIS components are installed on Windows Server 2008 or 2008 R2 systems.

1. Log on to the MUSE application server as an administrator user.
2. Open **Server Management (CompMgmtLauncher.exe)**.
3. Go to **Action > Add Roles**.

The **Add Roles Wizard** window opens.

If the **Before You Begin** window opens, click **Next**.

The **Select Server Roles** window opens.

4. Perform one of the following steps:
 - a. If the box next to the **Web Server (IIS)** is not already selected, perform the following steps:
 - i. Select the box next to **Web Server (IIS)**.
If an **Add features required for Web Server (IIS)?** window opens, click **Add Required Features**.
 - ii. Proceed to step 5.
 - b. If the box next to **Web Server (IIS)** is already selected, perform the following steps:
 - i. Click **Cancel**.
 - ii. Click **Yes** when prompted to cancel the wizard.
 - iii. From **Server Manager**, expand **Roles** and select **Web Server (IIS)**.
 - iv. Go to **Action > Add Role Services**.
 - v. Proceed to step 7.

5. Click **Next**.

The **Web Server (IIS)** window opens.

6. Click **Next**.

The **Select Role Services** window opens.

7. Confirm that the following items are selected.

Static Content	ISAPI Filters
Default Document	HTTP Logging
Directory Browsing	Request Monitor
HTTP Errors	Basic Authentication
ASP.NET	Windows Authentication
.NET Extensibility	Request Filtering
ISAPI Extensions	IIS Management Console

If an **Add role services and features required for ...?** window opens, click **Add Required ...**

8. Perform one of the following steps:
 - a. If one or more role services had to be enabled and the **Next** button is available to click, perform the following:
 - i. Click **Next**.
The **Confirm Installation Selections** window opens.
 - ii. Click **Install**.
The requested roles, role services, and features are installed.

- iii. When the **Installation Results** window opens, verify the message, **Installation succeeded**, appears.
 - iv. Click **Close**.
 - b. If all of the role services required are already enabled and the **Next** button is not available, perform the following:
 - i. Click **Cancel**.
 - ii. Click **Yes** when prompted to cancel the wizard.
- 9. If the **Add Roles Wizard** indicates a restart of the system is required, reboot the system.

Installing IIS 8 Role Services on Windows Server 2012 or 2012 R2

Use the following steps to install or verify that the required IIS components are installed on Windows Server 2012 or 2012 R2 systems.

1. Log on to the MUSE application server as an administrator user.
2. Open **Server Management (CompMgmtLauncher.exe)**.
3. Go to **Manage > Add Roles and Features**,
The **Add Roles and Features Wizard** opens.
If the **Before You Begin** window opens, click **Next**.
The **Select Installation Type** window opens.
4. Select the **Role-based or feature-based installation** radio button and click **Next**.
The **Select Destination Server** window opens.
5. Confirm that the **Select a server from the server pool** radio button is selected.
6. Confirm that the local computer is selected in the **Server Pool** list.
7. Click **Next**.
The **Select server roles** window opens.
8. Perform one the following steps:
 - a. If the check box next to **Web Server (IIS)** is not already selected, perform the following steps:
 - i. Select the box next to **Web Server (IIS)** .
If an **Add features that are required for Web Server (IIS)?** window opens, confirm that **Include management tools (if applicable)** is selected and then click **Add Features**.
 - ii. Proceed to step 9.
 - b. If the check box next to **Web Server (IIS)** is already selected or shaded, proceed to step 12.
9. Click **Next**.
The **Select Features** window opens.
10. Click **Next**.
The **Web Server (IIS)** window opens.

11. Click **Next**.
The **Select Role Services** window opens.
12. Expand all of the web server subcomponents and confirm that the following items are selected:

Default Document	Basic Authentication
Directory Browsing	Windows Authentication
HTTP Errors	.NET Extensibility 4.5
Static Content	ASP.NET 4.5
HTTP Logging	ISAPI Extensions
Request Monitor	ISAPI Filters
Request Filtering	IIS Management Console

If an **Add features that are required for...?** window opens, confirm that **Include management tools (if applicable)** is selected and then click **Add Features**.

13. Click **Next**.
14. Perform one of the following steps:
 - a. If the **Confirm installation selections** window opens, perform the following steps:
 - i. Click **Install**.
The **Installation progress** window opens and the requested roles, role services, and features are installed.
 - ii. Leave the **Installation progress** window open until the installation is complete and the **Installation succeeded** message opens.
 - iii. Click **Close**.
 - b. If the **Select features** window opens and the **Next** button is available to click, perform the following steps:
 - i. Click **Next**.
The **Confirm Installation Selections** window opens.
 - ii. Click **Install**.
The **Installation progress** window opens and the requested roles, role services, and features are installed.
 - iii. Leave the **Installation progress** window open until the installation is complete and the **Installation succeeded** message opens.
 - iv. Click **Close**.
 - c. If the **Select Features** window opens and the **Next** button is not available (shaded, because all of the required roles, role services, and features are already installed), click **Cancel**.
The **Add Roles and Features Wizard** window closes.
15. If the **Add Roles and Features Wizard** indicates a restart of the system is required, reboot the system.

MACCRA Compatibility

This chapter describes how to install MACCRA Compatibility for use with MUSEAPI3 and MUSE v9.

Theory of Operation

If you have a system with a third-party interface designed to communicate with the MUSE system using MACCRA or MUSEAPI2, MACCRA Compatibility will allow you to continue to use those systems with the new MUSEAPI3 without the need to redesign the interface.

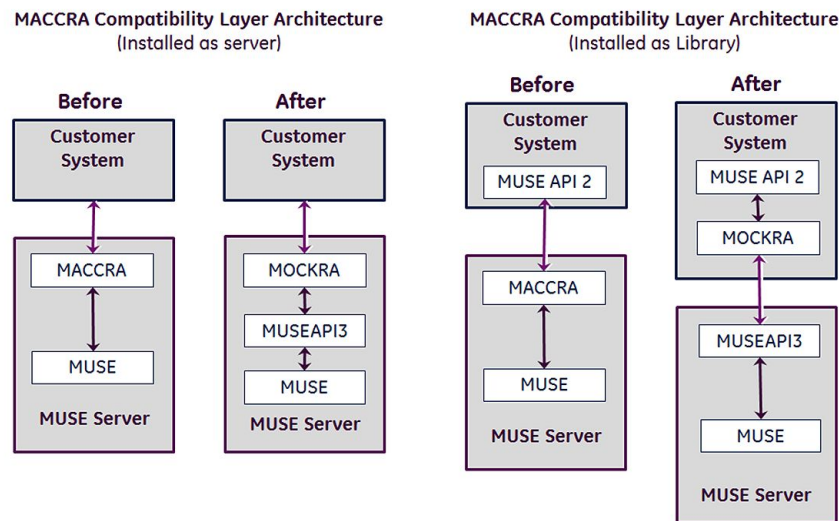
NOTE:

Installation of this compatibility layer should be discussed with GE Healthcare Technical Support or Engineering before being applied at a customer site.

MACCRA Compatibility can be installed as an application on servers that interface with the MUSE system using IDispMUSEAPI, a COM interface provided by MACCRA. MACCRA Compatibility can also be installed as a library application on clients that interface with the MUSE system using MUSEAPI2.

The MACCRA Compatibility layer installs a new Windows Component service, called **MOCKRA**, under COM+ Applications. The **MOCKRA COM+** component service recognizes requests from the customer interface designed to use MACCRA and

prepares them for use by MUSEAPI3. See the following illustration to compare how the interface components will change with the MACCRA Compatibility layer installed.



Installation Requirements

Before You Begin

If it is determined that MACCRA Compatibility should be installed, you need to determine:

- verify that MUSEAPI3 is installed. MACCRA Compatibility requires MUSEAPI3 to function. See [Chapter 9 “MUSEAPI3 Installation” on page 105](#) for information on installing MUSEAPI3.
- whether the installation will be installed as a Server Application or Library Application.
- which MUSEAPI3 server to use for connection. This is typically the MUSE application server that has MUSEAPI3 installed on it.
- which MUSEAPI3 port and protocol to use. MUSEAPI3 supports HTTP, HTTPS, and net.tcp protocols.

Customer Requirements

The customer is responsible for appropriate network connectivity, including name resolution, between the systems requiring MACCRA Compatibility and the MUSE application server.

MACCRA Compatibility with CV Web v1.x and v2.x

NOTE:

CV Web v3.0 is not compatible with MACCRA.

CV Web v1.x and v2.x use MACCRA to communicate with the MUSE database. The following information can be used to ensure CV Web v1.x and v2.x work with MUSE v9.

- The Windows **Application Server Role** and **COM+ Network Access Role Service** must be installed on the MUSE application server.
- Any users or groups that need access to CV Web v1.x and v2.x must be a member of the local **Distributed COM Users** group on the MUSE application server. Typically **Everyone** would be a member of this group to ensure all users have access, however this can be modified to meet the customer's needs.
- Ensure the local security policy **Network access: Let Everyone permissions apply to anonymous users** is set to **Enabled** on the MUSE application server.
- MUSE API v3.1 must be installed on the MUSE application server.
- Install MACCRA Compatibility as a server application on the MUSE application server.
- Configure the CV Web v1.x or v2.x to communicate with the MUSE application server. Refer to appropriate CV Web documentation for CV Web configuration information.

Creating a MUSE User for MACCRA Compatibility

The MUSE v9 system includes patient access logging. All use of MACCRA Compatibility is logged in the MUSE audit logs as the MUSE user configured for the MACCRA Compatibility. It is recommended that you create and use a new MUSE user for MACCRA Compatibility to allow for MUSE patient access logging details to reflect this specific MUSE user.

Perform the following steps to create a new MUSE user:

1. From within the MUSE application, go to **Setup**.
2. Select **Users**.
The list of users opens.
3. Select **Action > New**.
4. Select the **General** page and complete the fields as indicated in the following table:

NOTE:

You may accept the default value for all fields, with the exception of those specified in the following table.

MUSE User Creation – General Page Field Requirements

Field	Action
Last Name	Enter a last name for the MACCRA user, for example, MACCRAUser.
First Name	Enter a first name for the MACCRA user, for example, MACCRAUser.
MUSE USER name	Enter a MUSE User Name for the MACCRA user, for example, MACCRAUser.
MUSE Password	Enter a password for the MACCRA user. Make a note of this password as it will be needed later when installing and configuring MACCRA Compatibility.

MUSE User Creation – General Page Field Requirements (cont'd.)

Field	Action
Re-enter MUSE Password	Re-enter the password you entered in the MUSE Password field. The password you enter here and the password you enter in the MUSE Password field must be identical.
Active Sites	Select the box next to each site to which this user needs access.

5. Select the **Advanced** page and complete the fields in the following table:

NOTE:

You may accept the default for all fields, with the exception of those specified in the following table.

MUSE User Creation – Advanced Page Field Requirements

Field	Action
User ID	Enter a user ID. This ID must be unique and may not be used by any other MUSE users.
Role	Set this to All Privileges .
Job Titles	Clear all boxes in this list.
Display User in Personnel Lists	Clear this box.

Installing MACCRA Compatibility

Complete the following procedure to install MACCRA Compatibility.

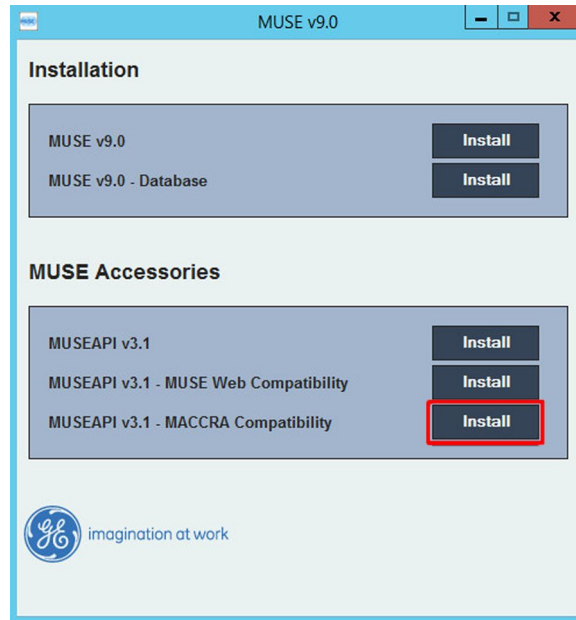
1. Log on to the system where MACCRA Compatibility will be installed using an account that has **administrator** privileges.
2. Have the customer disable any antivirus software during the installation. The antivirus software should be re-enabled after the installation is complete.
3. Insert the MUSE v9 installation media into the optical drive of the system.
If any **Autorun** or **AutoPlay** screens appear, close or cancel them.
4. Browse the optical drive in Windows Explorer and perform one of the following:
 - If the MUSE v9 Application and Support DVD is inserted, navigate to the **MUSE Application** folder and execute the **Autorun.exe** application.
 - If the MUSE v9 Application ISO is being used, navigate to the root folder and execute the **Autorun.exe** application.

NOTE:

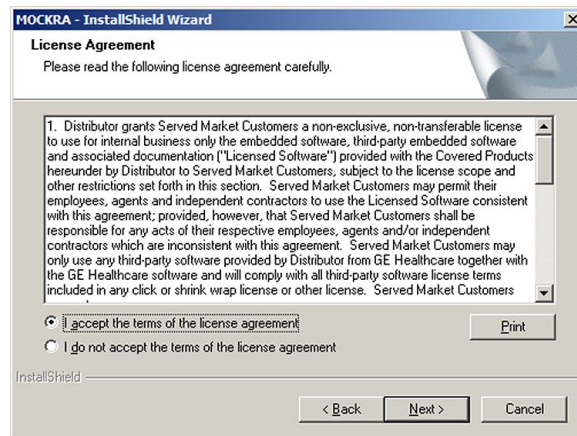
Be sure to execute **Autorun.exe** and not **Autorun.exe.config**.

The MUSE v9.0 installation options window opens.

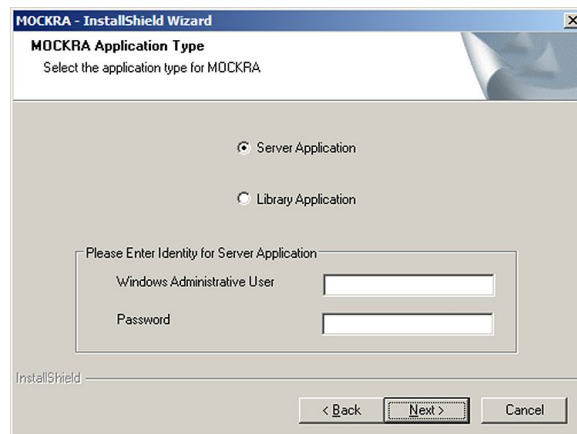
5. Click **Install** next to **MUSEAPI v3.1 – MACCRA Compatibility**.



6. If a User Account Control Prompt opens, click **Yes** or **Allow**.
One of two windows opens. How you proceed depends on which window opens.
- If a window opens with a message that states:
MOCKRA requires the following items to be installed on your computer.
Click Install to begin installing these requirements.
proceed to step 7.
 - If a window opens that states:
Welcome to the InstallShield Wizard for MOCKRA
proceed to step 8.
7. Click **Install**.
The installation program extracts and installs .NET Framework 4.5.1.
After the installation of .NET Framework 4.5.1, the **Welcome to the InstallShield Wizard for MOCKRA** window opens.
8. Click **Next**.
The **License Agreement** window opens.



9. Read and accept the **License Agreement**.
 10. Click **Next**.
- The **MOCKRA Application Type** window opens.



11. Select the **MOCKRA Application Type** that was determined in “[Before You Begin](#)” on [page 140](#).

If the **Server Application** is selected, enter the required information in the **Please Enter Identity for Server Application** area.

- For a domain user, use **<domain>\<user name>** format.
- For a local user, use **.\<user name>** format. This user must be a Windows Administrator User on the system. It will be set as the identity for the MOCKRA component being used as a **COM+** service.

If installing on the MUSE Application server, the same MUSE Background user that is configured to start the MUSE services may be used here.

12. Click **Next**.

The **MOCKRA Configuration** window opens.

13. Complete the fields in the MOCKRA Configuration window; these fields are mandatory. Use the information in the following table to complete the fields.

Field	Description / Action
MUSE API3 Web Service End Point	Enter the Uniform Resource Identifier (URI) of the server where MUSEAPI3 is installed. The endpoint is composed of the protocol and port selected for MUSEAPI3 when it was installed and the name of the MUSE Server it is installed on. For example, to communicate with a MUSE Server installed on the local box using the MUSEAPI3 default install settings, you would enter: http://localhost:8100/ or net.tcp://localhost:8101/. If MUSEAPI3 is installed on a different server, replace localhost with the IP address or server name of the server it is installed on.
MUSE User Name	A MUSE user (not Windows user) who is assigned all MUSE privileges and has access to all MUSE sites. It is recommended that a new MUSE user be created for the purpose of accessing the MUSE system via the MACCRA Compatibility. Refer to "Creating a MUSE User for MACCRA Compatibility" on page 141.
Password	Enter the password for the MUSE user entered in the MUSE User Name field.
Maximum Connections Allowed	By default, the maximum allowed connections for the MOCKRA Server Application is 100. Change this value if a different number is desired.

14. Click **Next**.

15. When the **InstallShield Wizard Complete** window opens, click **Finish**.

Verifying the MACCRA Compatibility Installation

Complete the following procedure to verify the MACCRA Compatibility installation.

1. In Windows, go to **Administrative Tools>Component Services**.
The **Component Services** window opens.
2. Expand **Component Services**, and select **Computers>My Computer>COM+ Applications**.
3. Verify that **MOCKRA** is present.
4. Right-click **MOCKRA** and select **Properties**.
The **Properties** window opens.
5. Select the **Activation** tab.
6. Verify the **Activation** type is correct (**Server Application** or **Library Application**).
7. If installed as **Server Application**, select the **Identity** tab and verify that the identity matches the Windows administrator user specified during the install.

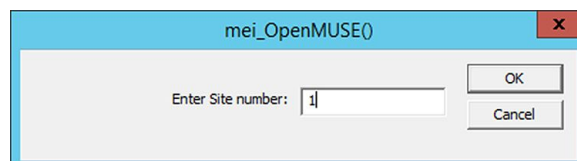
System Checkout

Complete the following procedure to ensure MACCRA Compatibility Layer can communicate with MUSEAPI3 and the MUSE database.

NOTE:

This procedure can only be used to test MACCRA Compatibility installed as a **Library Application**. To test MACCRA Compatibility installed as a **Server Application**, the actual MACCRA client (such as CV Web v2.x) needs to be used to verify MACCRA Compatibility Server Application functionality.

1. Log on to the system where MACCRA Compatibility is installed.
2. Insert the MUSE v9 installation media into the optical drive of the system.
If any **Autorun** or **AutoPlay** screens appear, close or cancel them.
3. Browse the optical drive in Windows Explorer and perform one of the following:
 - If the MUSE v9 Application and Support DVD is inserted, navigate to the **\MUSE Support\MUSE API DCOM** folder.
 - If the MUSE v9 Support ISO is being used, navigate to the **\MUSE API DCOM** folder.
4. Run **MUSEAPI DCOM Tester.exe**.
5. Go to **API Functions > 1. mei_OpenMUSE**.
The **mei_OpenMUSE()** dialog box opens.



6. Enter a valid MUSE Site number and click **OK**.
7. Verify the message **Operation Succeeded** is displayed.
8. Click **OK**.
9. Go to **API Functions > 3. mei_TestsForPatient**.
The **TestsForPatient** window opens.

TestsForPatient

Patient ID: 878787878

Test Month: 255 Test Hour: 255

Test Day: 255 Test Min: 255

Test Year: 65535 Test Sec: 255

Test Type: 1

OK Cancel

10. Identify a patient that has an ECG test for the MUSE site you selected in step 6. Enter the Patient ID for the selected patient into the **Patient ID** field. Accept the defaults for the remaining fields.
11. Click **OK**.
12. Verify you get a message dialog box indicating the number of tests found and the entries for each.

mei_OpenTestsForPatient

Found 2 entries for PID: 878787878, Test Type=1

Entry 1: Test Date:20-12-2006, Test Time: 11:55:05, PSIG = 12

Entry 2: Test Date:20-12-2006, Test Time: 11:55:05, PSIG = 11

OK

13. Write down the PSIG for one of the entries.
14. Click **OK**.
15. Go to **API Functions > 5. Mei_CreateOutputForTestInfo**.
16. The **mei_CreateOutputForTestInfo** window opens.

mei_CreateOutputForTestInfo

PSIG: 12

Test Type: 1 Output Type: 12

Output File Name: D:\TEMP\OUTPUT.PDF

OK Cancel

17. In the **PSIG** field enter the PSIG you wrote down in step 13.
18. Verify the **Test Type** is **1** and the **Output Type** is **12**.

19. In the **Output File Name** field, type in a path and filename with a PDF extension. The path specified here must be a valid, pre-existing path.
20. Click **OK**.
21. Verify the message **Output saved in file...** is displayed.
22. Click **OK**.
23. Verify the output file was created in the location and with the name specified in step 19 and that it can be viewed in a PDF viewer, such as Adobe Reader.

Changing MACCRA Compatibility Configuration

The installer copies the following tools to **C:\Program Files (x86)\MOCKRA**:

- **MOCKRAConfigWriter.exe**
- **MOCKRAServerProvisioner.exe**

These are command line tools that can be used to change the **MOCKRA Configuration** without the need to remove and reinstall MACCRA Compatibility.

MOCKRAConfigWriter.exe

1. Using an account that has administrator privileges, log on to the system where MACCRA Compatibility is installed.
2. Open a command prompt window using **Run as Administrator** and change to the **MOCKRA** installation folder. The default is **C:\Program Files (x86)\MOCKRA**.
3. Run **MOCKRAConfigWriter.exe** with the appropriate command line string as shown.

You must enter the complete string even if you are changing only one of the settings. If the **defaultconnectionlimit** is not being changed, it can be left off.

- If MOCKRA is installed as a **Server Application**, enter the lines below as one continuous string adding a space between each line entry shown below.
filename:MOCKRA.xml
endpoint:URI of MUSEAPI3
username:muse user name
password:password for muse user name
defaultconnectionlimit:the maximum number of connections allowed
- If MOCKRA is installed as a **Library Application**, enter the lines below as one continuous string adding a space between each line entry as shown:
filename:library\MOCKRA.xml
endpoint:URI of MUSEAPI3
username:muse user name
password:password for muse user name

defaultconnectionlimit:the maximum number of connections allowed

4. Open the appropriate **MOCKRA.xml** file to verify the changes:

Application Type	Path and Filename
Server Application	C:\Program Files (x86)\MOCKRA\MOCKRA.xml
Library Application	C:\Program Files (x86)\MOCKRA\Library\MOCKRA.xml

NOTE:

Changes can also be made by opening the appropriate **MOCKRA.xml** file in Notepad and editing it directly. If changing the MUSE username password you must use the **MOCKRAConfigWriter.exe** as described in step 3.

MOCKRAServerProvisioner.exe

Use the following procedure to change the identity for the MOCKRA COM+ component service. This is only required if MACCRA Compatibility has been installed as a **Server Application**.

1. Using an account that has administrator privileges, log on to the system where MACCRA Compatibility is installed.
2. Open a command prompt window using **Run as Administrator** and change to the MOCKRA installation folder. The default is **C:\Program Files (x86)\MOCKRA**.
3. Run **MOCKRAServerProvisioner.exe** with the appropriate command line string as shown.

identity:Identity User Name

For a domain user use <domain>\<user name> format. For a local user use .\<user name> format. This user must be a Windows administrator user on the system. It will be set as the identity for the MOCKRA component being used as a **COM+** Service.

password:Password for the specified user.

4. Verify the change.
 - a. Go to **Administrative Tools>Component Services**.
 - b. Expand **Component Services**, and select **Computers>My Computer>COM+ Applications**.
 - c. Right-click **MOCKRA** and select **Properties**.
The **Properties** window opens.
 - d. Select the **Identity** tab and verify that the identity matches the Windows administrator user specified.

NOTE:

The Identity can also be changed manually from **Component Services** rather than using **MOCKRAServerProvisioner.exe**.

Uninstalling MACCRA Compatibility

Use the following instructions to uninstall MACCRA Compatibility, if needed.

NOTE:

Uninstalling MACCRA Compatibility completely removes the software and all configuration files.

1. Go to **Control Panel>Programs and Features**.
2. Select **MOCKRA** from the list and click **Uninstall**.
The **Welcome** window opens.
3. Verify **Remove** is selected and click **Next**.
4. At the **Do you want to completely remove the selected application and all of its features?** prompt, click **Yes**.
5. When the **Uninstall Complete** window opens, click **Finish**.

12

CardioDay to MUSE System Interface

This chapter describes how to set up and configure the interface between CardioDay V2.5 Holter ECG Analysis system and the MUSE v9 (SP6 or later) Cardiology Information System to exchange HL7 Holter Order and final report data.

Theory of Operation

The CardioDay to MUSE Interface features allows you to exchange HL7 Holter Order and final report data between the CardioDay V2.5 Holter ECG Analysis system and a MUSE v9 (SP6 or later) Cardiology Information System. CardioDay to MUSE system communication allows you to obtain Holter Order/Patient demographics from the MUSE system and export Holter reports from the CardioDay V2.5 or higher system to the MUSE system for viewing, editing, printing, and storage. Both features are intended to improve user workflow in institutions which share CardioDay V2.5 and MUSE v9 (SP6 or later).



CardioDay to MUSE Holter Patient ADT/Order Interface

This feature allows the CardioDay user to import patient data from an open MUSE Holter order to a connected Holter recorder. When the data is imported and the Holter recording is started on the device, the order's **Status** is changed from **Open** to **Pending**.

The CardioDay V2.5 MUSE Orders feature has been added to provide the ability to retrieve open Holter orders from MUSE v9 (SP6 or later) systems, allowing the transfer of patient demographic and order information to the SEER 1000 and other Holter recorder devices. The communication between the CardioDay and MUSE system is done via a RESTFUL Windows Web Services HTTP interface to the MUSE v9 MUSEAPI3.1 or later interface.

If your CardioDay V2.5 system is configured to query and retrieve Patient Demographic and Order data from MUSE, the MUSE Orders option button is enabled in the Transfer

Patient Data and Recorder Hookup Preview windows. Select Query Orders to open the MUSE Holter/Order list.

NOTE:

Only MUSE Orders for Holter test types with an Open status are displayed at the CardioDay Orders list. If no MUSE Orders meet these criteria, the list will be empty.

The configuration of CardioDay MUSE Order Option requires that the following details of the customer's MUSE environment be known or confirmed:

- MUSE v9 Cardiology Information System (SP6 or later) with MUSEAPI3.1 or later option installed and configured with service running
- MUSE System network hostname or IP address
- MUSE System MUSEAPI3 TCP Port for "HTTP Service Endpoint"
- MUSE User and Password

NOTE:

It is suggested that a dedicated MUSE user be created for communication to the MUSE Orders interface. For additional details, see ["Creating a Dedicated MUSE User Account for CardioDay Holter Orders Query"](#) on page 158.

CardioDay Holter Report Export to the MUSE System

After the Holter recording, download, and analysis is complete on the CardioDay system, the user can export the Holter PDF Report and metadata back to the MUSE system for review. When the report and metadata is imported in the MUSE system, the order's **Status** is changed from **Pending** to **Unconfirmed** and the order is linked to report.

The CardioDay V2.5 system can be configured to automatically archive a recording after it has been exported to the MUSE system.

In CardioDay to MUSE system communication, Holter Reports are exported from CardioDay to a shared folder as a pair of files: the Holter PDF Report (*.pdf file extension) and the report metadata (*.txt file extension) back to the MUSE system for review. CardioDay MUSE system communication uses the **MUSE Generacq** service to acquire the CardioDay tests from the configured share folder. The **MUSE Generacq** service searches that folder for *.txt files and processes the report data when detected. Holter report tests are then normalized on the MUSE system and stored in the database.



Transmission Flow Chart

Determining MUSE eDoc Connect Parameters

Gather the following information prior to beginning the CardioDay to MUSE interface setup.

Information Needed	Description
eDoc Connect option enabled?	Determine if the eDoc Connect option is already enabled. If it is not, it will need to be temporarily enabled and then must be disabled (if not purchased/in use by customer for other data/report type imports) after the CardioDay to MUSE Communication configuration is complete.
MUSE Site	This is the MUSE Site Number that the CardioDay data will be imported into.
MUSE Site Location	This is the MUSE Location for the Site that the CardioDay data will be imported into.
Share Folder	The location that the MUSE Generacq will monitor for CardioDay data. To be able to transfer CardioDay reports to MUSE, a shared folder must be created. While this share can be configured on either the MUSE or CardioDay systems, it is necessary that both systems can create and retrieve report files from that share. It is recommended, but not mandatory, that the share be created on the CardioDay system and be provided full access (Read/Write/Delete) to all CardioDay Users and the MuseBkgnd user.

CardioDay to MUSE Interface Prerequisites

To use the optional CardioDay to MUSE System Interface features, the following requirements must be met:

Prerequisite Description	CardioDay Feature	System
CardioDay MUSE Connection option must be licensed and activated	Orders Interface/Report Export	CardioDay
MUSE v9 (SP6 or later) Cardiology Information System	Orders Interface/Report Export	CardioDay/MUSE Cardiology Information System
MUSE API v3.1 interface, must be installed and properly configured	Orders Interface	MUSE Cardiology Information System

Prerequisite Description	CardioDay Feature	System
Standard HTTP network connection must be allowed between the CardioDay and MUSE systems on the configured TCP port (default 8100)	Orders Interface	CardioDay/MUSE Cardiology Information System
MUSE System Holter Data Storage enabled	Orders Interface/Report Export	MUSE Cardiology Information System
ADT/ORM Holter Orders interface must be active for CardioDay/ MUSE Holter Orders	Orders Interface	MUSE Cardiology Information System
CardioDay and MUSE systems must have "FULL Control" (Read, Write, Delete) write access to the shared MUSE import folder using the Windows Authentication and SMB protocol	Report Export	CardioDay/MUSE Cardiology Information System
MUSE eDoc Connect Option must be enabled to configure CardioDay Acquisition Profile (can be disabled after configuration)	Report Export	MUSE Cardiology Information System
Known MUSE User account and Password	Orders Interface	CardioDay/MUSE Cardiology Information System
The MUSE Site Number that Holter Orders will be queried from and the CardioDay Holter Report data will be imported into.	Orders Interface/Report Export	CardioDay

Verifying the CardioDay Software Version

CardioDay to MUSE v9 interface functionality requires CardioDay V2.5 or higher. Verify the CardioDay system is V2.5 or higher before configuring CardioDay V2.5 to MUSE Communication.

To find the CardioDay Application Version, select **Help > Version** in the CardioDay application.

Verifying the MUSE System Software Version

The CardioDay to MUSE v9 interface functionality requires MUSE v9 (SP6 or later). Verify the MUSE system is MUSE v9 (SP6 or later) before configuring CardioDay V2.5 to MUSE Communication.

About MUSE

To find the MUSE Application Version, select **Help > About MUSE** in the MUSE Editor application.

Customer Requirements

The customer is responsible for supplying appropriate network connectivity between the CardioDay V2.5 and MUSE v9 Systems, including name resolution, unrestricted TCP port communication and file share authentication and access rights.

Additional Resources

For additional information on configuring the CardioDay MUSE Interface prerequisites, see CardioDay V2.5 Pre-Installation Manual (GEHC PN 2092513-001).

For additional information on configuring the CardioDay MUSE Interface options, see CardioDay V2.5 Installation and Field Service Manual (GEHC PN 2092513-002).

Configuring CardioDay and MUSE Interface Settings

To configure the setting for the CardioDay and MUSE interface, perform the following procedures in the order that they are listed:

- “Enabling the Holter Data Storage, eDoc Connect, and HIS Interface Option on the MUSE System” on page 155
- “Enabling MUSE Holter Test Type for Each Site” on page 156
- “Enabling MUSE ADT Orders and Holter Orders for Each Site” on page 156
- “Creating the CardioDay Acquisition Profile on the MUSE System” on page 157
- “Setting Up the CardioDay Share Folder in the MUSE System” on page 157
- “Creating a Dedicated MUSE User Account for CardioDay Holter Orders Query” on page 158
- “Configuring the CardioDay System for MUSE Holter Orders” on page 159
- “Configuring the CardioDay System to Export Holter Reports to the MUSE System” on page 159
- “Disabling the eDoc Connect Option” on page 159

Enabling the Holter Data Storage, eDoc Connect, and HIS Interface Option on the MUSE System

1. Log on to the MUSE application server as an Administrator.
2. Perform a full or partial shutdown of the MUSE system.
Use the shutdown procedures describe in the *AutoShutdown* section of the *System Administration* chapter of *MUSE Cardiology Information System Service Manual*.
3. From the Windows **Control Panel**, go to **Programs and Features**.
4. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
5. Choose **Modify** and click **Next**.
The **Select Feature** window opens.

6. Continue to click **Next** on each window until you reach the **Choose MUSE Options** window.
7. Select the **Holter Data Storage**, **eDoc Connect**, and **HIS Interface** options.

NOTE:

If the customer has not purchased the eDoc Connect option, it must be temporarily enabled for the setup of the CardioDay v2.5. Make sure you disable the eDoc Connect option after the CardioDay v2.5 has been set up. See [“Disabling the eDoc Connect Option” on page 159](#).

NOTE:

The Holter Data Storage option is required for CardioDay export to the MUSE system. If the Holter Data Storage option is not already enabled and has been purchased as part of the CardioDay implementation, verify the option codes and activate this option.

8. Click **Next**.
The **MUSE Serial Number** window opens.
9. Enter the **Options Configuration Password**.
If you do not know the password, contact GE Healthcare Technical Support.
10. Click **Next** until your changes are applied and the **Maintenance Complete** window opens.
11. Select **Finish**.

Enabling MUSE Holter Test Type for Each Site

Enable a MUSE Holter Test Type for each site that will be using the CardioDay/MUSE Holter orders or reports.

1. From within the MUSE application, go to **System > Setup > Test Type**.
2. Right-click the **Holter Test Type** (or Action Properties) to edit the Holter **Test Type** properties.
3. Enable the Holter **Test Type ID** for all MUSE System Sites that will use the Holter orders or report data interfaces.
4. In the **Test Type Properties** window, select the **General** tab and enable the Holter **Test Type** for all the sites that will be storing Holter data types.

Enabling MUSE ADT Orders and Holter Orders for Each Site

Use this procedure to enable MUSE System ADT orders and Holter Orders for each site using CardioDay and MUSE Holter Order Interface.

1. From within the MUSE application, go to **Setup > Sites**.
2. To select the desired site and edit its properties, choose of the following;
 - **Action > Properties**
 - **Right-Click > Properties**

3. In the **HIS Settings > General** tab, confirm that the site has the following **Interface Settings** properties:
 - **Site Has ADT Interface** enabled
 - **Site Has Orders Interface** enabled

NOTE:
HIS Orders Interface Option is required for Holter orders. If this option is not enabled and was purchased as part of the CardioDay implementation, be sure to coordinate with the HL7 engineer for implementation and activation.
4. Click **OK**.

Creating the CardioDay Acquisition Profile on the MUSE System

1. From within the MUSE application, go to **Setup**.
2. Select **Acquisition Profile**.
The list of existing acquisition profiles will be displayed. If this is the first acquisition profile, the list will be empty.
3. Right-click on the right side of the screen and choose **New**.
4. Complete the fields using the following table.

Field	Value
Name	Type a descriptive name, such as Site0001-Loc 12-CardioDay Holter.
Test Type	Select Holter from the drop-down list.
Site	Select the MUSE site pre-determined in "Determining MUSE eDoc Connect Parameters" on page 153 .
Location	Select or browse to the MUSE share location pre-determined in "Determining MUSE eDoc Connect Parameters" on page 153 , and in the "Setting Up the CardioDay Share Folder in the MUSE System" on page 157
Profile	Click Import , browse to <code><MUSE_INSTALL_PATH\AcquisitionProfiles\CardioDay Acquisition Profile.xml></code> , and click Open .

5. Click **OK**.

Setting Up the CardioDay Share Folder in the MUSE System

1. From within the MUSE application, go to **Setup**.
2. Select **Share Folder**.
The list of existing share folders is displayed.
3. Right-click on the right side of the screen and select **New**.

4. Complete the fields using the following table as a guide.

Field	Description
Entry	Enter the MUSE Share Folder name predetermined in "Determining MUSE eDoc Connect Parameters" on page 153.
File Name Filter	Enter *.txt .
Profile Name	Select the Acquisition Profile that you created in "Creating the CardioDay Acquisition Profile on the MUSE System" on page 157

5. Click **OK**.

Creating a Dedicated MUSE User Account for CardioDay Holter Orders Query

Create a new User and Password to be used by CardioDay to query the MUSEAPI3 Orders Interface. Enable this user for all sites which will use the Holter Orders Query.

1. From within the MUSE application, go to **Setup**.
2. Select **User Properties**.
3. Complete the fields as indicated in the following table.

Field	Description
Last Name	Type an appropriate user name, such as CardioDay .
First Name	Type an appropriate user name, such as OrdersAccount .
MUSE User Name	Type the appropriate MUSE user name to allow access to the system when logging in with MUSE authentication such as CardioDayOrders .
MUSE Password	Type a password with a maximum of 15 characters. Characters can be alpha or numeric.
Re-enter MUSE Password	Retype the same password as you entered in the MUSE Password field.
Account is Enabled	Check this box to enable sites to use the CardioDay Holter Orders Query.
User cannot change password	Check this box to block users from changing the MUSE password.
Password never expires	user never expires and does not have to be changed.

4. In the **Active Sites** panel, select all the sites that will be using the Holter Orders Query.

5. On the **User > Advanced** tab, assign a unique **User ID** and the role of **MUSE Service**.
6. Click **OK**.

Configuring the CardioDay System for MUSE Holter Orders

CardioDay needs to be configured to Query Holter Orders from the MUSE System via the MUSEAPI3.1 or later interface. For more information about this configuration, see "Configuring MUSE connectivity > Configuring MUSE Orders" section of the CardioDay V2.5 Installation and Field Service Manual.

Configuring the CardioDay System to Export Holter Reports to the MUSE System

CardioDay needs to be configured to export data in the MUSE compatible format to the Share Folder configured in "[Setting Up the CardioDay Share Folder in the MUSE System](#)" on page 157. For more information about this configuration, see the "Configuring MUSE connectivity > Configuring MUSE Export" section of the CardioDay V2.5 Installation and Field Service Manual.

Disabling the eDoc Connect Option

If the customer has not purchased the **eDoc Connect** option, it must be disabled after the CardioDay to MUSE Communication has been configured and tested. Perform the following steps to disable the **eDoc Connect** option.

NOTE:

This procedure may only be performed by a qualified GE Healthcare service representative.

1. Log on to the MUSE application server as a system administrator.
2. Perform a full or partial shutdown of the MUSE system.
Use the shutdown procedures in "AutoShutdown" in the MUSE Cardiology Information System Service Manual.
3. From the Windows **Control Panel**, go to **Programs and Features**.
4. Select **MUSE 9** and click **Change**.
The **Welcome** window opens.
5. Select **Modify** and click **Next**.
The **Select Feature** window opens.
6. Continue to click **Next** on each window until you reach the **Choose MUSE Options** window.
7. Uncheck the **eDoc Connect** option.
8. Click **Next**.
The **MUSE Serial Number** window opens.
9. Enter the **Options Configuration Password**.
If you do not know the password, contact GE Healthcare Technical Support.

10. Click **Next** until your changes are applied and the **Maintenance Complete** window opens.
11. Click **Finish**.

CardioDay / MUSE System Checkout

Complete the following procedures to ensure that the CardioDay system can query the MUSE system for open Holter Orders and MUSE system can successfully acquire CardioDay exported Holter Reports.

CardioDay Holter Report Export to MUSE Checkout

1. Export a CardioDay Holter report to the Shared Folder defined in the MUSE system.
2. Log on to the MUSE System.
3. Verify the CardioDay Holter report is displayed in the MUSE system **Edit List** for the appropriate site.
4. Verify the CardioDay Holter report can be opened in the **MUSE Editor** and is for the appropriate site.

For more information about the usage and checkout of CardioDay report export to the MUSE system, see "Exporting Reports to MUSE" in CardioDay V2.5 Installation and Field Service Manual.

MUSE Order Option Checkout

For more information about the CardioDay MUSE Orders usage and checkout, see the "Importing MUSE Orders" section of the CardioDay V2.5 Installation and Field Service Manual.

Troubleshooting

Holter report data from the CardioDay system to the MUSE system and when using the CardioDay MUSE Order Option.

Troubleshooting the CardioDay Holter Report Export to the MUSE System

For information on troubleshooting the CardioDay Holter Report export to the MUSE system, see ["Troubleshooting" on page 79](#).

Troubleshooting the CardioDay MUSE Order Option and eDoc Connect

Use the following table to assist you in troubleshooting the CardioDay MUSE Order Option and eDoc Connect.

Trouble Indicators	Cause	Recommendation
MUSE Connection Test failure during setup.	Wrong hostname or IP address.	Confirm proper hostname and/or IP address of the MUSE System.
Query Orders button missing from Add Patient tab.	Hostname to IP address lookup (DNS) not functioning.	Confirm hostname resolution/ lookup is working on iOS device. Try entering the IP address of the MUSE system in the URL.
	Wrong IP Port used for MUSE MUSEAPI3.	The proper listening IP PORT number of the MUSEAPI3 service (default 8100) must be included as part of URL configuration.
	MUSE MUSEAPI3 service is not running.	Confirm with MUSE administrator or GE Healthcare service representative that the MUSE MUSEAPI3 service is configured properly and is running without errors.
	User name or password is not a valid MUSE user.	Confirm that the configured User Name and Password match that of a valid MUSE user.
	Other network communication fault or port blocking.	Check for other network communication faults, restrictions, and firewalls.
	Improper Site Number in configuration.	Confirm the presence of MUSE orders with the proper Site Number.
No MUSE patient/exam orders displayed in Order List .	No Holter orders with Open order status.	Confirm the presence of MUSE order using: TestType=Holter Status=OPEN

Trouble Indicators	Cause	Recommendation
Document imported with incorrect acquisition profile.	An electronic document was copied to an incorrect folder or bulk acquired using the wrong acquisition profile. If this happens then it is most likely acquired with incorrect attributes (test type, site, location, etc.).	To correct this, discard the test. Once on the Discarded Data List , you can reacquire the electronic document using the correct acquisition profile. Right-click on the test on the Discarded Data List , choose Correct Acquisition Profile , and choose the correct acquisition profile with which to re-import the test.
Cannot acquire electronic documents.	The user account that is configured to start the MUSE Generacq service on the MUSE application server does not have access to the folder or share defined for the Share Folder in the MUSE system.	Ensure the user account configured to start the MUSE Generacq service on the MUSE application server has access to the folder or share defined for the Share Folder in the MUSE system.
	The Share Folder is not set up correctly for the location of the electronic document files in MUSE System Setup .	Ensure the Share Folder set up in MUSE System Setup is correctly defined.

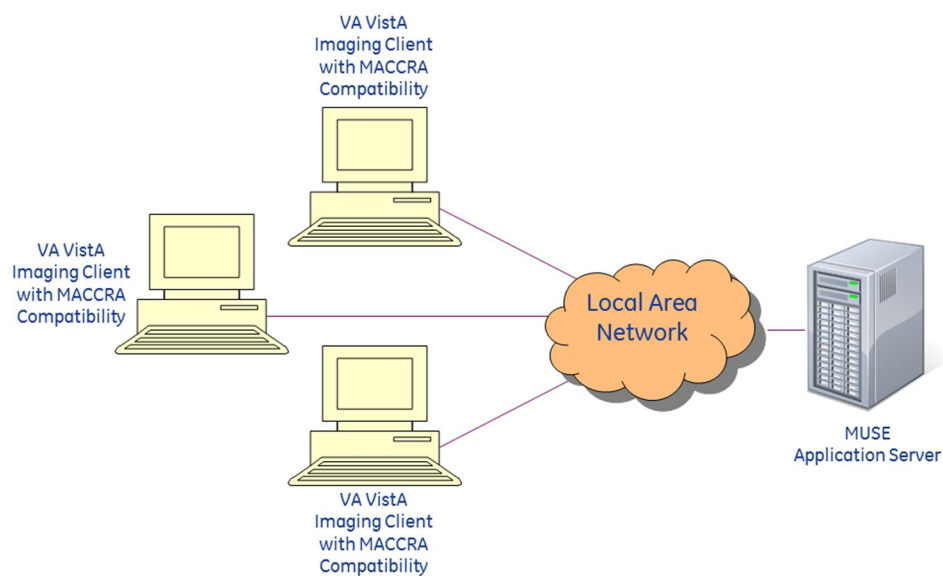
13

MUSE Configuration for VA VistA Imaging

This chapter describes how to configure a MUSE v9 system to allow communication between the MUSE system and VA VistA Imaging systems.

Theory of Operation

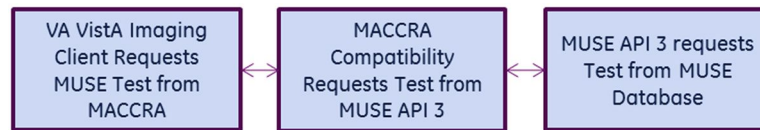
Vista Imaging is the software the US Veterans Administration (VA) hospitals use to interface with the MUSE system. Vista Imaging requires MUSEAPI3 and MACCRA Compatibility to operate. Installation of the MUSEAPI3 components at VA facilities must be closely coordinated with the local IT department, since it requires installation of MACCRA Compatibility and the Vista Imaging client as well as any appropriate Vista Imaging client patches or setup. GE Healthcare service personnel are responsible for installing the MUSEAPI3 on the MUSE v9 system. The VA hospital is responsible for installing MACCRA Compatibility and the VA Vista Imaging client software on the VA Vista Imaging client computers.



Example Network Diagram

Information Transmission

The VA VistA Imaging Client requests test information from MACCRA. MACCRA Compatibility, installed on the VA VistA client, sends that request to the MUSEAPI3 service running on the MUSE application server, which requests the test information from the MUSE database. The results of the request are then sent back through MACCRA Compatibility to the VA VistA Imaging Client.



Transmission Flow Chart

Customer Requirements

The customer is responsible for supplying the following:

- Network connectivity between the VA VistA Imaging clients and the MUSE application server
- Installation of the MACCRA Compatibility component on each VA VistA Imaging Client

Process Overview

The process of configuring the MUSE system for VA VistA Imaging Clients consists of the following high-level tasks:

- [“Configuring the VOL000 Share” on page 164](#)
- [“Configuring VA VistA Imaging Formats” on page 165](#)
- [“Installing MUSEAPI3” on page 167](#)
- [“Installing MACCRA Compatibility” on page 167](#)

Configuring the VOL000 Share

As required by the VistA Imaging software, the interface requires a VOL000 share on the MUSE server. Use the following procedure to configure the VOL000 share.

1. Create a **\VOL000** folder on the MUSE application server.
Following normal conventions, create it on the partition where the database resides. No files are required in the folder.
2. Share the folder as **VOL000**, assigning **Full Control** file and share permissions to the **MUSE Web Users** group.
3. Add the **Imaging IU** accounts that will be accessing the MUSE system from VA VistA Imaging clients to the **MUSE Web Users** group on the MUSE application server.

The accounts should follow this format: **VHAxxx\VHAxxxIU**, where xxx is a standard 3-character code for the site.

You may add more than one IU account to the **MUSE Web Users** group if multiple remote sites access the MUSE application server.

4. If the **Everyone** group is listed with share permissions, remove it.

Configuring VA VistA Imaging Formats

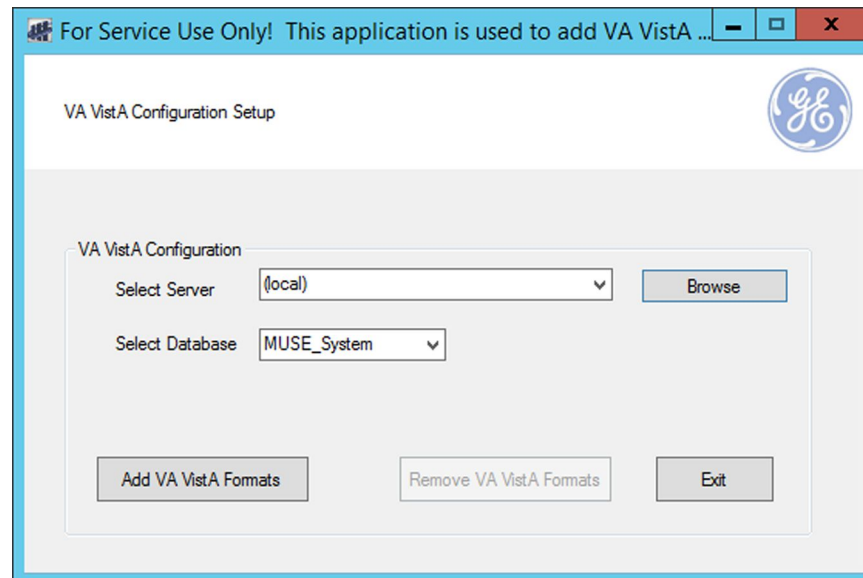
The VA VistA Imaging interface to MUSE v9 systems uses the MUSE system's format settings to determine the format for each of the four data types (ECG, HiRes, Stress, and Holter).

The VA VistA Configuration Utility automatically creates new VistA specific format settings in the MUSE system and updates the **cfgDeviceFormats** table in the **MUSE_System** database to set device ID 5 to the newly created format settings.

Use the following procedure to run the configuration utility for VA VistA.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Run **VAVistAConfig.exe** from the MUSE application installation folder. The default location is **C:\Program Files (x86)\MUSE** for a 64-bit OS, and **C:\Program Files\MUSE** for a 32-bit system.

The **VA VistA Configuration Setup** program opens.



The **Select Server** field defaults to **(local)**.

The **(local)** setting means that the MUSE database resides on the same server as the MUSE application. If the database is local, skip to step 4.

3. If the database is on a remote server, click **Browse** or type the name of the SQL Server where the MUSE databases are located.

If the MUSE 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 the SQL Server, include the instance name. For example, if the databases are located on SQLSERVER1 on a named instance called MUSE, browse to or type: SQLSERVER1\MUSE.

4. Verify **MUSE_System** is selected from the **Select Database** drop-down list.
The default is **MUSE_System** and normally does not need to be changed.
5. Click **Add VA VistA Formats**.
If this button is grayed out, they were already added.
6. Click **Exit**.
7. In the MUSE system, go to **System>Setup**.
8. Select **Formats** and verify that the four new formats were added: **VistA ECG**, **VistA HiRes**, **VistA Stress**, and **VistA Holter**.

NOTE:

If you need to remove the new formats, repeat this procedure but click the **Remove VA VistA Formats** button in step 5 instead of **Add VA VistA Formats**.

The following tables list of the format settings that are created by the VA VistA Configuration Utility for reference.

VistA ECG and VistA HiRes Format Settings

Setting	Value
General Settings	
Display Barcode	Disabled
Grid Type	No Grid
Fonts Settings	
Title Font	Helvetica
Primary Font	Helvetica
Diagnosis Font	Helvetica
Diagnosis Font Size	3.5 mm
All other settings	
Default	

VistA Stress Format Settings

Setting	Value
General Settings	
Display Barcode	Disabled
Grid Type	No Grid
Fonts Settings	
Title Font	Helvetica
Primary Font	Helvetica
Diagnosis Font	Helvetica

VistA Stress Format Settings (cont'd.)

Setting	Value
Diagnosis Font Size	3.5 mm
Stress Specific Settings	
Graded Exercise Summary	Enabled
Trend & Medians Report	Enabled
Selected Medians Report	Enabled
ST Slope Info	Enabled
All other settings	
Default	

VistA Holter Format Settings

Setting	Value
General Settings	
Display Barcode	Disabled
Grid Type	No Grid
Fonts Settings	
Title Font	Helvetica
Primary Font	Helvetica
Diagnosis Font	Helvetica
Diagnosis Font Size	3.5 mm
Holter Specific Settings	
Cover Page	Enabled
Strip Pages	Enabled
All other settings	
Default	

Installing MUSEAPI3

If it is not already installed, install MUSEAPI3 on the MUSE application server. See [Chapter 9 “MUSEAPI3 Installation” on page 105](#) for installation instructions.

Installing MACCRA Compatibility

MACCRA Compatibility must be installed as a Library application on each VA VistA imaging workstation that needs access to the MUSE database. See [Chapter 11 “MACCRA Compatibility” on page 139](#) for instructions on installing MACCRA Compatibility.

System Checkout

The customer is responsible for performing the system checkout on the VA VistA Imaging interface. Using the following instructions, the customer verifies that the MACCRA Compatibility Layer can communicate with the MUSEAPI3 and the MUSE database. The customer can run these procedures wherever the MACCRA Compatibility Library application is installed.

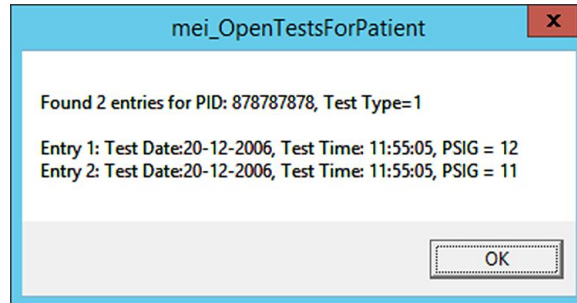
Creating Enhanced Metafile Using MUSE API DCOM Tester

1. Log on to the system where MACCRA Compatibility is installed.
2. Insert the MUSE v9 installation media into the optical drive of the system.
If any **Autorun** or **AutoPlay** screens appear, close or cancel them.
3. Browse the optical drive in Windows Explorer and perform one of the following:
 - If the MUSE v9 Application and Support DVD is inserted, navigate to the **\MUSE Support\MUSE API DCOM** folder.
 - If the MUSE v9 Support ISO is being used, navigate to **\MUSE API DCOM** folder.
4. Run **MUSEAPI DCOM Tester.exe**.
5. Go to **API Functions > 1. mei_OpenMUSE**.
The **mei_OpenMUSE()** dialog box opens.

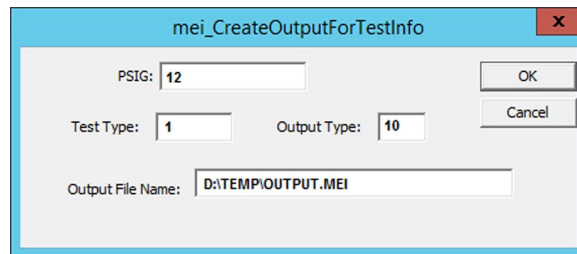
6. Enter a valid MUSE site number and click **OK**.
7. Verify the message **Operation Succeeded** is displayed.
8. Click **OK**.
9. Go to **API Functions > 3. mei_TestsForPatient**.
The **TestsForPatient** window opens.

10. Identify a patient that has a valid Patient ID and who has an ECG test for the MUSE site you selected in step 6. Enter this patient's ID into the **Patient ID** field. Accept the default values for all other fields.

11. Click **OK**.
12. Verify you get a message dialog that indicates the number of tests found and their associated entries.



13. Write down the PSIG for one of the entries.
14. Click **OK**.
15. Go to **API Functions > 5. Mei_CreateOutputForTestInfo**.
The **mei_CreateOutputForTestInfo** window opens.

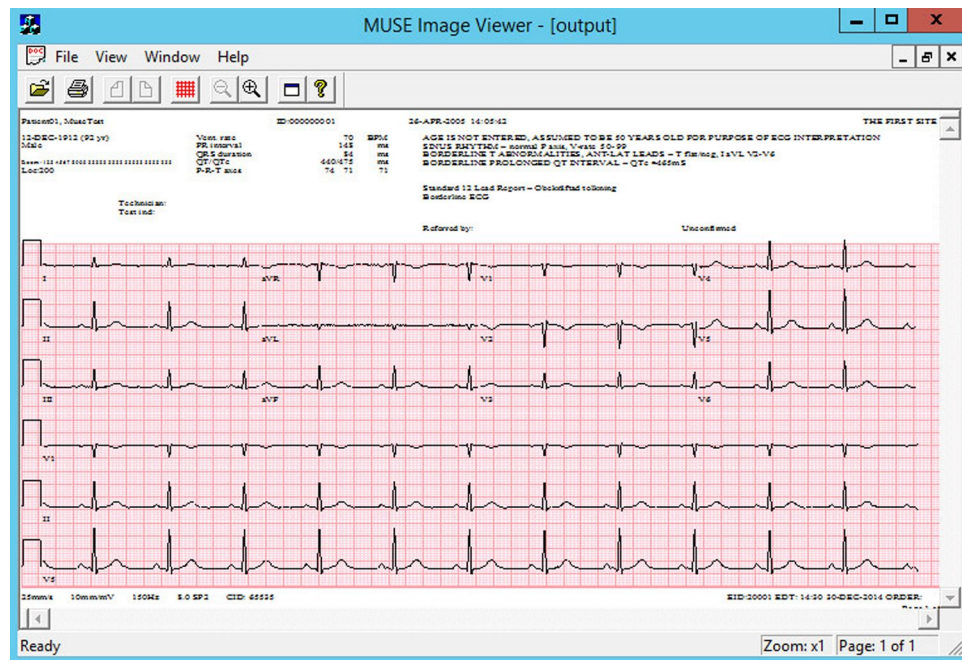


16. In the **PSIG** field, enter the PSIG you wrote down in step 13.
17. Verify the **Test Type** is 1 and the **Output Type** is 10.
18. In the **Output File Name**, type in a path and filename with the MEI extension.
The specified path must be a valid, pre-existing path.
19. Click **OK**.
The output file is created.
20. Verify the message **Output saved in file...** is displayed.
21. Click **OK**.
22. Verify the output file was created in the location and with the name specified in step 18.

Viewing Enhanced Metafile Using MUSE Image Viewer

1. Log on to the system where MACCRA Compatibility is installed.
2. Insert the MUSE v9 installation media into the optical drive of the system.
If any **Autorun** or **AutoPlay** screens appear, close or cancel them.

3. Browse the optical drive in Windows Explorer and perform one of the following:
 - If the MUSE v9 Application and Support DVD is inserted, navigate to the **MUSE Support\MUSE API DCOM** folder.
 - If the MUSE v9 Support ISO is being used, navigate to **MUSE API DCOM** folder.
4. Run **imgview.exe**.
The **MUSE Image Viewer** application opens.
5. Go to **File>Open**. Open the file created by the MUSE API DICOM Tester.
6. Verify the test file can be viewed.





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, Inc.*, a General Electric Company, going to market as GE Healthcare.

www.gehealthcare.com

