GE Healthcare

MUSE™ DICOM Gateway Pro
Service Manual
2059568-058 Revision J

MUSE DICOM Gateway Pro
English

Publication Information

The information in this document applies only to MUSE ™DICOM Gateway Pro system. It does not apply to earlier product versions. Due to continuing product innovation, specifications in this document are subject to change without notice.

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	April 27, 2015	Initial release.
B	17 July 2015	Customer release.
C	10 September 2015	Added regulatory information in product overview section.
D	19 October 2015	Updates to the section "Configure the Outbound DICOM Device(s) in the System."
E	10 November 2015	Updated the System Configuration chapter with Site properties screen and added Setting Up Sites — HIS Settings section.
F	24 May 2016	Updated the Configure the System DICOM Modality Worklist Client Service section.
G	1 December 2016	Updated to support HCSDM00433985.
H	12 September 2017	Updated to support HCSDM00468531, HCSDM00468530, and HCSDM00468529,
J	23 February 2018	Updated to support HCSDM00485912 and HCSDM00486327.

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 DICOM Gateway Pro 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 DICOM Gateway Pro system if you are not part of the intended audience or have not read and understood these instructions in their entirety.

The MUSE DICOM Gateway Pro 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.

NOTE:

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

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

Service Manual Language Information

WARNING (EN)	This service manual is available in English only. • 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)	Това упътване за работа е налично само на английски език. • 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)	本维修手册仅提供英文版本。 • 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)	本維修手冊只提供英文版。 • 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)	Ove upute za servisiranje dostupne su samo na engleskom jeziku. • 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)	Tento provozní návod existuje pouze v anglickém jazyce. • 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)	Denne servicemanual findes kun på engelsk. • 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)	Deze service manual is alleen in het Engels verkrijgbaar. • 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)	Käesolev teenindusjuhend on saadaval ainult inglise keeles. • 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)	Tämä huolto-ohje on saatavilla vain englanniksi. • 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)	Ce manuel technique n'est disponible qu'en anglais. • 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.)

WARNUNG (DE)	Diese Serviceanleitung ist nur in englischer Sprache verfügbar. • 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.
ΠΡΟΕΙΔΟΠΟΙΗΣΗ (EL)	Το παρόν εγχειρίδιο σέρβις διατίθεται στα αγγλικά μόνο. • 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.
FIGYELMEZTETÉS (HU)	Ez a szerviz kézikönyv kizárólag angol nyelven érhető el. • Ha a vevő szerviz ellátója angoltól eltérő nyelvre tart igényt, akkor a vevő felelőssége a fordítás elkészíttetése. • Ne próbálja elkezdeni 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.
AÐVÖRUN (IS)	Þessi þjónustuhandbók er eingöngu fáanleg á ensku. • Ef að þjónustuveitandi viðskiptamanns þarfnast annars tungumáls en ensku, er það skylda viðskiptamanns að skaffa tungumálaþjónustu. • 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.
PERINGATAN (ID)	Manual servis ini hanya tersedia dalam bahasa Inggris. • 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 kejut listrik, bahaya mekanis atau bahaya lainnya.

Service Manual Language Information (cont'd.)

AVVERTENZA (IT)	Il presente manuale di manutenzione è disponibile soltanto in Inglese. • 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)	このサービスマニュアルは英語版しかありません。 • 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)	Tài Liệu Hướng Dẫn Sửa Chữa chỉ có bản tiếng Anh. • 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)	Бұл қызмет көрсету бойынша нұсқаулығы тек ағылшын тілінде қолжетімді. • 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 елемеу қызмет провайдері, оператор немесе емделушінің электр шогынан, механикалық немесе басқа қауіптер нәтижесінде жарақат алуына әкелуі мүмкін.
BRĪDINĀJUMS (LV)	Šī apkalpotāju rokasgrāmata ir pieejama tikai angļu valodā. • Ja apkalpošanas sniedzējam nepieciešama informācija citā, nevis angļu, 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.
ĮSPĖJIMAS (LT)	Šis eksploatavimo vadovas yra prieinamas tik anglų kalba. • 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)	Denne servicehåndboken finnes bare på engelsk. • 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)	Niniejszy podręcznik serwisowy dostępny jest jedynie w języku angielskim. • 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)	Este manual de assistência técnica só se encontra disponível em inglês. • 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)	Este manual técnico só se encontra disponível em inglês. • 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)	Acest manual de service este disponibil numai în limba engleză. • 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 şi 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)	Настоящее руководство по обслуживанию предлагается только на английском языке. • 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)	Ovo servisno uputstvo je dostupno samo na engleskom jeziku. • 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 servisera, rukovaoca ili pacijenta usled strujnog udara, ili mehaničkih i drugih opasnosti.
VAROVANIE (SK)	Tento návod na obsluhu je k dispozícii len v angličtine. • 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)	Ta servisni priročnik je na voljo samo v angleškem jeziku. • 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)	Este manual de servicio sólo existe en inglés. • 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)	Den här servicehandboken finns bara tillgänglig på engelska. • 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)	Bu servis kılavuzunun sadece İngilizcesi mevcuttur. • 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.)

ЗАСТЕРЕЖЕННЯ (UK)	Дане керівництво з сервісного обслуговування постачається виключно англійською мовою. • 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 невірного обслуговування обладнання.
CẢNH BÁO (VI)	Tài Liệu Hướng Dẫn Sửa Chữa chỉ có bản tiếng Anh. • 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

5 System Status

6 MUSE Monitoring Gateway

C Roles and Privileges

1

Product Overview

This chapter describes the MUSE DICOM Gateway Pro system (also referred to as "the system" throughout this manual). It also defines requirements for installing the system.

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	*MobileLink Installation Manual*
2020299–025	*LAN Option for MAC Installation and Troubleshooting*
2059568–022	*MUSE DICOM Gateway Pro Pre-Installation Manual*
2059568–023	*DICOM Conformance Statement for MUSE v9 and MUSE DICOM Gateway Pro*
2059568–026	*InSite ExC Installation Manual*

Safety Conventions

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

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

Definitions of Safety Conventions

Safety Convention	Definition
DANGER	Indicates an imminent hazard, which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in death or serious injury.

Definitions of Safety Conventions (cont'd.)

Safety Convention	Definition
CAUTION	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in moderate or minor injury.
NOTICE	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in the loss or destruction of property or data.

Safety Hazards

The following safety messages alert you to potentially hazardous conditions that could arise during the normal use of this product and recommend steps that can be taken to avoid those conditions. Safety messages pertaining to hazardous conditions that may arise during specific actions may also be provided during the discussion of those actions in this or other manuals for this product.

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

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

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

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

CAUTION:
LOSS OF DATA: MUSE services may automatically restart after making changes to the installation configurations.

To avoid losing changes to open records, schedule a maintenance downtime with the customer before making changes.

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

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

Prescription Device Statement

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

Product Description

The MUSE DICOM Gateway Pro system is a software-only utility that enables GE Healthcare devices to receive orders from DICOM Modality Worklist Service Class Provider systems and send patient ECG tests to DICOM Storage Service Class Provider systems. Compatible GE Healthcare cardiographs exchange data with the system, and the system translates the received data into DICOM IOD or encapsulated PDF (Portable Document Format) tests that different DICOM systems can accept. The system can also translate orders for ECGs entered in the DICOM system into a format compatible with the cardiograph, eliminating the need to reenter the patient demographics.

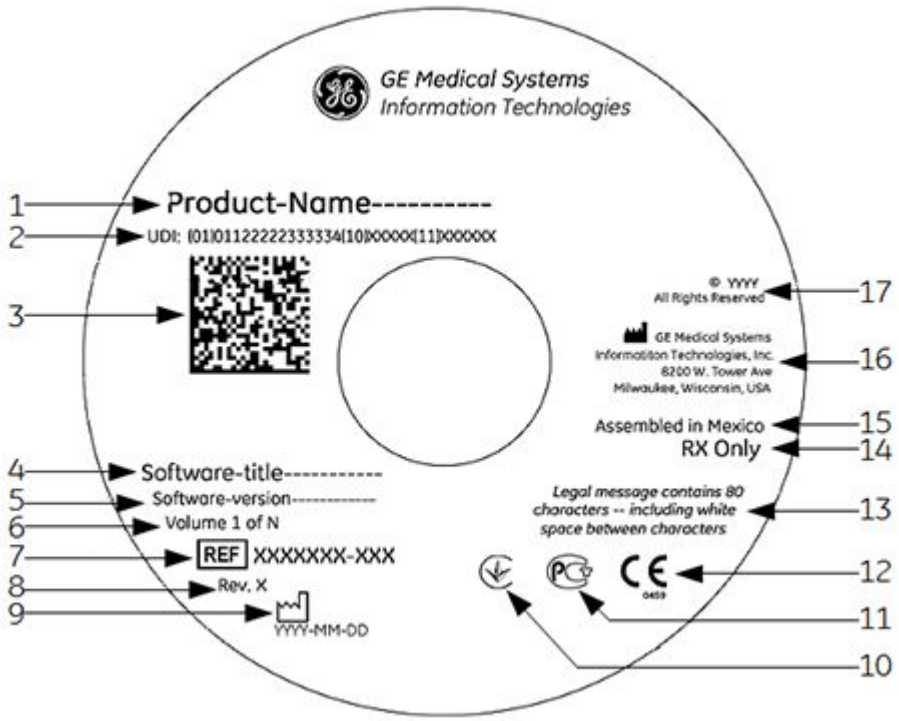
Intended Use

The MUSE DICOM Gateway Pro application is intended to electronically transfer data to and from non-invasive medical acquisition devices (Resting ECG) and a DICOM based Hospital Information system (DMWL and PACS).

The MUSE DICOM Gateway Pro application is not intended to control any functions of the medical device to which it connects, nor is it intended to provide editing capability of diagnostic or demographic information regarding patient data. The MUSE DICOM Gateway Pro has no clinical user interface; its user interface is intended for software administrators and service personnel.

Software Label

The following illustration and table describe the label on your CD or DVD.



Descriptions of the CD/DVD Label

Item	Description
1	**Product Name** Identifies the product brand and model.
2	**UDI** Unique Device Identification required for all medical devices. It consists of the software UDI plus the CD/DVD production date. It is required when reporting a damaged or defective disk.
3	**2D Barcode** Machine-readable representation of the UDI.
4	**Software Title** Identifies the contents of the CD/DVD.
5	**Software Version** Identifies the software version.
6	**Volume Number** Identifies the disk sequence when more than one CD/DVD is required.
7	**Part Number** Identifies the orderable part number of the CD/DVD.
8	**Revision** Identifies the revision level of the CD/DVD.
9	**Date of Manufacture** Identifies the date the CD/DVD was produced in `YYYY-MM-DD` format.
10	**Ukraine registration** Indicate compliance with applicable requirements for export to Ukraine.
11	**GOST-R Mark** Indicates compliance with applicable requirements for export to Russia.
12	**CE Mark** Indicates compliance with applicable EU (European Union) directives.
13	**Legal message** Identifies any legal notices or disclaimers.
14	**Prescription Device Statement** Indicates U.S. federal law restricts the device to sale by, or on the order of, a physician
15	**Country of Origin** Identifies the country in which the CD/DVD was produced. Blank if it is produced in the USA.
16	**Manufacturer's Name and Address** Identifies legal name and address of the manufacturer.
17	**Copyright Notice** Identifies the copyright year and the extent of rights reserved.

System requirements

This section describes the hardware and software requirements for installing the system and the required network ports.

Hardware Requirements

The hardware used for the system must meet the hardware requirements described in the *MUSE DICOM Gateway Pro Pre-Installation Guide*.

Software Requirements

The operating system for the system must meet the software requirements described in the *MUSE DICOM Gateway Pro Pre-Installation Guide*.

If you are installing the system database on a separate server, the customer must have the appropriate version of SQL Server Management Studio installed on the system application server. See "Verifying SQL Server Management Tools are Installed" on page 25 for more information.

WARNING:

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

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

Required Network Ports

Refer to the *MUSE DICOM Gateway Pro Pre-Installation Guide* for required network port information.

Antivirus Software

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

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

The real-time antivirus software installed on your system should be able to be disabled during the installation of the application server.

Additionally, GE Healthcare reserves the right to request:

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

Security Updates

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

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

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

1. Browse to the GE Healthcare Product Security website:

   http://prodsecdb.gehealthcare.com

   The ***Single Sign On (SSO)*** window opens.

2. Enter your SSO number and password and click ***Log In***.

   If you do not have an SSO number, click the ***Sign Up*** link to obtain one.

3. Use the features on the GE Healthcare Product Security Database Website to identify security patches that you can apply to your system.

2

Preparing System Application and Database Servers

Before beginning the system installation, complete the following tasks:

Verifying Potential SQL Issues with Local Database Administrator

If you are installing the system database on a separate server, verify with the local Database Administrator (DBA) the following items:

- SQL Server is installed on the database server prior to starting the system installation.
- If the system database is being installed on a named instance of SQL, the instance was created.
- SQL Server is configured to allow remote connections from the system application server.
- SQL Server Management Tools are installed on the system application server.

NOTE:
Refer to the *MUSE DICOM Gateway Pro Pre-Installation Guide* for complete SQL server requirement information.

Setting Up MUSE Service Users

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

Account	MUSE System User Name	Description
MUSE Administrator	***MuseAdmin***	The MUSE Administrator account is used by GE Healthcare service personnel to log into the system to perform initial setup and configuration, and to provide ongoing service and support.
MUSE Background	***MuseBkgnd***	The MUSE Background account is used to start the system-related background services on the system application server.

These service users and the user running the system InstallShield wizard must have their Windows and SQL permissions configured according to the information in Appendix A "MUSE Service Users" on page 133.

Creation and configuration of the MUSE service users is the responsibility of the customer. Confirm all service user requirements are met prior to beginning the installation of the system software.

Verifying Hardware and Operating System Requirements

Verify that the site's system meets the hardware and operating system requirements to install the system. For the required specifications for both the hardware and operating system, refer to the *MUSE DICOM Gateway Pro Pre-Installation Guide*. Also, use the instructions in the following table to qualify if your system meets the requirements.

Required Information	How to Locate the Information
CPU Cores	Use ***Windows Device Manager*** > ***Processors*** to determine the number of cores. A separate processor is listed for each core.
CPU Speed	Use ***Windows System Properties*** to determine CPU Speed, RAM Memory, and Operating System.
RAM Memory	
Operating System	
Available Disk Space	Use ***Windows Explorer*** to determine available disk space. **NOTE:** When installing the system database, use the drive with the most available disk space.

If any of the prior items do not meet the requirements as documented in the *MUSE DICOM Gateway Pro Pre-installation Guide*, work with the customer to ensure the hardware where the system is being installed meets the requirements before proceeding with the installation or upgrade.

Verifying SQL Server Management Tools are Installed

SQL Server Management Tools, including SQL Server Management Studio, must be installed on the system application server. These are installed with SQL server. If the SQL database resides on the system application server, these management components should already be installed. If the SQL database is located on a different server, you need to install these components on the system application server. These tools are extremely important to ensure that GE Healthcare service has access to the system database from the application server.

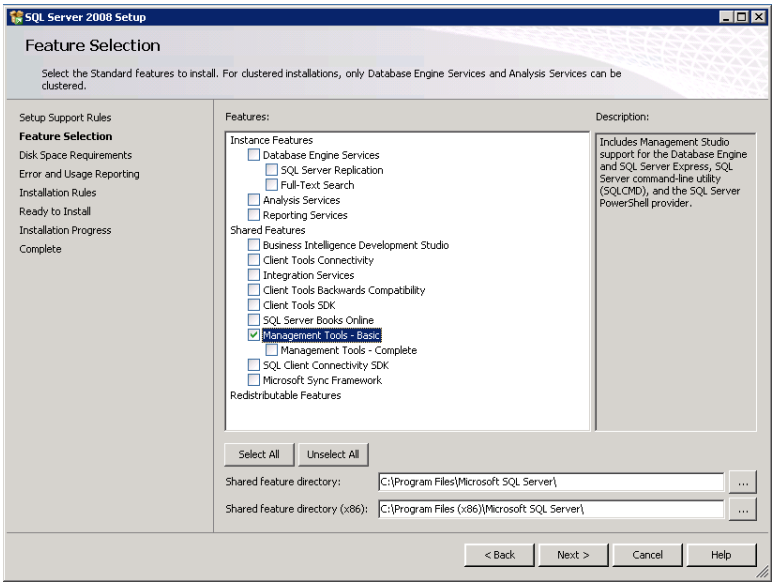
These tools are extremely important to ensure that GE Healthcare service has access to the system database from the application server.

To verify that the SQL Management Tools are installed, use the following procedure:

1. Log in to the system application server as the MUSE Administrator or MUSE Background user.
2. From Windows ***Desktop Search***, search for ***SQL Server Management Studio***.
3. Verify the ***SQL Server Management Studio*** is found.

   If you cannot find ***SQL Server Management Studio***, contact the local IT or DB administrator and ask them to add these components to the system application server. This may require running the SQL installer on the system application server.

   In the SQL installer, select ***Management Tools – Basic*** under the ***Shared Features***.



Verifying SQL Server Logins and Server Role(s) for MUSE Administrator and MUSE Background Users

Perform the following to verify that the SQL Server logins for the ***MUSE Administrator*** and the ***MUSE Background*** user exist and have the appropriate server roles assigned to them.

1. Log on to the system application server as the ***MUSE Administrator***.
2. From the ***SQL Server Management Studio***, log in to the SQL Server instance where the system databases are installed.

   NOTE:
   Use the same user ID to log in to SQL Server as you did to log on to Windows.
3. In ***Object Explorer***, expand the database server.
4. Navigate to and expand ***Security*** > ***Logins***.
5. Right-click on the ***SQL Login*** for the MUSE Administrator user and choose ***Properties***.
6. Select the ***Server Roles*** page.
7. Verify the user has the appropriate server role(s) assigned.

   Use the following table as a reference.

User	SQL Server Role(s)
MUSE Administrator	***public*** and ***sysadmin*** (typical for local database) or ***public*** (minimum; typical for remote database)
MUSE Background	***public*** and ***sysadmin*** (typical for local database) or ***public*** and ***dbcreator*** (minimum; typical for remote database)

8. Verify that the user is assigned the appropriate server role(s).

   Use the following table as a guide.

User	SQL Server Role(s)
MUSE Administrator	***public*** and ***sysadmin*** (typical for local database) or ***public*** (minimum; typical for remote database)
MUSE Background	***public*** and ***sysadmin*** (typical for local database) or ***public*** and ***dbcreator*** (minimum; typical for remote database)

9. Repeat steps 1 through 7 for the MUSE ***MUSE Background*** Windows user.

   If the SQL server role(s) cannot be verify for either or both the ***MUSE Administrator*** login and the ***MUSE Background*** login, the customer SQL administrator needs to assign the roles. See Appendix A "MUSE Service Users" on page 133 for more information about the SQL server role requirements.

10. Click ***OK***.

Verifying the SQL Service Pack

Confirm the SQL Server version and service pack using the following the procedure.

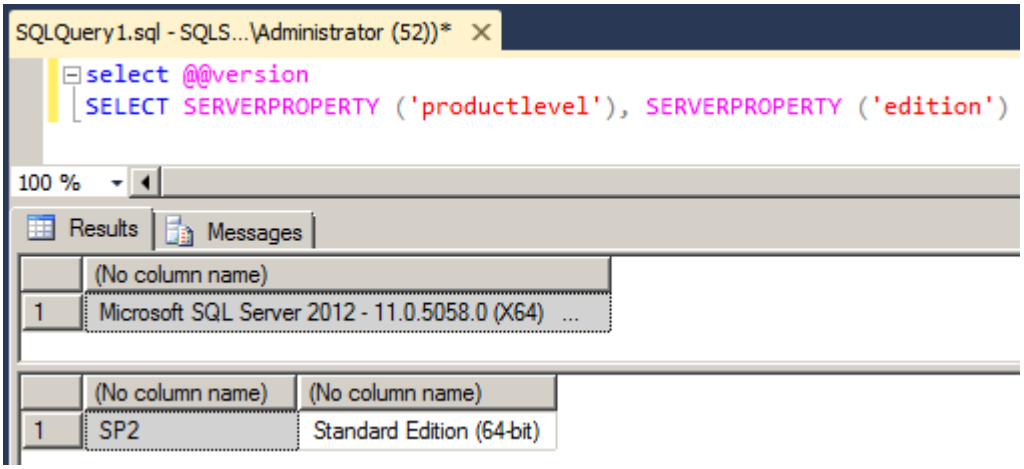
1. Log on to the system application server as the ***MUSE Administrator*** user.
2. Launch ***SQL Server Management Studio*** and login to the SQL Server instance where the MUSE databases will be installed or upgraded.
3. Click ***New Query*** and execute the following query:

   ```
   select @@version
   ```

   ```
   SELECT SERVERPROPERTY ('productlevel'), SERVERPROPERTY
   ('edition')
   ```

   This provides the SQL version, service pack, and whether it is 32-bit or 64-bit.
4. Verify that one of the following SQL versions and latest service pack is installed.
   - SQL Server 2008 (SP4) (32/64–bit)
   - SQL Server 2008 R2 (SP3) (32/64–bit)

- SQL Server 2012 (SP2) (64-bit)
- SQL Server 2014 (RTM) (64-bit)



NOTE:
The service packs listed were the current ones in effect at the time of publication. For later service packs, refer to the GE Healthcare Security Web site or contact GE Healthcare Technical Support to determine if the service pack has been tested and can be used with the system.

5. From within SQL Server Management Studio, go to ***Help*** > ***About*** and verify the SQL Server Management Studio version is the same or greater than the version of the database engine identified in step 4.

NOTE:
If the version of SQL Server Management Studio is not the same or greater than the SQL Server database engine, do not proceed with the system installation or upgrade. Install a newer version of SQL Server Management Studio.

SQL Native Client 11

MUSE v9 SP5 and later require SQL Native Client 11 Provider to communicate with the MUSE database. Perform the following steps to download and install SQL Native Client 11 Provider if necessary.

NOTE:
If the MUSE application server is SQL Server 2012 or later, it should already have SQL Native Client 11 installed. Use step 5 below to verify whether it is installed.

1. Navigate to the following URL: https://www.microsoft.com/en-us/download/details.aspx?id=29065.
2. After loading this page, expand ***Install Instructions*** and look for ***Microsoft SQL Server 2012 Native Client***.
3. Download the appropriate package (x86 for 32–bit OS or x64 for 64–bit OS).
4. Install the downloaded package.
5. Verify ***Microsoft SQL Server 2012 Native Client*** is installed in ***Windows Programs and Features***.

Copying the MUSE DICOM Gateway Pro Software Files

Copy the complete contents of the MUSE DICOM Gateway Pro software discs (with a subfolder that includes the part number of the media for each disc) to a folder such as ***\MUSE_DICOM_Gateway_Pro_Software*** off the root directory of a drive on the system application server. This makes the system software easily available to the service engineers if needed.

3

Installation

This chapter describes how to install the MUSE DICOM Gateway Pro application and database, and InSite ExC. It also explains how to uninstall the MUSE DICOM Gateway Pro application.

Installing the MUSE DICOM Gateway Pro Application and Database

Always run the installer from the system application server, regardless of where the database resides. The installer is designed to locate and remotely install the database from the application server.

If necessary, contact the local Database Administrator (DBA) and request the name of the database server, the SQL instance (if not the default instance), and the port being used. The DBA must ensure that these are accessible from the MUSE application server before starting the installation.

The installation can be canceled by clicking the ***Cancel*** button during the installation. Once the Cancel button has been clicked, you must click ***Yes*** to confirm the cancellation and then ***Finish*** to close the InstallShield Wizard.

If an error or warnings are encountered during the installation process, see "System Application Server Installation Troubleshooting" on page 41.

NOTE:
MUSEAPI3 setup will be launched automatically after the Muse DICOM Gateway Pro installation finishes.

1. Log on to the system application server using an account that has ***administrator*** privileges on the system application server and ***sysadmin*** server role privileges to the SQL Server instance where the system databases will reside.

   See Appendix A "MUSE Service Users" on page 133 for more information about SQL permissions requirements for the system.

2. Disable any antivirus software during the installation.

   You may have to ask the customer to disable the antivirus software

   The antivirus software should be enabled after the installation is complete.

3. Insert or mount the MUSE DICOM Gateway Pro installation media into the optical drive.

   If any ***Autorun*** or ***AutoPlay*** screens appear, close or cancel them.

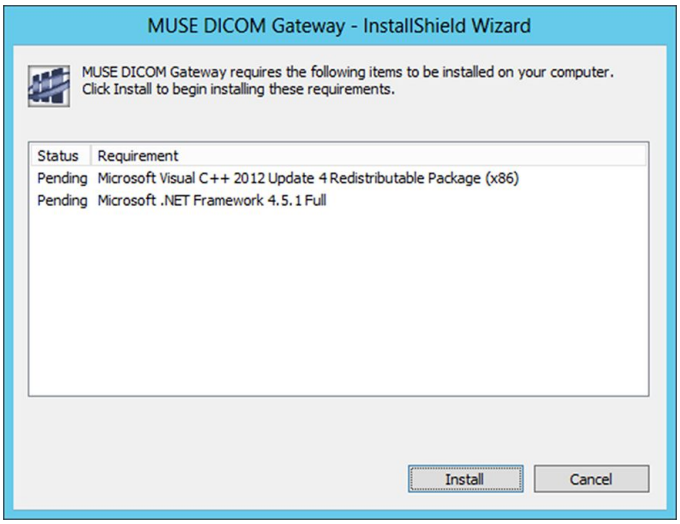
4. Browse to the ***MUSEDICOMGatewaySetup*** folder on the media and run ***Setup.exe***.

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

5. Perform one of the following steps:

   - If the requirement installer window opens that the following message, ***MUSE DICOM Gatewway requires the following items be installed on your computer***, proceed to step 6.
   - If the ***Welcome to the InstallShield Wizard for MUSE DICOM Gateway*** window opens, proceed to step 7.

6. When the requirements installer window opens, click ***Install***.

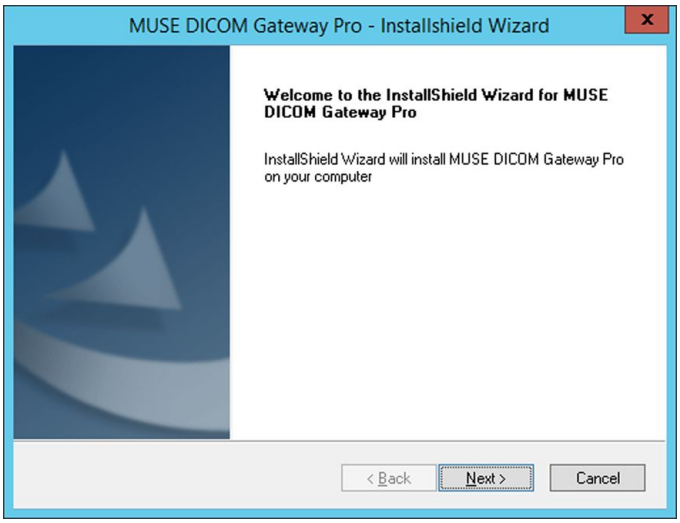


   The required software installs.

   The system may restart automatically during the installation of the required software. If the system automatically restarts, repeat these installation steps starting from step 1 when the system completes the restart.

   If Microsoft .NET Framework 4.5.1 opens the following prompt, ***Do you want Setup to close your programs?***, click ***Yes***.

The ***Welcome to the Installshield Wizard for MUSE DICOM Gateway*** window opens.



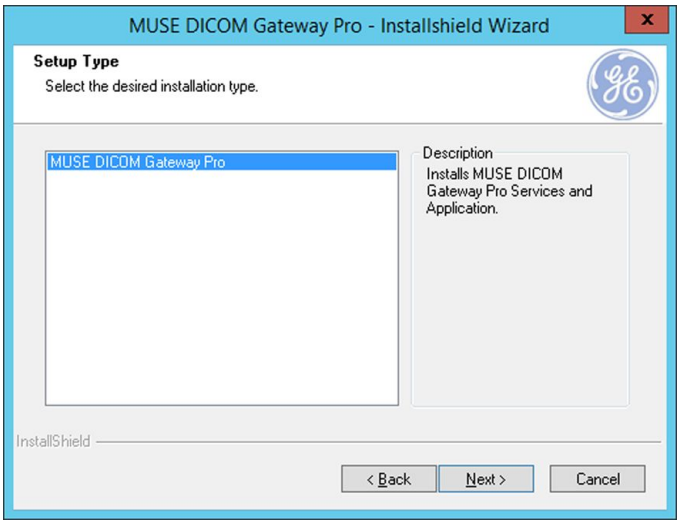
7. Click ***Next***.

   The ***License Agreement*** window opens.

8. Read the license agreement and then select the radio button for ***I accept the terms of the license agreement***.

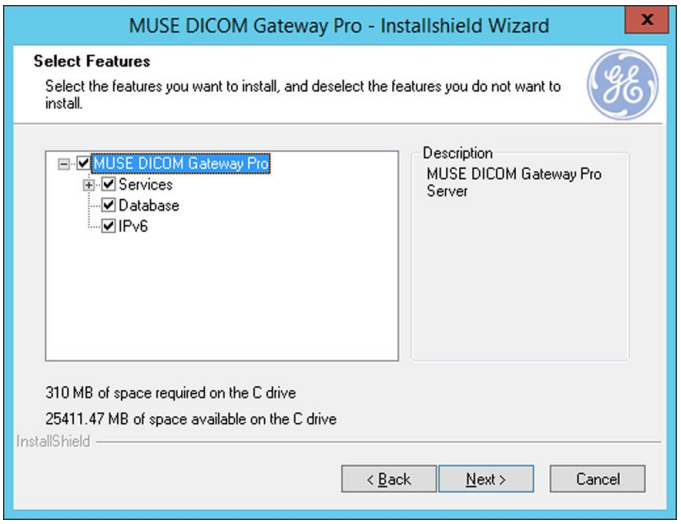
9. Click ***Next***.

   The ***Setup Type*** window opens.



10. Select ***MUSE DICOM Gateway Pro*** and click ***Next***.

    The ***Select Features*** window opens.

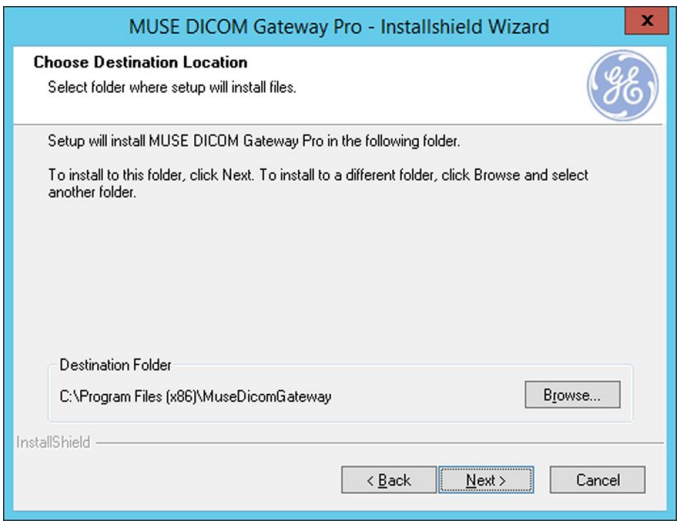


11. Select ***Services*** and confirm all the boxes are selected.
12. Confirm that the ***Database*** option is selected.
13. Select ***IPv6*** to confirm Middle Tier Communication.

    NOTE:
    Microsoft automatically enables IPv6 in Windows Server 2008 and newer. Enabling it here ensures compatibility.

14. Click ***Next***.

    The ***Choose Destination Location*** window opens.

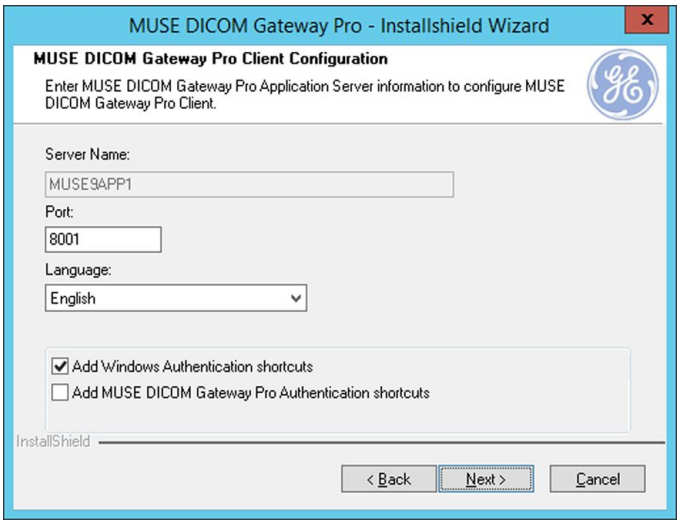


Select the destination folder in which to install the application files.

To change the default location, click the ***Browse*** button and select or type in the correct path.

15. Click ***Next***.

    The ***MUSE DICOM Gateway Pro Client Configuration*** window opens.



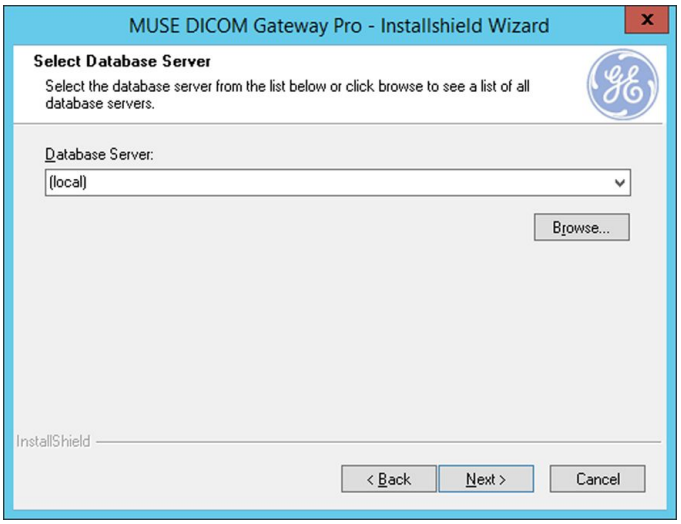
16. Complete the fields on the ***MUSE DICOM Gateway Pro Client Configuration*** window using the information in the following table:

Client Configuration Settings

Field	Action
Server Name	Automatically populated with the local server name where you are installing MUSE DICOM Gateway system application server. You cannot change this field.
Port	Defaults to 8001 This is the port the system server will listen on for incoming application connections. You can change the port number if required.
Language	Defaults to English English is the only supported language for MUSE DICOM Gateway Pro.
Add Windows Authentication shortcuts	Defaults to a selected checkbox. Clear the box if you do not want to add Windows authentication shortcuts.
Add MUSE DICOM Gateway Pro Authentication shortcuts	Defaults to an unchecked checkbox. Select if you want to add MUSE authentication shortcuts.

17. Click ***Next***.

    The ***Select Database Server*** window opens.



    The ***Database Server*** field defaults to ***(local)*** or can also be blank.

    The ***(local)*** setting indicates that the system database resides on the same server as the MUSE DICOM Gateway Pro application.

18. Perform on the following steps:

    - If you are installing the database on the local SQL Server, ensure the field is populated with either ***(local)*** or the computer name of the local server. If the field is blank, type the computer name of the local server.
    - If you are installing the database on a remote SQL Server, click ***Browse*** or type the name of the SQL Server where the system databases will be or are installed.

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

    Default instance example: ***SQLSERVER***

    Named instance example: ***SQLSERVER\INSTANCE***

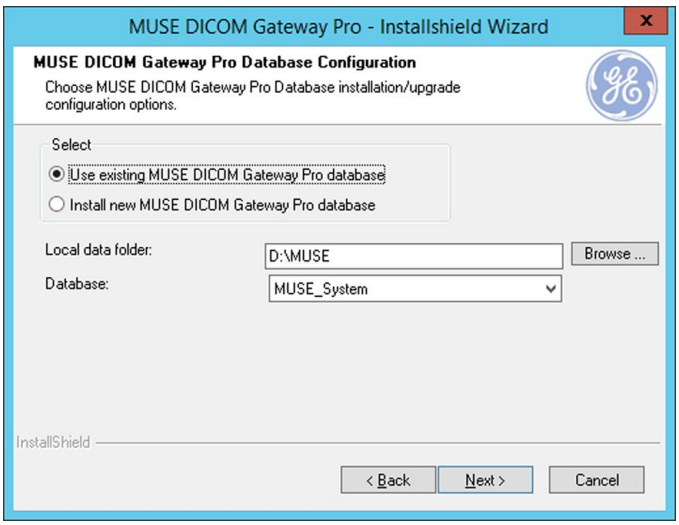
    NOTE:
    You must specify the SQL Server by name or ***(local)***. Do not use the IP Address of the SQL Server.

19. Click ***Next***.

    The ***MUSE DICOM Gateway Pro Database Configuration*** window opens.

20. Perform one of the following steps:

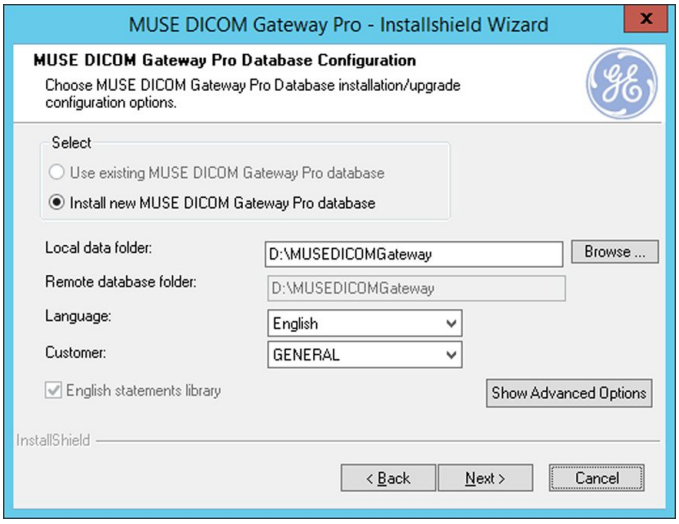
    - **Re-installations**: For a re-installation of the system, there is an existing database. Select ***Use existing MUSE DICOM Gateway Pro database*** and ensure the ***MUSE_System*** database is selected in the ***Database*** drop-down selection.



NOTE:

If the ***Use existing MUSE DICOM Gateway Pro database*** option is not available or shaded and this is not a new installation, the system installer did not find the MUSE database. The MUSE database may not be properly attached to the SQL Server.

- **New Installations**: For a new installation, select ***Install new MUSE DICOM Gateway Pro database*** and complete the fields on the ***MUSE DICOM Gateway Pro Database Configuration*** window using the following table:

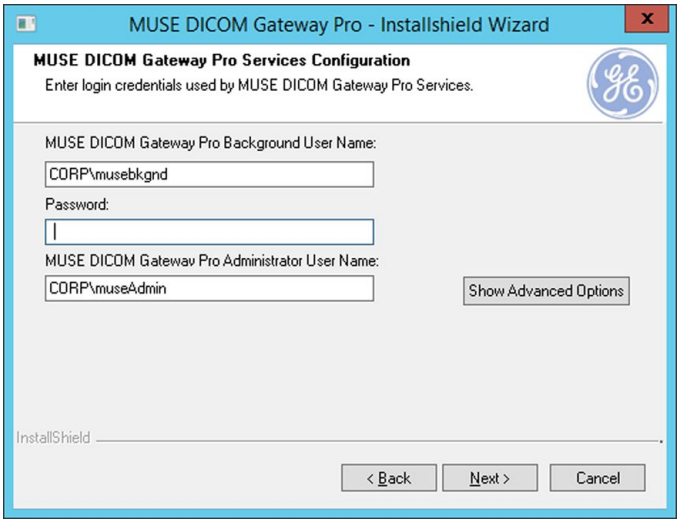


MUSE DICOM Gateway Pro Database Configuration Settings

Field	Description
Local data folder	The path where the MUSE db, backup, Acq, XML logs and other directories will be created on the system application server. If this folder does not already exist, the installer creates it.
Remote database folder	If you are installing a local database, this field is disabled. If the database will be installed on the remote database server, this field is enabled and you can enter the path where it will be installed. If this folder does not already exist, the installer creates it.
Language	The default is English. English is the only supported language for MUSE DICOM Gateway Pro.
Customer	This selects specific Customer IDs by country. The default is ***GENERAL***. This setting seldom needs to be changed. If necessary, use the drop-down menu to change the ***Customer*** field value. This selection activates special rules governing PIDs within the system application.
English statements library	The field is checked by default. This field is only enabled if you want to use the ***English statements library*** instead of the database library for the selected language.
Show Advanced Options button	Use this button to change the database prefix. There are few reasons to change the database prefix. **Do not** change the database prefix unless specifically directed to do so by MUSE Engineering or MUSE Technical Support.

21. Click ***Next***.

    The ***MUSE DICOM Gateway Pro Services Configuration*** window opens.



22. Type the ***User Name*** and ***Password*** for the ***MUSE DICOM Gateway Pro Background*** account and the ***User Name*** for the ***MUSE DICOM Gateway Pro Administrator*** account.

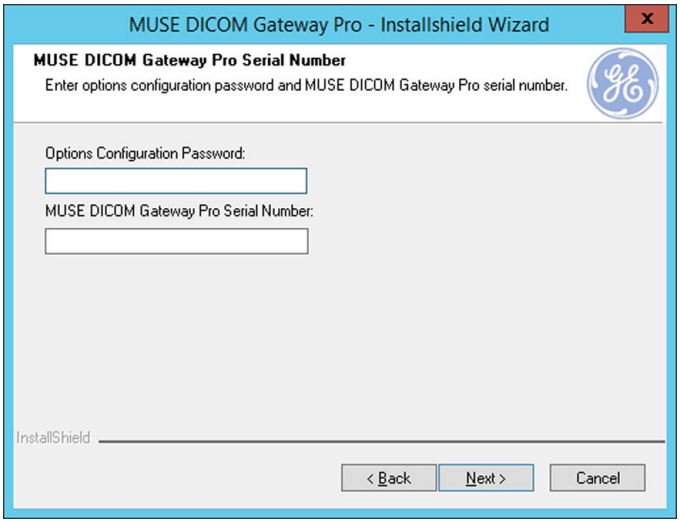
    - The user name for the MUSE DICOM Gateway Pro Background user and MUSE DICOM Gateway Pro Administrator user cannot be the same.
    - If you are using a domain account, type the user name in ***<domain name>\<user name>*** format.
    - If you are using a local account, type the user name in ***.\<user name>*** format.
    - No password is required for the MUSE DICOM Gateway Pro Administrator user account.

    The installer will install the MUSE DICOM Gateway services using the MUSE DICOM Gateway Pro Background account and password specified here. It updates the ***Windows User Name*** field of the ***MuseAdmin*** and the ***MuseBkgnd*** user accounts in the system database with the user accounts that you entered.

    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 MUSE Engineering or MUSE Technical Support.

23. Click ***Next***.

    The ***MUSE DICOM Gateway Pro Serial Number*** window opens.



24. Type the ***Options Configuration Password***.

NOTE:

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

25. Type the ***MUSE DICOM Gateway Pro Serial Number***.

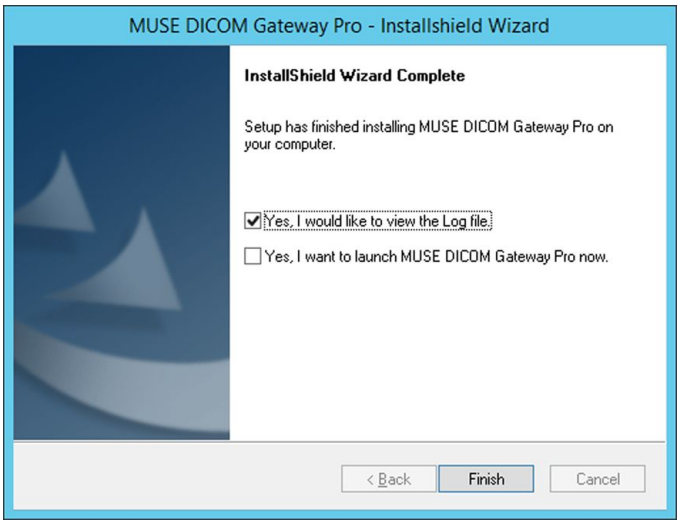
Refer to the Options Activation Sheet or contact the Project Manager for the correct serial number.

26. Click ***Next***.

The ***Review Installation*** window opens.

- If you need to make changes, click ***Back*** and return to the previous windows and make the necessary changes using the preceding steps.
- If everything is correct, click ***Next*** to begin the installation and the System Application Server software installs.

When the installation is complete, the ***InstallShield Wizard Complete*** window opens.



27. Click ***Finish***.

    The current ***MUSEDICOMGatewayPro_Installer_Log_xxx.log*** file opens.

28. Review the log file for any failures, errors, or warnings.

    NOTE:
    The installation log files are located on the root of the ***c:\ drive***.

29. If you selected ***Yes, I want to launch MUSE DICOM Gateway Pro now***, the system application starts.

    If you did not select the option to launch the MUSE DICOM Gateway Pro, manually launch the system application.

30. Verify you can successfully log on to the system application.

31. Verify that the ***MUSE DICOM Gateway*** services have started.

System Application Server Installation Troubleshooting

Message	Description	Action
SQL server 2008 or SQL server 2008 R2 or SQL server 2012 or SQL server 2014 is not installed.. This warning can be ignored if you are installing the MUSE database on a different machine. Do you want to continue? **NOTE:** The following error is also logged in the ***MUSEDICOMGatewayPro_Installer_Log*** file for this ***Error retrieving SQL server registry information***.	This message indicates that a compatible SQL Server database engine was not detected on the machine where the System InstallShield Wizard is being installed.	This message is normal if the database will be remote since the SQL Server database engine won't be installed on the computer where the System InstallShield Wizard is being run from. If the intention is to install the database locally, ensure a compatible version of SQL Server is installed before proceeding.
Microsoft SQL Server client not found. Please install SQL Server Client and retry installation.	This message indicates that SQL Server Management Studio was not found.	SQL Server Management Studio, which includes essential SQL Server Client files, needs to be installed on the System Application server, even if the database is remote. Ensure SQL Server Management Studio is installed.
The user does not have sufficient database privileges.	This message indicates the user running the InstallShield Wizard does not have sysadmin server role access to the SQL Server database instance specified.	Ensure the user running the System InstallShield Wizard has sysadmin server role access to the SQL Server database instance.
	This message can also indicate that the SQL Server instance specified is not valid.	Ensure the SQL Server instance name specified is valid and accessible from the System Application server.

Message	Description	Action
Selected database not found. Please verify connectivity or select a different database.	This message indicates that the Database Server specified could not be found.	Ensure the Database Server specified is valid and accessible from the System Application server.
User validation failed. Either this user does not exist in the specified domain/computer or the password is wrong.	This message indicates that the MUSE Background user specified does not exist or the password is incorrect.	Verify the correct MUSE Background user name and password are correct.
User validation failed. The MUSE Background user does not have access to the database server.	This message indicates that the MUSE Background User Name specified does not have a valid SQL Server Login.	Confirm the MUSE Background User Name specified has a valid SQL Server Login on the SQL Server Database Instance.
User validation failed. The MUSE Administrator user does not have access to the database server.	This message indicates that the MUSE Administrator User Name specified does not have a valid SQL Server Login.	Confirm the MUSE Administrator User Name specified has a valid SQL Server Login on the SQL Server Database Instance.
User validation failed. The MUSE Background user does not have the correct database permissions. Do you want to continue?	This message indicates that the MUSE Background User Name specified has a valid SQL Server Login, but does not have the expected database permissions. The expected database permissions are either sysadmin server role and/or dbcreator server role.	Confirm the MUSE Background User Name specified has either sysadmin server role or dbcreator server role. If the MUSE Background User Name has neither sysadmin server role nor dbcreator server role, the installer will allow you to proceed and the installation will be successful, however no new sites can be created after the system is installed until the MUSE Background User is given the sysadmin server role or dbcreator server role.
MUSE Background User Name entered is already present in the database as a non-service user. Please enter different user name and proceed.	This message indicates that the MUSE Background User Name specified is already associated with a MUSE User other than MuseBkgnd (PersonID 2). The system does not allow two MUSE Users to have the same Windows User Name.	Use a different MUSE Background User Name.
MUSE Administrator User Name entered is already present in the database as a non-service user. Please enter different user name and proceed.	This message indicates that the MUSE Administrator User Name specified is already associated with a MUSE User other than MuseAdmin (PersonID 1). MUSE does not allow two MUSE Users to have the same Windows User Name.	Use a different MUSE Administrator User Name.

Real Time Virus Scanners Settings

If the system has a virus scanner that executes in real time, the entire system installation folder and subfolders should be excluded from the virus scanning after the installation is complete. Work with the customer to exclude this folder.

Installing InSite ExC

Install InSite ExC on the application server to ensure GE Healthcare service can remotely service the system. For instructions on installing InSite ExC, refer to the *InSite ExC Installation Manual*.

Next Steps

The following high-level steps can be used as a guide when configuring the system for end-to-end use after initial installation.

1. Configure the system to download DICOM MWL orders from DICOM Modality Worklist Service Class Provider(s). For instructions, see "Configuring the System to Query for DICOM Orders" on page 114.
2. Configure outbound DICOM device(s) to send tests to DICOM Storage Service Class Provder(s). For instructions, see "Configuring the System to Send DICOM Tests" on page 111.
3. Configure Report Distribution on the system to route incoming tests to the outbound DICOM Devices. For instructions, see "Setting Up Report Distribution" on page 66.
4. Configure the system for CSI Modem, CSI Network, and/or DCP Inbound. For instructions, see "MAC Resting ECG Systems to MUSE DICOM Gateway Pro" on page 103.
5. Configure the MAC Resting ECG system(s) to communicate with CSI Modem, CSI Network, and/or DCP Inbound configured for the system. For instructions, refer to the appropriate documentation:
   - *MobileLink Installation Manual*
   - *LAN Option for MAC Installation and Troubleshooting*
6. Perform a system checkout to ensure everything is working as expected. For instructions, see "System Checkout" on page 121.

Uninstalling the System Application and Database

You can remove the MUSE DICOM Gateway Pro application using the Windows ***Programs and Features*** (located in ***Control Panel***).

Uninstalling the MUSE DICOM Gateway Pro application removes the following:

- MuseDicomGateway installation folder in ***Program Files***
- MUSE DICOM Gateway services
- MUSE DICOM Gateway shortcuts

Uninstalling the MUSE DICOM Gateway Pro application does not remove the following:

- MUSE databases
- MUSE database subfolders
- .NET Framework and other MUSE prerequisites

Any software not uninstalled by the MUSE DICOM Gateway installer can be removed using Windows ***Control Panel*** > ***Programs and Features***.

Use the following procedures to uninstall the MUSE DICOM Pro Gateway application:

1. Verify no users are logged on to the server, including remote users.
2. Stop the ***MUSE*** services.
3. Go to ***Control Panel*** > ***Programs and Features***.
4. Select ***MUSE DICOM Gateway Pro*** and click ***Uninstall***.
5. At the confirmation prompt, click ***Yes***.
6. When the ***Uninstall Complete*** window opens, click ***Finish***.
7. Reboot the system and confirm that the ***MuseDicomGateway*** installation directory is removed.

   If it is not removed, manually remove it.

   The default MUSE installation directory is ***C:\Program Files (x86)\MuseDicomGateway***.

   NOTE:
   If you re-install the system at a later time and want to use the existing database, select ***Use existing MUSE DICOM Gateway Pro database*** during the installation procedure.

4

System Configuration

This chapter describes how to configure your system. Specifically, it addresses the following areas, all of which can be configured by a system administrator:

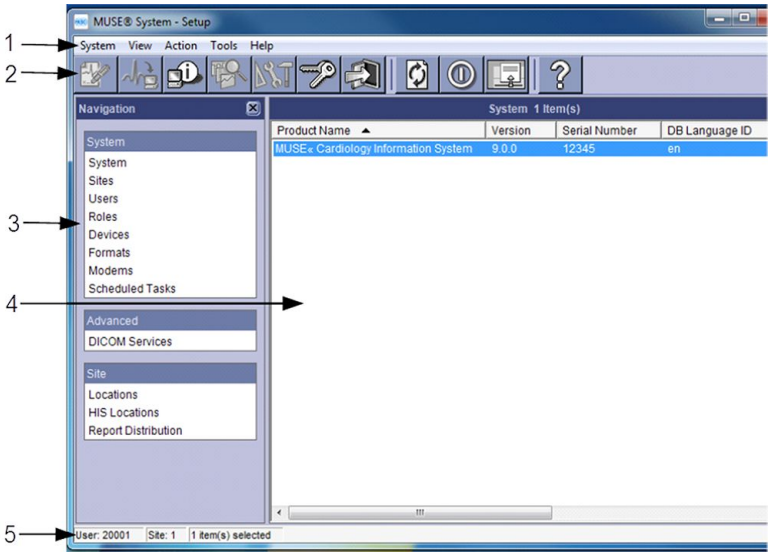
- System Setup
- Sites
- Users
- Roles
- Devices
- Formats
- Modems
- Scheduled Tasks
- Share Folder
- DICOM Services
- Locations
- HIS Locations
- Report Distribution

System Setup

Proper privileges are required to perform system setup.

To access the ***Setup*** window, select ***System*** > ***Setup***.

The ***Setup*** window opens.



Setup Window Description

Item	Name	Description
1	Menu Bar	Displays the name of current menus.
2	Tool Bar	Displays icons for easy access to Menu Bar functions.
3	Navigation Pane	Allows easy access to System and Site Setup features.
4	Main Window	Displays System and Site information.
5	Status Bar	Displays information regarding the User, Site, and selected items.

Setting Up the System Properties

The ***System Properties*** window is where you set up password constraints and DCP configurations, and enable the race list and enhanced patient race list.

Setting Up System Properties — General

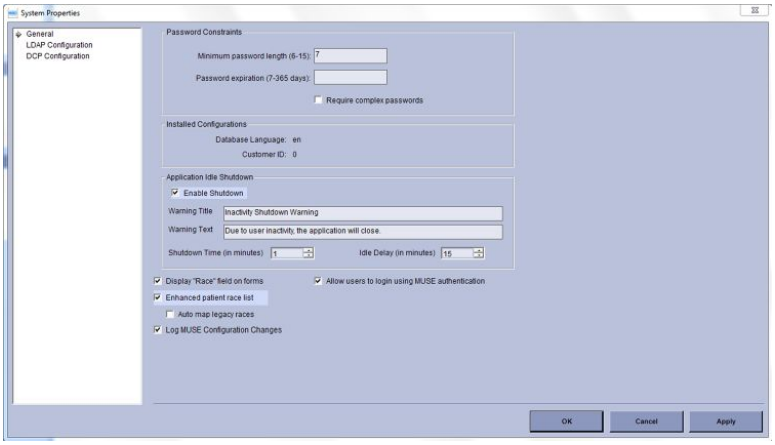
1. From the ***Navigation*** pane, click ***System***.

   A list of available systems is displayed.

2. Double-click on the appropriate system to select it.

   The ***System Properties*** window opens.

General is highlighted in the ***Navigation pane***.



3. Enter information for the following options:

Option	Action	Description
Minimum password length (6–15)	Type a number between 6 and 15.	Ensures passwords have a length greater than a configured value between 6 and 15. **NOTE:** This does not constrain the maximum password length, only the minimum.
Password expiration (7–365 days)	Type a number between 7 and 365.	Defines the time period in days before a new password expires, which the user must change on the next login. **NOTE:** To define password configuration rules per user, see "Adding Users" on page 53.
Require complex passwords	Select the check box to enable this option.	Requires that new passwords meet the following complexity rules: • Contains characters from three of the following four categories: lowercase alphabetic, upper case alphabetic, numeric, other characters. • Does not contain the user name.
Database Language	This option is information set up during installation and cannot be changed.	Displays the database language.

Option	Action	Description
Customer ID	Default	The Customer ID is set up during initial installation of the MUSE system and cannot be changed.
Enable Shutdown	Select the check box to enable this option.	Allows you to enable or disable the MUSE idle/shutdown feature. The MUSE system will shutdown if there is no mouse or keyboard activity for the set period of time. The ***Warning Title***, ***Warning Text***, ***Shutdown Time (in minutes)*** and ***Idle Delay (in minutes)*** must also be configured.
Warning Title	Type title text that displays in the shutdown warning window.	Allows you to customize the warning title text that displays in the user's shutdown window before the MUSE system does a shutdown. The default text is ***Inactivity Shutdown Warning***.
Warning Text	Type the warning text that displays in the shutdown warning window.	Allows you to customize the warning text that displays in the user's shutdown window before the MUSE system does a shutdown.
Shutdown Time (in minutes)	Select a number between 1 and 60.	Defines the time period in minutes that the shutdown warning screen displays on the screen before the MUSE system shuts down.
Idle Delay (in minutes)	Select a number between 1 and 60.	Defines the time period in minutes that the MUSE system is idle before the shutdown window is displayed on the screen.
Display "Race" field on forms	Select the check box to enable this option.	Displays the race field on forms. If disabled, the race field does not display.
Allow users to login using MUSE authentication	Select the check box to enable this option.	Allows you to log on with MUSE authentication.
Enhanced patient race list	Select the check box to enable this option.	Enables the enhanced race list to display in the system application.

Option	Action	Description
Auto map legacy races	Select the check box to enable this option only if ***Enhanced patient race list*** in ***System*** > ***System Properties*** > ***General*** is enabled.	Enables the mapping of incoming retired legacy races from acquired tests or messages from the HIS. This option maps the retired legacy race to a race from the enhanced race list. For a table of auto-mapped races, see Appendix B "Enhanced Patient Race List" on page 141. **NOTE:** If both ***Enhanced patient race list*** and ***Auto map legacy races*** are enabled, and a test with a race (for example, "Oriental") is acquired from the cart that does not support the enhanced race list, the MUSE system auto-maps the retired race to a race in the enhanced list (in this case, "Asian") as shown in Appendix B "Enhanced Patient Race List" on page 141. If this test is printed at a cart that does not support the enhanced race list, the race field is displayed as blank at the cart.
Log MUSE Configuration Changes	Select the check box to enable this option.	Logs any MUSE system configuration changes in the ***Configuration Change Log*** in ***Status***.

4. Click ***OK*** or ***Apply*** to save your changes.

Setting Up System Properties – DCP Configuration

For information pertaining to DCP configuration, see Chapter 8 "MAC Resting ECG Systems to MUSE DICOM Gateway Pro" on page 103.

Setting Up Sites

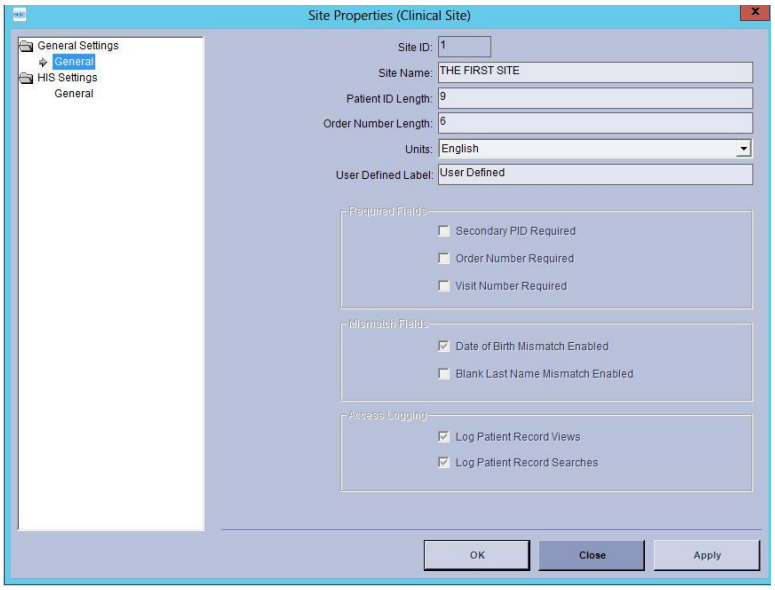
Sites are useful for organizing incoming patient tests and locations (including remote locations) within a hospital or large clinic setting, and assisting in the workflow of reading patient tests. You can assign specific users and devices to specific sites.

Setting up sites creates unique databases. The data in Site 1 is unique from the data stored in other sites.

All patients within a site need to have a unique patient ID. The MUSE system assumes that all patients with a single patient ID are one patient. If two patients could potentially share a patient ID, then they cannot share the same site.

Creating and Modifying Clinical Sites

1. In the ***Navigation*** pane on the ***Setup*** window, highlight ***Sites***.
   - Select ***Action*** > ***New*** > ***Clinical*** to set up a clinical site.
   - Click on an existing site to open it for editing.
2. The ***Site Properties*** window opens.

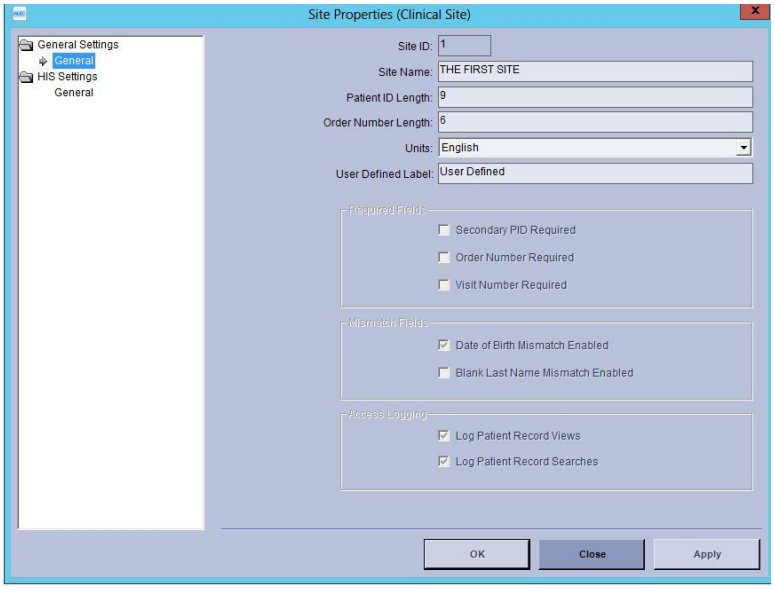


Site Properties Window — Clinical Site

NOTE:
When you change a field value, the value line box turns blue. If you type an invalid entry, the value line box turns red. If the value line box is empty and turns red, you must enter a value.

Site Properties – General Setup

1. In the menu tree at the left side of the ***Site Properties*** window, select ***General***.



2. Enter information for the following fields.

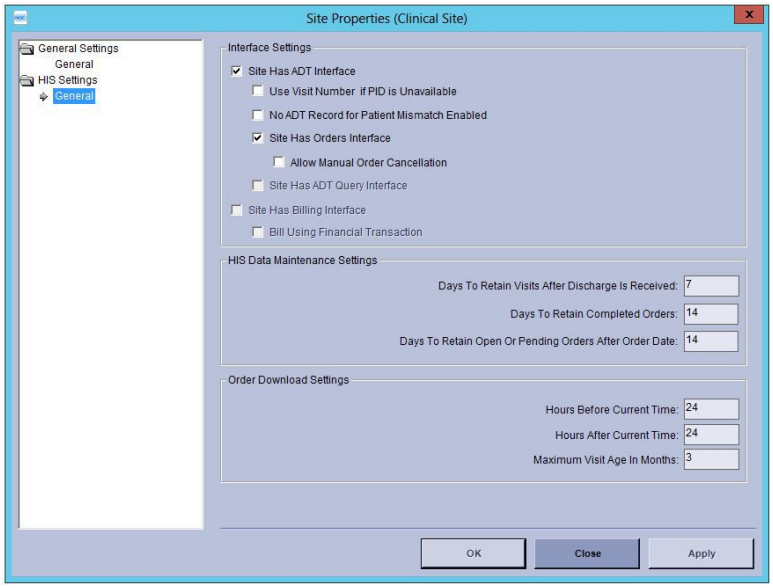
Field	Action	Description
Site ID	Type the site ID.	Sets up a new site, if necessary.
Site Name	Type the site name.	Names a new site, if necessary. This is the name that will display on the ECGs that are printed from the system (in the upper-right corner).
Patient ID Length	Type a number from 6 to 16.	Configures the maximum number of characters that you can enter manually in the ***Patient ID*** field on the system.
Order Number Length	Type a number from 1 to 22.	Configures the maximum number of characters that you can enter manually in the ***Order Number*** field on the system if the site does not have the HIS orders interface.
Units	Select English or Metric.	Determines how units are displayed in reports from this site.
User Defined Label	Type appropriate text.	Adds a field to the ***Clerical*** tab of the ***Editor***. For example, if you add "Medicare Number" in the user-defined field, every test record has a field for "Medicare Number".

3. Click ***OK*** or ***Apply*** to save your changes.

Setting Up Sites — HIS Settings

Setting Up HIS — General

1. In the menu tree on the left of the window, select ***HIS Settings > General***.



2. In the ***Interface Settings*** section, make sure that ***Site Has ADT Interface*** and ***Site Has Orders Interface*** are selected.

3. The following ***HIS Data Maintenace Settings*** are relevant for MUSE DICOM Gateway Pro in managing orders that are received from the ***Modality Worklist*** provider.

Field	Description
Days to Retain Completed Orders	Set the number of days before completed orders are purged. Type a number from 0 to 255 days. This option is grayed out it ***Sited has Orders Interface*** is not selected.
Days to Retain Open Orders After Order date	Set the number of days you want an open order left in the open order list. Type a number from 0 to 255 days.

4. The following ***Order Download Settings*** are relevant for MUSE DICOM Gateway Pro in managing Order downloads to ECG carts.

Field	Description
Hours before Current Time ***Hours after Current Time***	Set up the number of hours to use when downloading a list of open orders to the ECG device. The ***Hours before Current Time*** option gives you the number of hours before the current time for which an order is available to download. The ***Hours after Current Time*** option gives you the number of hours after the current time for which an order is available to download. For example, if the ***Hours before Current Time*** is set to 8, and the ***Hours after Current Time*** is set to 4, and the current time is 1:00 p.m., then all tests scheduled between 5:00 a.m. and 5:00 p.m. are on the order list at the ECG device. This option is grayed out if ***Site has Orders Interface*** is not selected.
Maximum Visit Age in Months	Set up a window of time in months. When a MAC 3500 or MAC 5500 (version 10 or higher), or a MAC 2000, queries the system for patient demographics based on a visit number it ignores all visits older than XX months (XX is the number of months specified in this field). The visit number is not guaranteed to be unique at all facilities and can overlap after a certain amount of time passes. This option is grayed out if ***Site has Orders Interface*** is not selected.

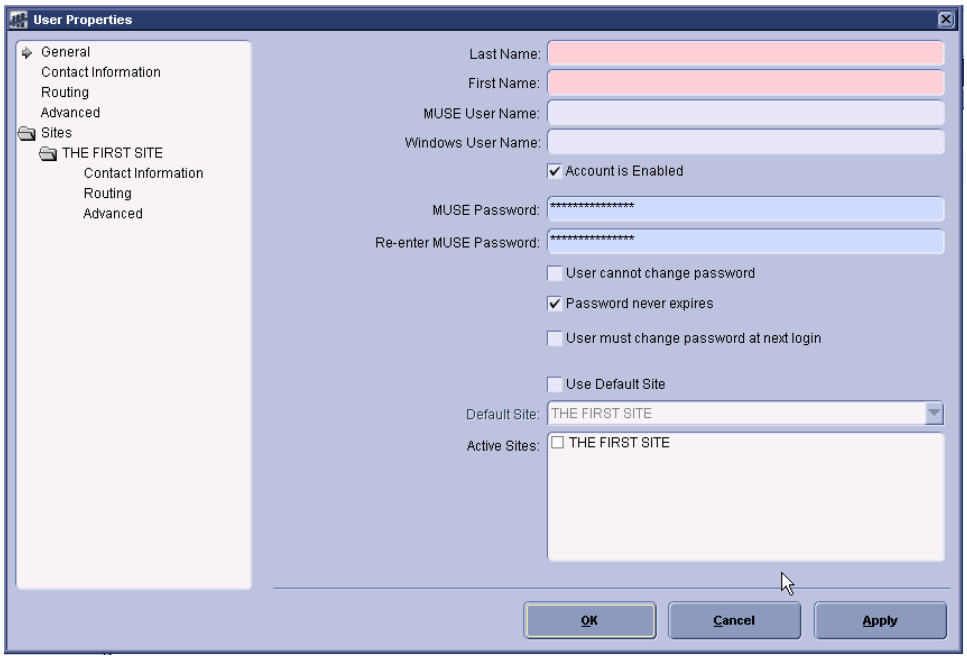
Adding Users

Each individual using the system has a user account.

To add a new user:

1. In the Navigation pane on the ***Setup*** window, highlight ***Users*** to view the ***Users*** window.
2. Click ***Action*** > ***New***.

The ***User Properties*** window opens.



Setting Up User Properties – General Information

1. On the menu tree at the left side of the window, highlight ***General***.
2. Modify the fields described in the following table.

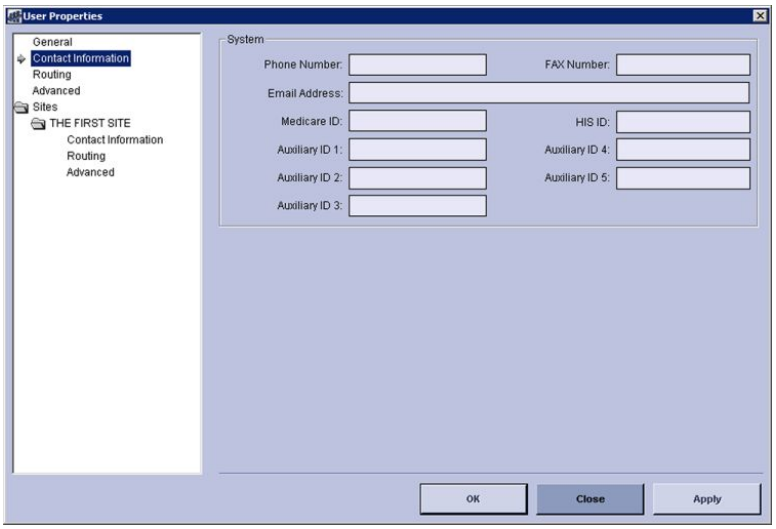
Field	Description
Last Name ***First Name***	Type the user's first and last name. The user's first and last name are displayed in test reports and forms.
MUSE User Name	Type the appropriate MUSE user name to allow access to the system when logging in with MUSE authentication.
Windows User Name	If using Windows authentication to log on to the system, type the Windows user name entered at the Windows login screen.
Account is Enabled	This check box enables or disables user access to the system.
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.
User cannot change password	If this check box is enabled, the user cannot change their MUSE password.
Password never expires	If this check box is enabled, the user password does not expire and does not require to be changed.
User must change password at next login	If this check box is enabled, the user is forced to change their password during the next login.

Field	Description
Use Default Site (check box) ***Default Site (drop-down list)***	If this check box is enabled, you can select a default site from the list. If a default site is selected, you log onto this site when re-entering the application.
Active Sites	Select all check boxes that apply to grant access to those sites.

3. Click ***OK*** when finished.

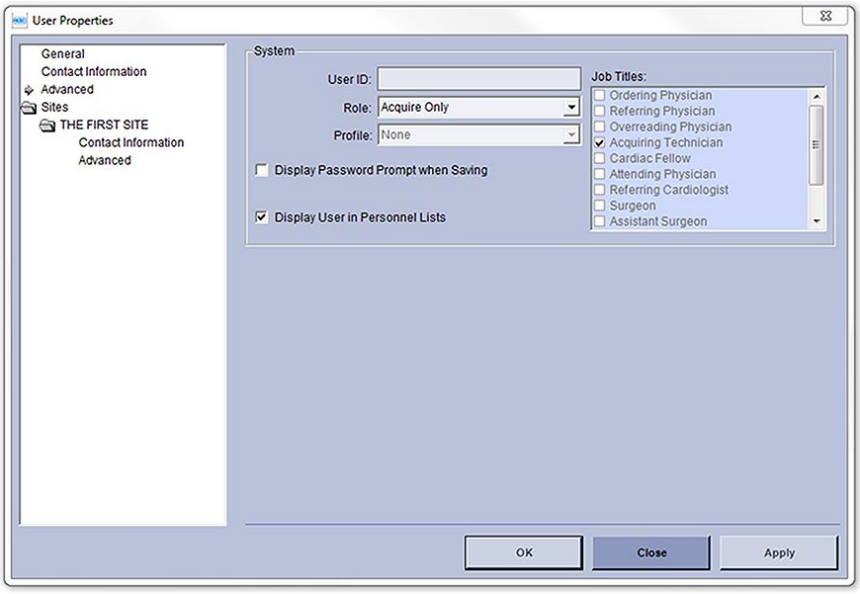
Setting Up User Properties – Contact Information

To review the contact information, select ***Contact Information*** on the menu tree at the left side of the window. All fields on the ***Contact Information*** page are reference only and not used in other parts of the application.



Setting Up User Properties – Advanced

1. Select ***Advanced*** in the menu tree at the left side of the window.



NOTE:

In the MUSE DICOM Gateway Pro system, the following fields and option are not used:

- ***Profile*** field
- ***Job Titles*** field
- ***Display User in Personnel Lists*** option

2. Configure advanced information as described in the following table:

Field	Description
User ID	Type the User ID for this user. Every user who performs any function on the system or acquires tests at a peripheral device should be a system user and have a User ID. **NOTE:** The User ID is the same as the ID entered at the Cart as the ***Technician ID*** in the ***Technician*** field.
Role	Select the correct user role. The role defines the privileges for this user and determines what this user can or cannot do on the system. See Appendix C "Roles and Privileges " on page 143.
Display Password Prompt when Saving	If enabled, the user is required to provide his or her password when saving data.
Display User in Personnel List	If enabled, the users are displayed in the personnel list.

3. Click ***OK*** when finished.

Setting Up User Properties – Site Overrides

User Properties can be overridden on a per site basis. You can override the user properties for a site to:

- Modify roles, profiles, or job titles on a per site basis.
- The user has a different user ID across multiple sites.

After each site is added to the system, it is visible in the ***User Properties – Sites*** folder.

1. On the menu tree at the left side of the window, highlight ***Sites*** to view user privileges for a site (including routing privileges, contact information, and user privileges that were previously set up).
2. Select the appropriate site from the list.
3. Select ***Contact Information***, ***Routing***, or ***Advanced*** for the site.

   The top half of the window shows the system user configuration for reference.

   The bottom half of the window shows the overridden user configuration which can be modified.
4. To change these settings, select the ***Override for this Site*** check box.

   The data fields are active and ready to modify. The ***User Properties*** fields are the same as those described in "Setting Up User Properties – General Information" on page 54.
5. Make any necessary changes.

   NOTE:
   Any changes made to the overridden site user configuration overrides the system user configuration when the user accesses the overridden site.
6. Click ***OK*** when finished.

   For additional information on how and when to configure site overrides, contact GE Healthcare Clinical Application support.

Setting Up Roles

User privileges are included in predefined groupings known as roles. System Administrators can assign roles to allow users access or prevent users from accessing certain functions on the system. Each individual who uses the system is assigned a role. In order to avoid confusion, a user is assigned only one role per site. The system provides a default set of roles to use, however, you can create new roles. System-defined roles are locked and the user cannot change them. Roles are defined at the system level so all sites can share the same list of roles.

The system default roles include:

- Acquire Only
- Site Manager
- System Owner
- MUSE Service
- All Privileges

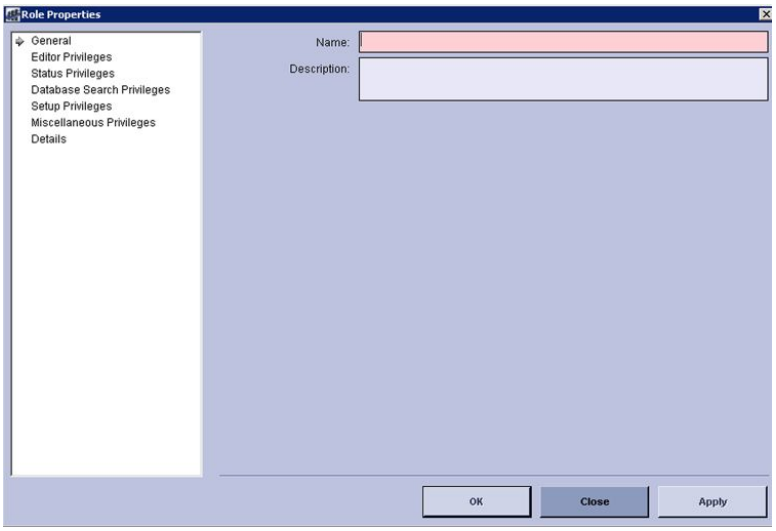
Creating User-Defined Roles

1. On the menu tree at the left side of the window, select ***Roles***.

   The ***Roles*** window opens.

2. Select ***Action*** > ***New***.

   The ***Role Properties*** window opens.



3. In the ***General*** window, type the name and description of the new role.
4. Assign the appropriate privileges at the ***Editor...***, ***Status...***, ***Database Search...***, ***Setup...***, and ***Miscellaneous...*** windows.
5. Click ***OK*** when finished.

   Once the new role is created, you can attach it to a user.

   For a definition of roles and privileges, see Appendix C “Roles and Privileges ” on page 143.

Modifying a User-Defined Role

1. In the menu tree at the left side of the window, highlight ***Roles***.

   The ***Roles*** window opens.

2. Double-click on a user-defined role that you want to modify.

   Do not click on a system-defined role as those cannot be modified.

   For a definition of roles and privileges, see Appendix C “Roles and Privileges ” on page 143.

3. Select ***Status Privileges*** and ***Setup Privileges*** to turn the appropriate privilege on or off.

   For a definition of roles and privileges, see Appendix C “Roles and Privileges ” on page 143.

4. Click ***OK*** when finished.

Deleting User-Defined Roles

1. In the ***Roles*** window, highlight the user-defined roles you want to delete.
2. Select ***Action*** > ***Delete***.
3. Confirm by clicking ***Yes***.

   The user-defined role is permanently deleted from the system.

Configuring Devices

For information on configuring devices for DICOM communication see Chapter 9 "DICOM Communication" on page 109.

Setting Up Modems

For information on setting up modems, see "Setting up Modems" on page 104.

Setting Up Scheduled Tasks

The ***Scheduled Tasks*** are used to perform functions on the system at regular intervals. The following tasks can be scheduled to execute:

- ***HIS Data Maintenance***
- ***Log and Queue Maintenance***
- ***Temporary File Maintenance***
- ***Test Maintenance***

HIS Data Maintenance Scheduled Task

The ***HIS Data Maintenance*** task performs cleanup activities on HIS data stored on the system.

1. On the ***Navigation*** panel, select ***Scheduled Tasks***.
2. Select ***HIS Data Maintenance***, right-click and select ***Properties***.

   The ***Scheduled Task Properties — HIS Data Maintenance*** window opens.
3. Set the ***Scheduled Time***.

   It is recommended that you set the ***Scheduled Time*** to execute when no other activities are being performed on the system.

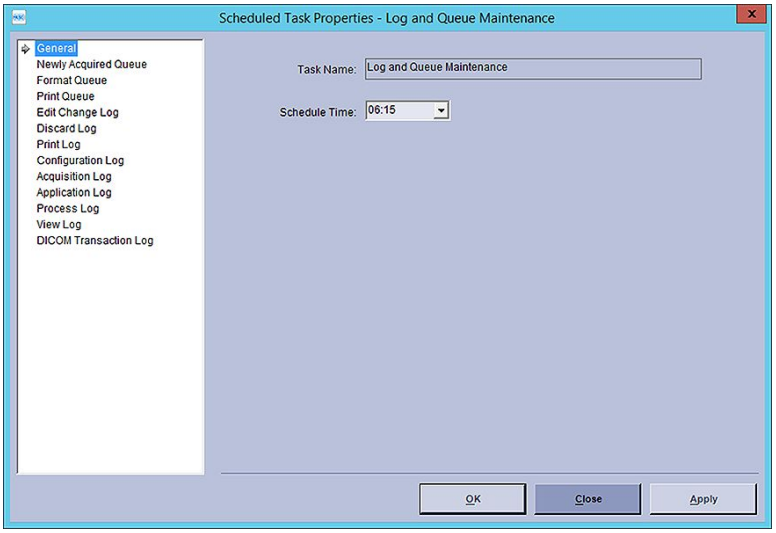
   The default time is 6:30 a.m.
4. Click ***OK*** when finished.

Log and Queue Maintenance Scheduled Task

The ***Log and Queue Maintenance*** task performs all cleanup activities on the logs and queues.

1. On the ***Navigation*** pane, select ***Scheduled Tasks***.
2. Select ***Log and Queue Maintenance***, right-click and select ***Properties***.

   The Scheduled Task Properties — Logs and Queues window opens.



3. On the ***General*** screen, set the ***Schedule Time*** of when you want to run the log and queue maintenance task.
4. Highlight each queue or log in the navigation tree and set the ***Days to Hold***.

   This action sets the duration of how many days of logs do you want to keep. If you set this for 15 days, for example, anything older than 15 days is deleted.

   NOTE:
   The ***Send Data as XML to device before deleting*** is not supported on the MUSE DICOM Gateway Pro.

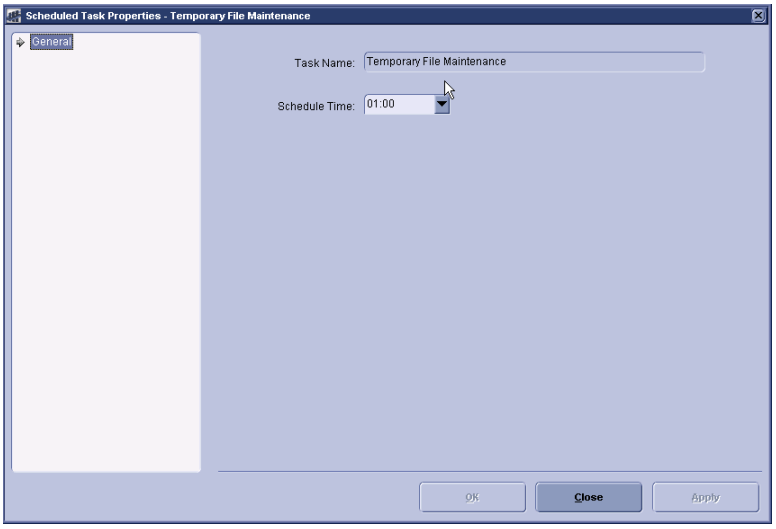
5. Click ***OK*** when finished.

Temporary File Maintenance Scheduled Task

The ***Temporary File Maintenance*** task performs cleanup activities on temporary files created by the system.

1. On the ***Navigation*** pane, select ***Scheduled Tasks***.
2. Select ***Temporary File Maintenance***, right-click and select ***Properties***.

   The ***Scheduled Task Properties — Temporary File Maintenance*** window opens.



3. Set the ***Scheduled Time***.

   It is recommended that you set the ***Scheduled Time*** to execute when no other activities are being performed on the system.

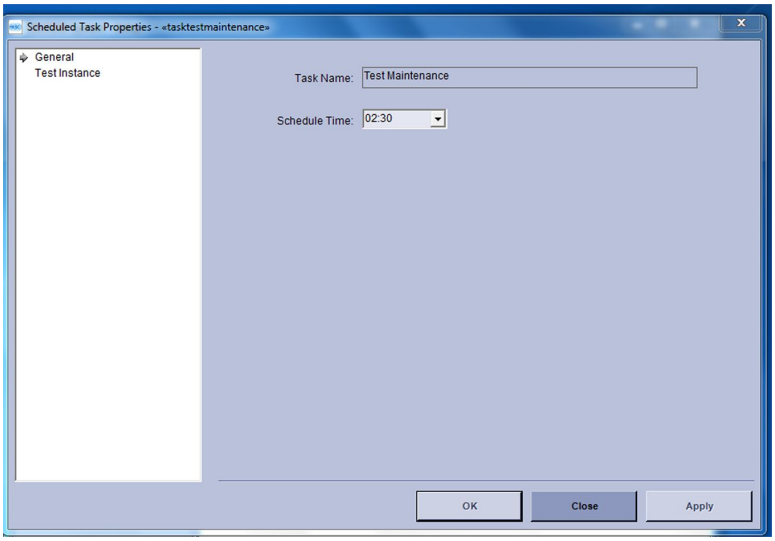
   The default time is 1:00 a.m.
4. Click ***OK*** when finished.

Test Maintenance Scheduled Task

The ***Test Maintenance*** scheduled task performs cleanup activities on the tests and related DICOM files created by the system.

1. On the ***Navigation*** pane, select ***Scheduled Tasks***.
2. Select ***Test Maintenance***, right-click and select ***Properties***.

   The ***Scheduled Task Properties — Test Maintenance*** window opens.



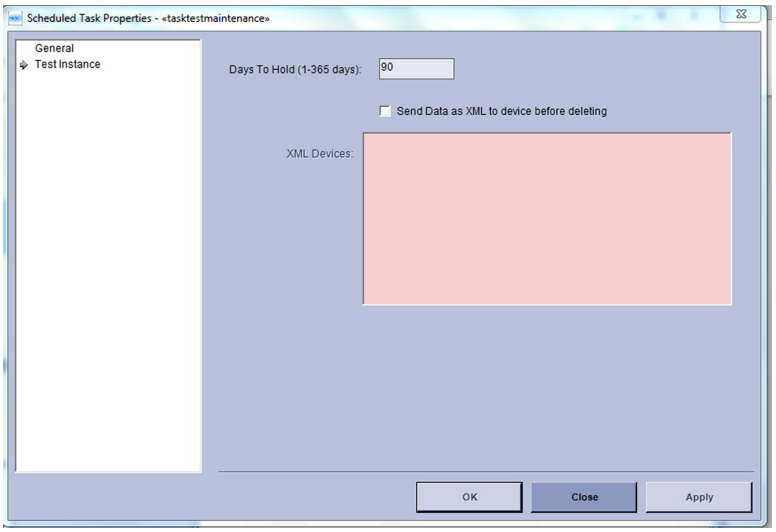
3. Set the ***Schedule Time***.

   It is recommended that you set the ***Schedule Time*** to execute when no other activities are being performed on the system.

   The default time is 2:30 a.m.

4. Click on ***Test Instance*** to configure the ***Days To Hold (1–365 days)***.

   The system purges tests from the DICOM database based on the number of ***Days To Hold (1–365)*** specified.



5. Click ***OK*** when finished.

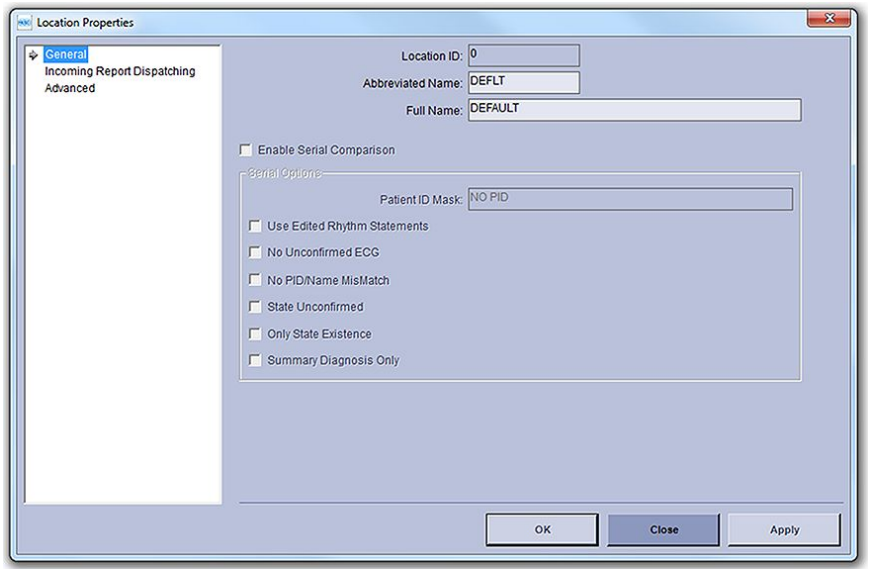
Configuring DICOM Services

For information on configuring DICOM services see Chapter 9 “DICOM Communication” on page 109.

Setting Up Locations

Locations specify routing destinations. You can auto-route tests coming from locations to outbound DICOM devices.

To add a new location, from the ***Navigation*** pane, select ***Locations*** and then select ***Action*** > ***New***. The ***Locations Properties*** window opens.

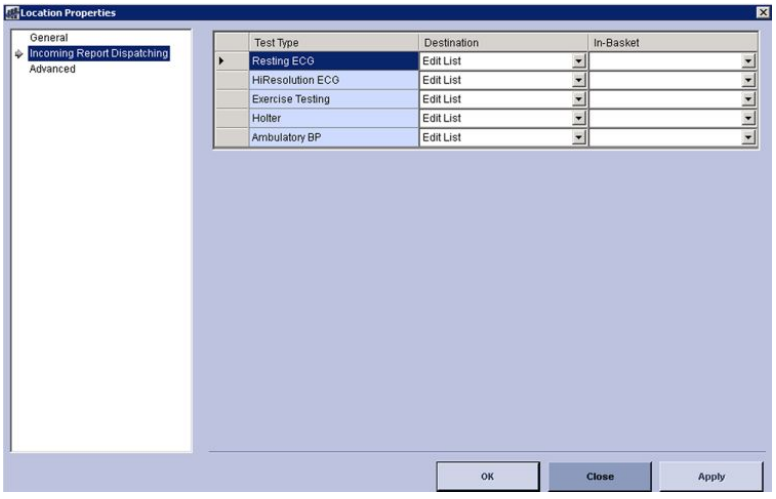


Type the appropriate information in the fields provided as described in the following sections.

Setting Up Incoming Report Dispatching

NOTE:
Incoming Report Dispatching to In-basket is not supported with the DICOM Gateway.

1. Select ***Incoming Report Dispatching*** from the navigation tree on the left side of the screen.
2. Select the locations from the drop-down lists (***In-Basket***, ***Database***, or ***Edit List***).

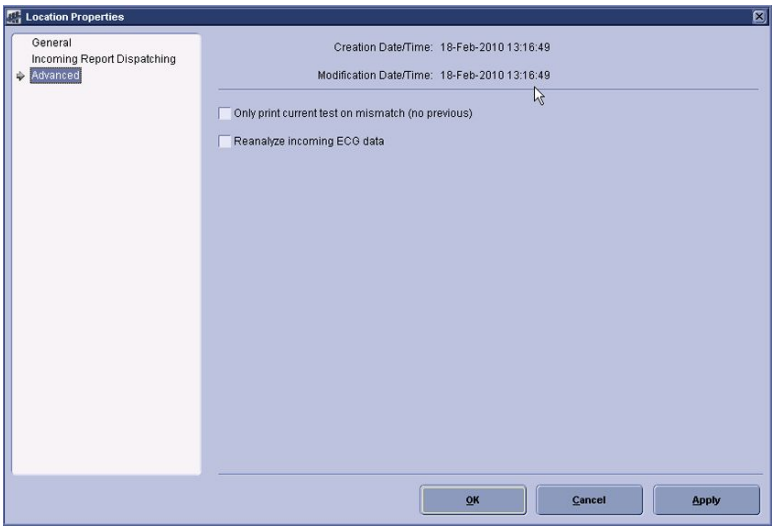


3. If ***In-Basket*** is selected as the ***Destination***, select the In-Basket number from the drop-down list at the ***In-Basket*** field.
4. Click ***OK*** when finished.

Setting Up Locations - Advanced

Set up the cart location at the ***Locations*** > ***Advanced*** window.

1. Select ***Advanced*** in the navigation tree on the left side of the screen.



2. Select the ***Only print current test on mismatch (no previous)*** check box, if appropriate.

   If a first previous is set up for this location, it does not print if there is a mismatch with the current ECG. Only the current ECG prints during routing for this location with a mismatch.

3. Click ***OK***.

Setting Up HIS Locations

You can use HIS Locations in MUSE to map DICOM locations to MUSE locations so that orders downloaded to the ECG device can be filtered by MUSE locations. More than one DICOM location can point to the same MUSE location, but a single DICOM location cannot map to more than one MUSE location.

Creating New HIS Locations

1. On the ***HIS Location*** window, select ***Action***>***New***.

   The ***HIS Locations Properties*** window opens.

2. Type the ***HIS Location Name*** exactly as it would exist in the Current Patient Location, DICOM tag (0038,0300), on the MWL Order (including spaces, special characters, and so on).

   Contact your IT department for the correct location list.

   NOTE:
   The maximum HIS location length is 19.

3. Select the corresponding ***MUSE Location Name*** from the drop-down list.

4. Click ***OK*** when finished.

Setting Up Report Distribution

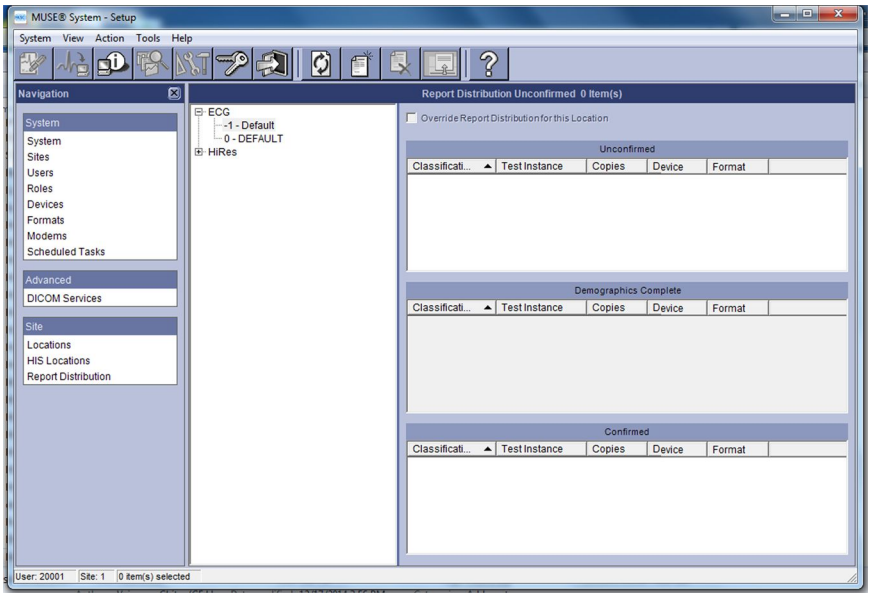
Report distribution allows you to set up where to distribute reports, how many reports to route, and what the reports look like. This is done using a default location or a per location basis.

Unconfirmed routes in report distribution route when tests are transmitted into the system.

NOTE:

Demographics Complete and ***Confirmed*** routes are not applicable for use with MUSE DICOM Gateway Pro and are disabled.

To open the ***Report Distribution...*** window, select ***Report Distribution*** from the ***Navigation*** pane.



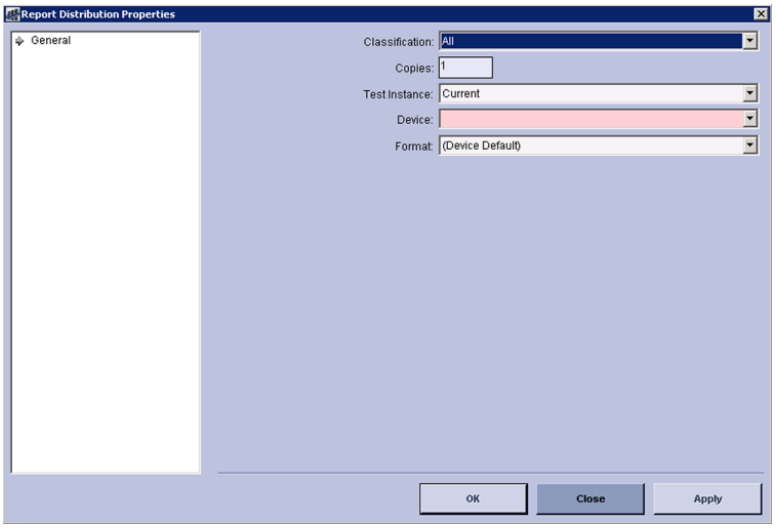
Setting Up Default Actions

Set up a default action for each test type and each location.

1. Select ***1–Default*** >***Action***>***New***.

   The ***Report Distribution Properties*** window opens.

   The default route is the action that is taken for all test locations, unless the location has specified that the route be ***Overridden***.



2. Select the fields as described in the following table:

Field	Description
Classification	Select whether you want this action to be for ***Normal***, ***Abnormal***, or ***All*** reports.
Copies	Enter the number of copies you want printed.
Test Instance	Only ***Current*** Test Instance is supported with MUSE DICOM Gateway Pro.
Device	Select the output device of the report. **NOTE:** ADMITTING MD, ATTENDING MD, ORDERING MD, OVERREADING MD, PRIMARY CAR MD, AND REFERRING MD devices are not supported with the DICOM Gateway.
Format	Select the format to be used for the device. Many devices already have a default ***Format*** at the device level. In this case, do not select a format, but leave it as ***(Device Default)***.
Always route on confirm to database	Select the check box to route the report to the next action each time the user confirms the report to the database on the ***Edit List***.

3. Repeat the previous steps for each data type.

Adding a New Action

Set up a location that does not follow the system default ***Report Distribution***:

1. Select the appropriate location.
2. Select the ***Override Report Distribution for this location*** check box.

   If the ***Override Report Distribution for this location*** check box is not selected, the ***Report Distribution*** reverts to the system default.
3. Repeat the steps in "Setting Up Default Actions" on page 66.

5

System Status

This chapter describes the quick link views, the queues, and logs used in the MUSE DICOM Gateway Pro system.

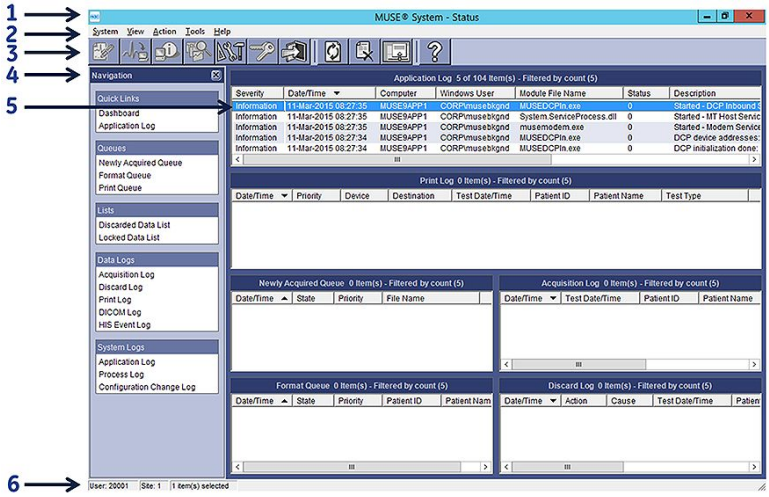
Status Window

The ***Status*** window allows you to view system activity and performance through a series of different views.

To view system information, select ***System*** > ***Status***. The ***Status*** window opens.

NOTE:

You must have proper privileges to view the ***Status*** window.



Status Window Description

Item	Name	Description
1	Title Bar	Displays the name of the current application.
2	Menu Bar	Contains drop-down lists for various functions.
3	Toolbar	Displays icons for easy access to Menu Bar features. The icons change with each screen you view.

Status Window Description (cont'd.)

Item	Name	Description
4	Navigation Area	Provides easy access to ***Quick Links***, ***Queues***, ***Lists***, ***Data Logs***, and ***System Logs***. Selecting a queue, list, or log in the Navigation area opens that view on the main screen.
5	Main Screen	Displays selected queue, list, or log.
6	Status Bar	Provides user, site, and system information.

Status Log, Queue, and Lists Descriptions

The following sections provide a description of the Queues, Lists, and Logs in MUSE Status.

For instructions on retrying and deleting a bad request, displaying the ***Properties*** page, and refreshing the queue, see "Common Tasks Performed Within a Queue or Log" on page 79.

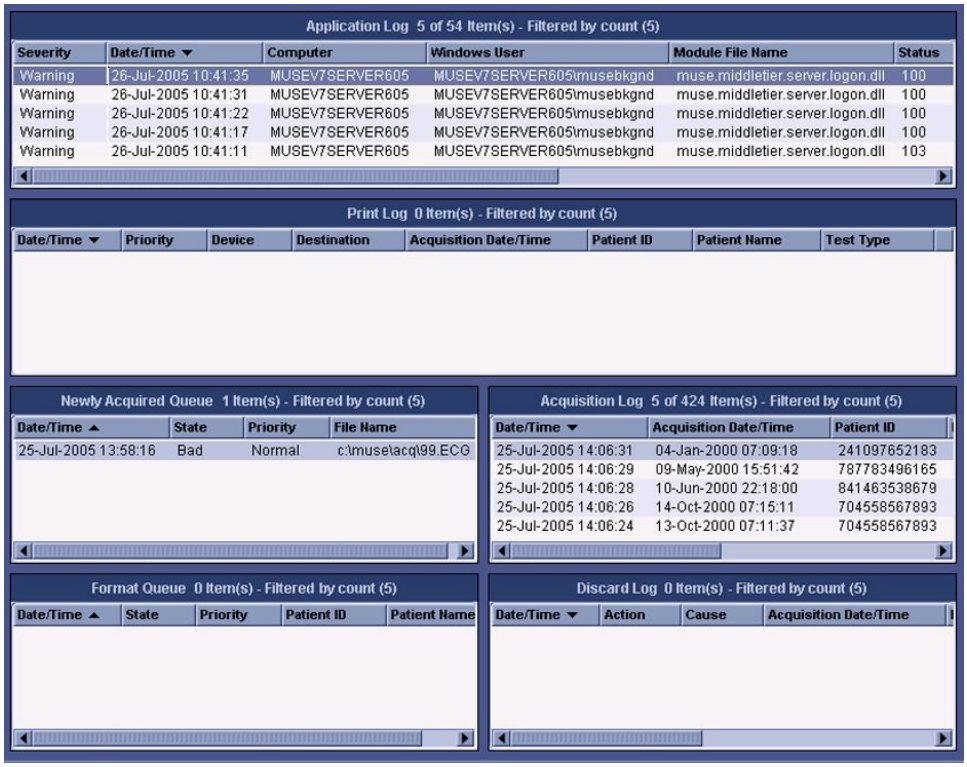
NOTE:

To change the column selection and order of a queue or log, click ***Tools*** > ***Options*** and the name of the queue or log you want to configure. See "Configuring the Queues, Lists, and Logs" on page 77.

Quick Links

This section describes the quick link views available in the MUSE DICOM Gateway Pro system.

Dashboard View



The ***Dashboard*** view summarizes system activity and performance on one screen. While this view provides a large amount of data on a single screen to facilitate overall system performance, using a specific view provides more flexibility and options in diagnosing a particular issue.

To open a specific view, double-click on the title. For example, to open the ***Application Log***, double-click on the title ***Application Log***.

Application Log

The ***Application Log*** is a list of events that occurred in the system. These events can be both status and error messages. For example, a status message can inform you that database search is being run, while an error message is logged because there was an unidentified communication problem while faxing a report.

For instructions on filter logs, see "Configuring the Queues, Lists, and Logs" on page 77.

Queues

This section describes the queues available in the MUSE DICOM Gateway Pro system.

Newly Acquired Queue

The ***Newly Acquired Queue*** is a list of requests for the normalization task to process. Tests to normalize are brought into the system by different acquisition devices. If the normalization of the test is successful, the request is deleted. A request is marked bad if a problem is encountered. You can retry bad requests and manually delete new or bad requests.

If deleting data in the ***Newly Acquired Queue***, the patient test is deleted from the MUSE system.

Format Queue

The ***Format Queue*** is a list of requests for the Formatter task to process. The Normalization task and user interface print requests add items to the format queue. If the formatting is successful, the status is changed to ***Done*** and the request is no longer displayed. A request is marked bad if a problem is encountered. You can retry bad requests with the proper security privileges. You also can delete requests manually.

Print Queue

The ***Print Queue*** is a list of all system and temporary devices the spooler tasks process. The formatter task adds items to spool. If the spooling is successful, the status is changed to ***Done*** and the request is no longer displayed. A device is marked broken if a problem is encountered. You can reset broken devices with the proper security privileges. You also can delete requests manually.

The ***Print Queue*** has a split-window view of two lists. The top list view (device list) displays information about each of the different devices, such as the name, type, documents in its queue, and status. The bottom list view (job list) displays information about each print request for the selected printer.

Resetting a Broken Device

If a print job fails, you can reset the print device from the ***Print Queue*** to retry the failed print job.

1. On the ***Navigation*** pane, click on ***Print Queue***.

   The ***Print Queue*** view opens.

2. Right-click the broken print device in the top list view.

   A menu opens.

3. Click ***Reset***.

Retrying a Print Job

You can retry sending a print job from the ***Print Queue***.

NOTE:
This option is only available for those print jobs that have a failed state. You must have proper privileges to retry requests.

1. On the ***Navigation*** pane, click ***Print Queue***.

   The ***Print Queue*** view opens.

2. Select the print device in the top list view.

   The list of print jobs display in the bottom list view.

3. At the bottom list view (***Job List***), right-click on the entry,

   A menu opens.

4. Click ***Retry*** to retry sending your print job.

Deleting a Print Job

You can delete a print job from the ***Print Queue***.

1. On the ***Navigation*** pane, click on ***Print Queue***.

   The ***Print Queue*** view opens.

2. Select the print device in the top list view.

   The list of print jobs is displayed in the bottom list view.

3. At the bottom list view, right-click on the entry.

   A menu opens.

4. Click ***Delete*** to delete the print job.

Refreshing the Top List View or Bottom List View

The ***Print Queue*** must be refreshed manually to see changes that have occurred after a period of time.

1. Right-click In the top list view or bottom list view window.

   A menu opens.

2. Click ***Refresh***.

Lists

Discarded Data List

The ***Discarded Data List*** is a list of tests that the user or the system has discarded. The system can discard a test because of an invalid site.

Once a test is on the Discarded Data list, a user can delete, restore, correct the site, and correct the acquisition profile.

Restoring a test places it back to the same state it was in at the time it was discarded. For example, if a record was discarded from the ***Edit List***, the record is restored to the

Edit List and it follows the routing and serial comparison setup for that particular site. Actions performed to tests on the ***Discarded Data List*** are logged in the ***Discard Log***.

NOTE:
Deleting a test permanently removes it from the system.

1. To delete a test, perform the following steps:
   a. Highlight the test, right-click, and select ***Delete***.
      The ***Confirm Delete*** window opens.
   b. Click ***Yes***.
      The test is deleted permanently from the system and an entry with a ***Deleted*** action is logged in the ***Discard Log***.
2. To recover a test, perform the following steps:
   a. Highlight the test, right-click, and select ***Recover***.
      The ***Confirm Recover*** window opens.
   b. Click ***Yes***.
      The test is recovered and an entry with a ***Recovered*** action is logged in the ***Discard Log***.
3. To correct a site and recover the test, perform the following steps.
   a. Highlight the test, right-click, and select ***Correct Site and Recover***.
      The ***Confirm Site Correction*** window opens.
   b. Click ***Yes***.
   c. From the list, select the site you want to move the test to and click ***OK***.
      The test is recovered and moved to the corrected site. When the ***Correct Site and Recover*** function is used, it generates both a ***Recovered*** action entry and a ***Deleted*** action entry in the ***Discard Log***. This occurs because the test is recovered to the corrected site and deleted from the original site.

Locked Data List

1. Highlight a test.
2. Right-click and select ***Unlock***.
   A message opens.
3. Click ***Yes*** to continue or ***No*** to exit without unlocking the text.

Data Logs

This section describes the logs available in the MUSE DICOM Gateway Pro system.

Acquisition Log

The ***Acquisition Log*** is a list of tests that were acquired into the system. The log facilitates determining if a test is acquired successfully.

For instructions on filtering logs, see "Configuring the Queues, Lists, and Logs" on page 77.

Discard Log

The ***Discard Log*** is a list of tests that were discarded, deleted, or restored. The system or a user can discard tests.

A user can delete or restore a test in the ***Discarded Data List***, not the ***Discard Log***.

For instructions on filtering logs, see "Configuring the Queues, Lists, and Logs" on page 77.

Print Log

The ***Print Log*** is a list of successful print requests. Currently, unsuccessful print requests are not captured in the system, except for a potential entry in the application log.

For instructions on filtering logs, see "Configuring the Queues, Lists, and Logs" on page 77.

DICOM Log

The ***DICOM Log*** is a list of all processed DICOM transactions such as C-Store, C-Echo, storage commitment, and association requests.

The following details are logged:

Field	Description
Date/Time	Indicates the date and time of the transaction.
Event Type Value	Indicates the logging of different DICOM event types such as C-Store and Storage Commitment requests.
Source AE Title	Indicates the sending of system Application Entity title.
Destination AE Title	Indicates receiving systems Application Entity title.
Description	Indicates the description log.
Source IP	Indicates the IP address of the sending system.
Source Port	Indicates the Port of the sending system
Destination IP	Indicates the IP address of the receiving system.
Destination Port	Indicates the Port of the receiving system.
SOPInstanceID	Indicates the instance UID of the DICOM test being sent/received.
TransactionID	Indicates the UID of the transaction that is currently in process.
AssociationID	Indicates UID of the Association established for a given DICOM event.

For instructions on filtering logs, see "Configuring the Queues, Lists, and Logs" on page 77.

HIS Event Log

The ***HIS Event Log*** is a list of all DICOM MWL Order events the system processed. Double-click on an entry to view more information about an event.

For instructions on filtering logs, see "Configuring the Queues, Lists, and Logs" on page 77.

System Logs

This section describes the system logs available in the MUSE DICOM Gateway Pro system.

Application Log

The ***Application Log*** is a list of events that occurred in the system. These events can be both status and error messages. For example, a status message can inform you that database search is being run, while an error message is logged because there was an unidentified communication problem while faxing a report.

For instructions on filtering logs, see "Configuring the Queues, Lists, and Logs" on page 77.

Process Log

The ***Process Log*** is a list of all of the processes the system executed. This log includes processes currently executing and those that terminated successfully. You can identify current processes because they do not have an end time. Processes with an old start time and no end time have most likely failed and you can investigate them for issues.

For instructions on filtering logs, see "Configuring the Queues, Lists, and Logs" on page 77.

Configuration Change Log

The ***Configuration Change Log*** displays configuration changes that were made by a MUSE user in MUSE ***Setup***.

New in this log are the following columns the column

Column	Definition
ConfigArea	Indicates the configuration item in MUSE setup that was changed.
ConfigArea ID	Indicates the internal ID configuration item in MUSE setup that was changed.
ConfigChangeEventID	Indicates a unique ID for each configuration change that was logged.

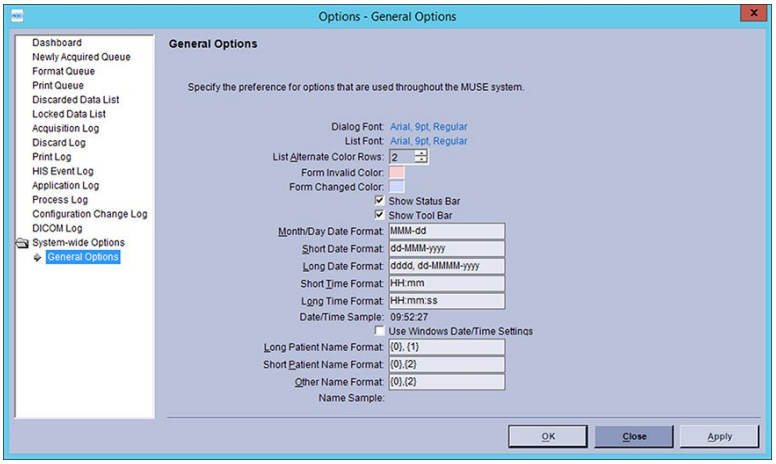
Click on a log entry to view the ***Properties*** window and a list of changes for a particular change event in the ***Details*** tab.

For instructions on filter logs, see "Configuring the Queues, Lists, and Logs" on page 77.

Configuring the Queues, Lists, and Logs

1. On the ***Status*** window, go to ***Tools*** > ***Options***.

   The ***Options window opens***.



2. Highlight ***General Options*** to configure options visible throughout the system as described in the following table:

Field	Description
Changing Fonts	To change the dialog or list font: 1. Place your cursor on the blue font name until a hand appears and the font name is underlined. 2. Click the mouse button. The ***Font*** window opens. 3. Select the font, font style, and size. 4. Click ***OK***.
List Alternate Color Rows	Change the number to customize the number of rows you want shaded in the logs.
Form Invalid Color ***Form Change Color***	To change the color: 1. Double-click the color square. The ***Color*** window opens. 2. Select the appropriate color for each item. 3. Click ***OK***.
Show Status Bar	Select the check box to make the ***Status Bar*** visible at the bottom of the ***Edit List*** window. The ***Status Bar*** displays user, site, overreader, patient, and test information,
Show Tool Bar	Select the check box to make the ***Toolbar*** visible at the top of each system window.

Field	Description
Date Format ***Time Format***	Place your cursor in the appropriate field and make the necessary changes. Refer to the default formats as a reference for configuring these formats. As you make your changes, refer to the ***Date/Time Sample*** field for a representation of the change you are making.
Use Windows Date/Time Settings	Select the check box to use the default Windows date and time formats.
Long Patient Name Format ***Short Patient name Format*** ***Other Name Format***	To customize name formats, place your cursor in the appropriate field and make the necessary changes. Long and Short patient name formats are configured for patient names. Other name format is configured for the ***In-Basket***, ***Referring Physician***, and ***Acquiring Technician***. See the following table of *Sample Formats for Names*.

Sample Formats for Names

	Long and Short Patient Names Formats	Other Name Formats
{0}, {1}	LastName, FirstName	LastName, FirstName
{0}, {2}	LastName, F.	LastName, F.
{0}, {3}	LastName, (Kanji)	LastName, (ID)

3. To configure which columns each queue, list, and log displays, click the appropriate name from the list in the left window pane.
   a. Select the check box of the column headings you want to move or display.
   b. Highlight the column heading and click the ***Move Up*** or ***Move Down*** buttons to display the column heading in that order in the queue, list, or log windows.
   c. For the queues, to display the ***File Data Property*** page, select the ***Display "File Data" property page*** check box.

      Additional information about the entry you are viewing is displayed in a tab labeled ***Data*** when this option is enabled.
   d. For the queues, to display a listing of past entries, select the ***Display "Done" records*** check box.
   e. The MUSE administrator or GE Healthcare service personnel can filter the following logs to create a view relevant your task.
      - Acquisition Log
      - Discard Log
      - Print Log
      - Process Log
      - DICOM Log

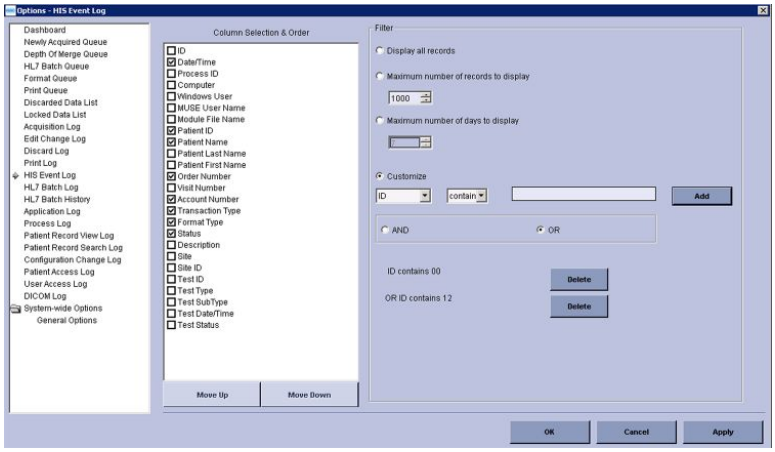
      Select the log name and click the correct option button to set up the desired filters.

You can customize options to build a query to filter a log by selecting a field from the list, the appropriate filter criteria, and entering the appropriate value.

The following logs have the filter option ***Customize***:

- HIS Event Log
- Application Log
- Patient Search Log
- Configuration Change Log

In the following illustration shows an example of the ***HIS Event Log*** filter with the ***Customize*** option.



Click the ***Customize*** radio button to enable the query fields, enter filter criteria, and click ***Add***. Click ***Delete*** to delete the custom query. You can make a query using multiple fields.

Common Tasks Performed Within a Queue or Log

Task	Action
Refreshing	1. Right-click the mouse button. A menu opens. 2. Click ***Refresh***.
Displaying the Properties Page	1. Right-click the mouse button. A menu opens. 2. Click ***Properties***. The ***Properties*** window opens. **NOTE:** Not all queues have a properties page available, such as the ***Print Queue***.

Common Task Performed Within a Queue

Task	Action
Retrying a Request	1. Select a record. 2. Right-click the record. A menu opens. 3. Click ***Retry***. **NOTE:** You must have the proper privileges to retry requests. **NOTE:** ***Done*** entries are automatically purged from the system after the designated number of days specified in ***Scheduled Tasks***.
Deleting a Request	1. Select a record. 2. Right-click the record. A menu opens. 3. Click ***Delete***. **NOTE:** You must have the proper privileges to retry requests. **NOTE:** ***Done*** entries are automatically purged from the system after the designated number of days specified in ***Scheduled Tasks***.

Common Tasks Performed Within a Log

NOTE:
All logs have a refresh, print list, and properties page. See "Common Tasks Performed Within a Queue or Log" on page 79.

Task	Action
Clearing a Log	1. Right-click the mouse button. A menu opens. 2. Click ***Clear Log***. **NOTE:** You must have the proper privileges to clear a log.

6

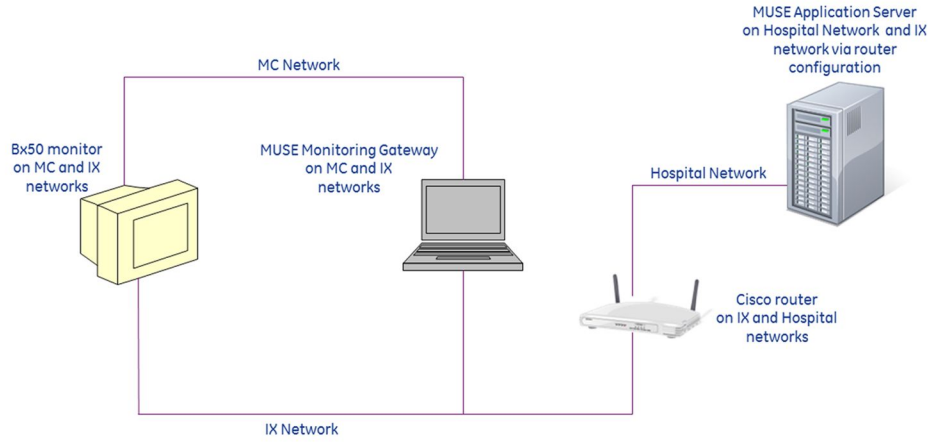
MUSE Monitoring Gateway

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

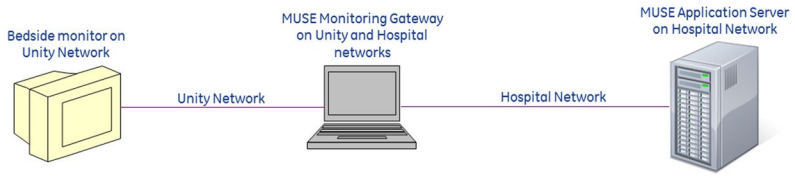
Theory of Operation

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.



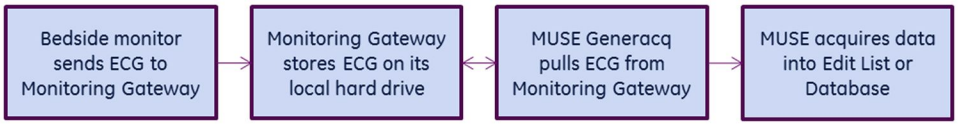
Example Network Diagram — MUSE Monitoring Gateway on the Mission Control and Information Exchange Networks



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:

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	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). If it is a customer configured network, the FE installer must work with the customer to determine appropriate configuration information.

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

System	Requirements
Monitoring Gateway	• Windows 7 Professional, Enterprise, or Ultimate **NOTE:** Only 32-bit English-language versions of Windows 7 are supported. • ***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 ***win.ini*** 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.

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***.

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***.

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.

1. From a bedside monitor, transmit a 12SL ECG to the MUSE system.
2. In the MUSE system, select ***System Status***.
3. Select the ***Acquisition Log***.
4. 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.	You need to add the following exceptions to the firewall: • **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.

7

MUSEAPI3 Installation

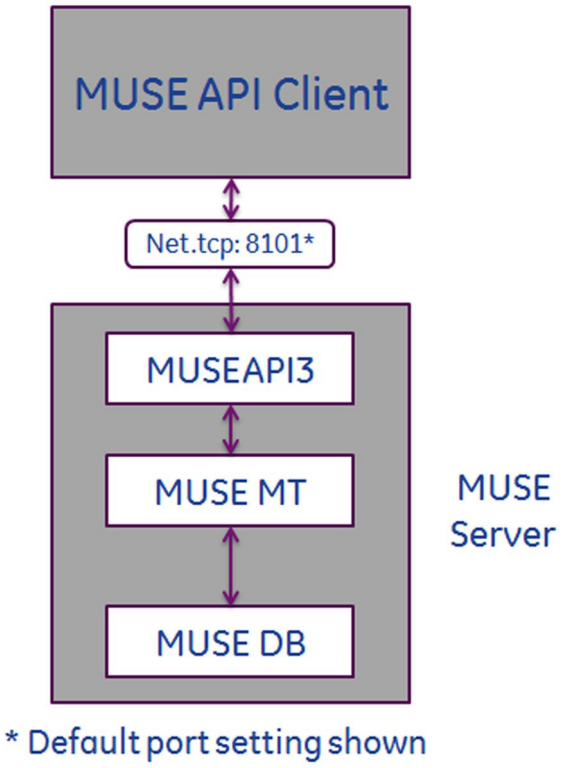
After the main installation of the MUSE DICOM Gateway Pro, the MUSEAPI3 installation begins automatically.

This chapter describes how to install MUSEAPI3 on MUSE DICOM Gateway Pro 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 DICOM Gateway Pro server and allows MUSE API clients, including CV Web v3, MUSE Web Compatibility Layer, and MACCRA

Compatibility, to communicate with the MUSE DICOM Gateway Pro system through the MUSE Middle Tier (MUSE MT Host Service).



NOTE:
Third-party developers can use MUSEAPI3 to interface with the MUSE DICOM Gateway Pro 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 DICOM Gateway Pro system may already have MUSEAPI3 installed if you are using CV Web 3 or another MUSEAPI3 client.

Go to Windows Services on the MUSE DICOM Gateway Pro 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 101 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 DICOM Gateway Pro application server.

1. Log on to the MUSE application server using an account that has ***administrator*** privileges on the MUSE DICOM Gateway Pro 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 DICOM Gateway Pro 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***.

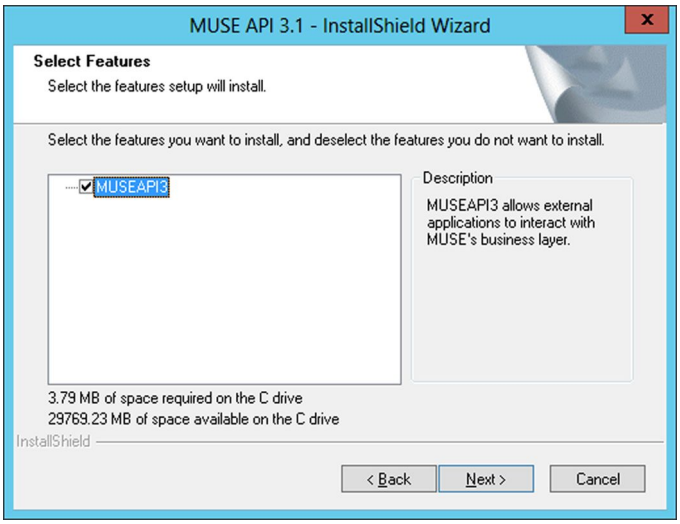
   If a ***User Account Control*** dialog opens, choose ***Yes*** or ***Allow***.

   The ***MUSE API 3.1– InstallShield Wizard*** window opens.
6. Click ***Next***.

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

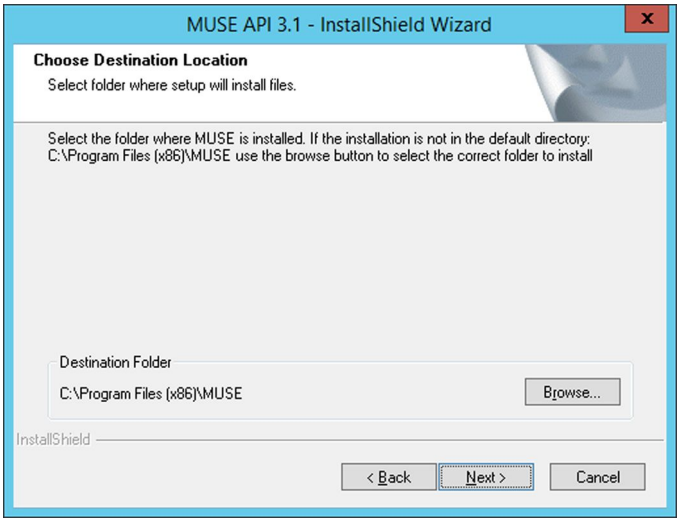
8. Click ***Next***.

   The ***Select Features*** window opens.



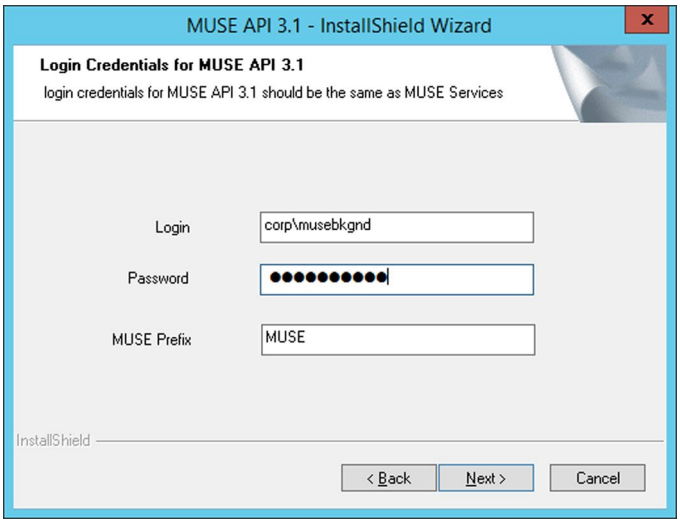
9. Ensure ***MUSEAPI3*** is selected and click ***Next***.

   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.

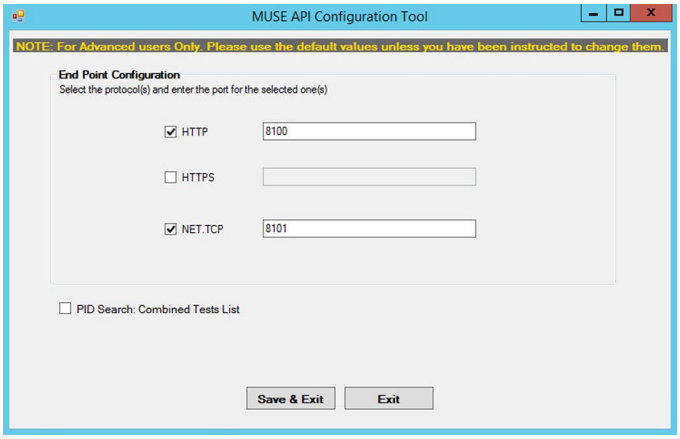
    This should be the same account used for the other MUSE services (typically the domain MUSE Background user).

    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 93.

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.

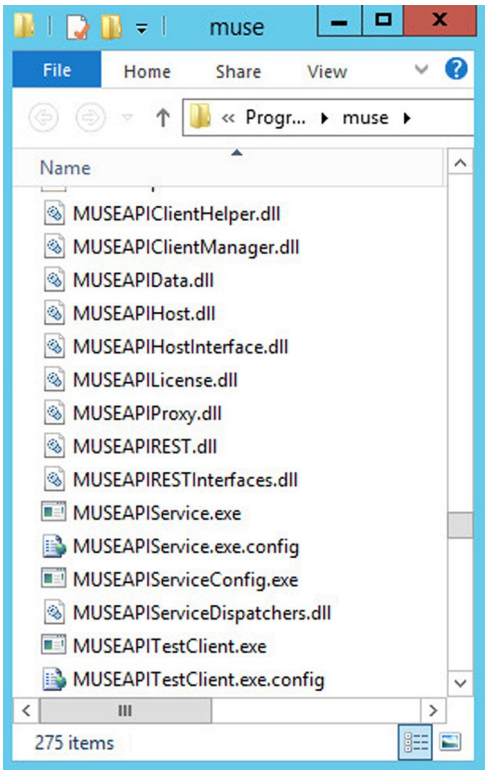
    NOTE:
    MUSE API 3.1 handles patient conflicts within the same MUSE site differently than MUSE API 3.0 did. MUSE API 3.1 only provides a response that includes patient conflicts if there is a Patient ID / Last Name mismatch, and that conflict response can be disabled by enabling this option. MUSE API 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 93.

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 DICOM Gateway Pro 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 DICOM Gateway Pro 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 DCIOM Gateway Pro 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 DICOM Gateway Pro 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 DICOM Gateway Pro Username	The username of a MUSE user whose role includes all privileges in the MUSE DICOM Gateway Pro system. The default is ***museadmin***.
Password	The password of the MUSE DICOM Gateway Pro 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 DICOM Gateway Pro ***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 DICOM Gateway Pro 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 DICOM Gateway Pro 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 ipport=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 ipport=[::]:(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 ipport=0.0.0.0:(port assigned for MUSEAPI3 HTTPS protocol)

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

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

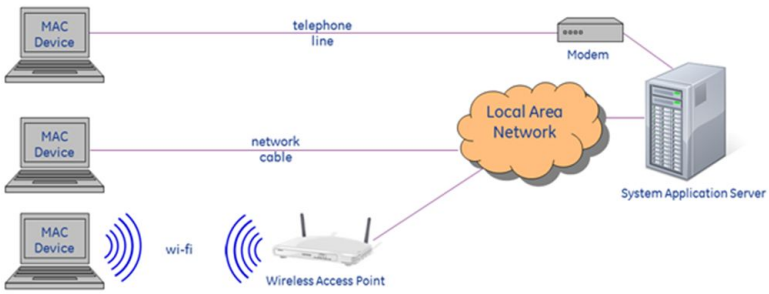
8

MAC Resting ECG Systems to MUSE DICOM Gateway Pro

This chapter describes how to configure MAC Resting ECG systems to send tests to the system.

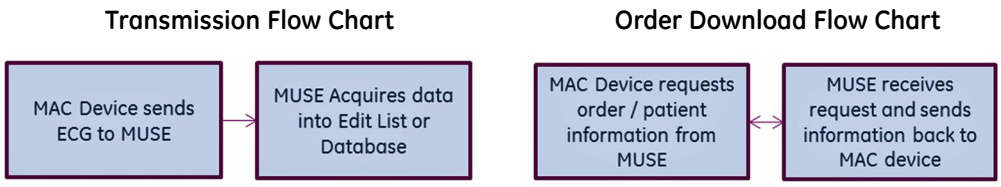
Theory of Operation

MAC Resting ECG to system communication allows you to transfer tests from MAC Resting ECG systems to the system for viewing, editing, printing, and storage. It also allows MAC Resting ECG systems to receive orders and/or patient demographics information from the system.



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

Data Flow Between MAC Resting ECG Systems and the MUSE System



Customer Requirements

The customer is responsible for appropriate serial, telephony, or network connectivity between the MAC Resting ECG systems and the systems where the Modem or DCP Communication feature is defined.

Configuring MAC Resting ECG to Sysem Communication

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

- Modem
  Use "Setting up Modems" for details on setting up modems in the system.
- Wireless Network via CSI
  The following section, "Setting up Modems", has some information on setting up the CSI Network type of modem required for wireless network communication. For detailed information on configuring MAC Resting ECG Systems to have wireless communication with the system, refer to the *MobileLink Installation Manual*.
- Local Area Network via CSI
  The following section, "Setting up Modems", has some information on setting up the CSI Network type of modem required for Local Area Network (LAN) communication. For detailed information on configuring MAC Resting ECG Systems to communicate with the system via local area network, refer to the *LAN Option for MAC Installation and Troubleshooting*.
- Wireless or Local Area Network via DCP (DCAR Communication Protocol)
  Some GE Healthcare MAC Resting ECG systems can use DCP to communicate with the system. The following section, "Setting Up DCP Inbound Communication" on page 107, has some information on setting up the MUSE DCP Server. For detailed information on configuring MAC Resting ECG Systems to communicate with the system via local area network, refer to the *LAN Option for MAC Installation and Troubleshooting*.

Setting up Modems

The MUSE DICOM Gateway Pro system uses the following modem types to receive data:

MUSE Modem Types

Modem Type	Description
CSI Modem	Supports Plain Old Telephone Service (POTS) modem communication for data upload and order download to compatible MAC Cart Systems. Requires physical modem.
CSI Network	Supports wireless and/or LAN cart connections with compatible MAC systems.

Setting up a Modem Device

Use the following instructions to set up a modem device.

1. Log on to the system as a user with privileges to change ***Setup***.
2. Go to ***System*** > ***Setup***.
3. In the ***Navigation*** panel, select ***Modem***.
4. Perform one of the following steps:
   a. To create a new modem, go to ***Action*** > ***New*** and select on the following:
      - ***CSI Modem***
        Used for physical modems.
      - ***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 select ***Properties***.

      The appropriate ***Modem Properties*** window opens.
5. Type the appropriate values described in the following tables.

Modem Properties

Field	Description
Computer Name	Name of the computer where the modem is physically installed. Typically, this is the application server.
Port	Communication port where the modem is physically connected
Baud	The baud rate is 9600.

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.
Port	Communication port that this virtual connection is using.
Retry Interval in Seconds	Defines the upper limit of the time delay between attempts for the cart to communicate with the 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 Systems:

- *MobileLink Installation Manual*
- *LAN Option for MAC Installation and Troubleshooting*

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

   Click ***Close*** or ***Cancel*** to ignore your changes.

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

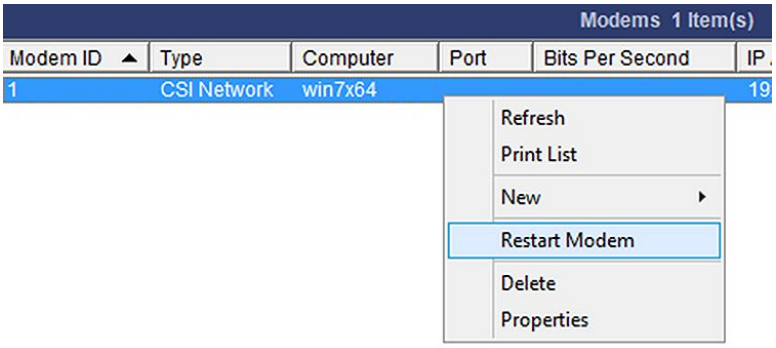
Restarting Modems

The individual threads that are running to support each connection are designed to automatically restart if they stop for some reason.

Use the following procedure if you want to restart them manually:

1. Log on to the system as a user with privileges to change ***Setup***.
2. Go to ***System*** > ***Modem***.
3. Select the modem(s) you want to restart.

   Right-click and select ***Restart Modem***.



You can also restart the modem by selecting the modem and selecting the ***Restart Modem*** icon.

A message opens stating the modem(s) was successfully restarted.

NOTE:
If you do not receive this message, the ***MUSE DICOM Gateway MT Host*** service was not able to communicate to the ***MUSE DICOM Gateway Modem*** services.

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

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

If the connection to a cart fails, the ***MUSE DICOM Gateway Modem*** service immediately attempts to restart the connection. The failure and restart are logged in the ***System Application*** log.

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

If there are three consecutive failures within one minute, a message is logged indicating that error message logging for this modem is stopped until the modem is working again. Halting error messages prevents the ***System 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 DICOM Gateway Pro can receive inbound tests and requests for orders via DCP Inbound communication. Compatible GE MAC Resting ECG systems can use the DCP Protocol instead of CSI to communicate directly with the application server through a wireless connection or a LAN connection.

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

Perform the following steps to modify these defaults:

1. Log on to the MUSE DICOM Gateway Application as a user with privileges to change MUSE Setups.
2. Go to ***System*** > ***Setup***.
3. In the Navigation panel, select ***System***.
4. Right-click on the system entry and select ***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.	Type a new name, if required.
Server port	This is the port that the ***DCP Inbound*** service is listening for inbound connections on. The default port is 9240.	Type a new port number, if required.
Network Interfaces	Specify on which network interface the DCP Server should listen. This field is blank by default so it will listen on all network interfaces on the MUSE DICOM Gateway Pro application server.	To configure the DCP Server to only listen 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 DICOM Gateway Pro system on a compatible DCP client device such as a MAC 2000. Multiple server addresses may be listed if the Network Interface field is blank.	Type the full URL for the service address.

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

   Click ***Close*** or ***Cancel*** to ignore your changes.

   NOTE:
   Refer to the *LAN Option for MAC Installation and Troubleshooting* for detailed installation and configuration information to use the DCP Protocol on compatible MAC system.

8. If any configuration changes were made, restart the ***MUSE DICOM Gateway DCP Inbound*** service on the system application server.

9

DICOM Communication

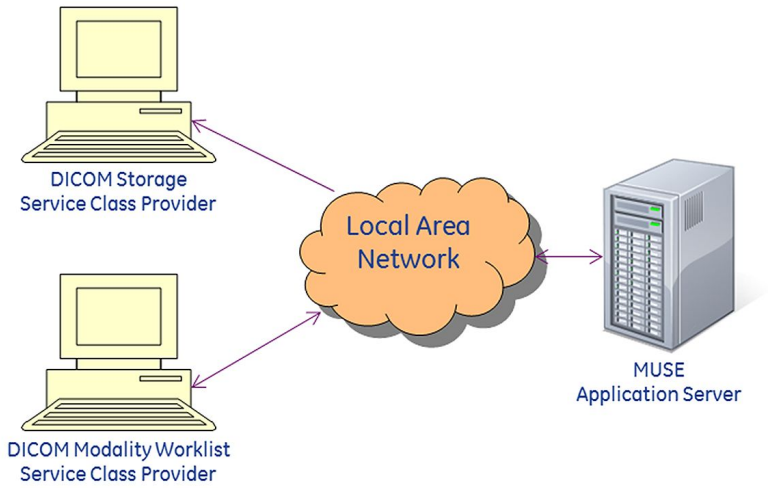
This chapter describes how to configure the system for DICOM communication. For detailed information on system DICOM conformance, refer to *DICOM Conformance Statement for MUSE v9 and MUSE DICOM Gateway Pro*.

Theory of Operation

The system supports DICOM functionality in two ways. The following table provides a description of each.

DICOM Storage Service Class User (SCU)	Allows tests to be sent from the 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 local system orders database. The system acts as a DICOM Modality Worklist Service Class User.

The following diagram shows network communication between the MUSE application server and the DICOM storage service class provider and the DICOM modality worklist service class provider.



Example Network Diagram

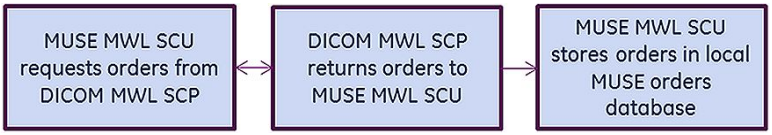
Transmission Flow Charts

DICOM SCU to DICOM SCP Flow Chart

The system 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 system sends a storage commitment request to the DICOM SCP and the DICOM SCP returns a storage commitment response to the system.

Modality Worklist SCU Flow Chart

The DICOM modality Worklist service class user service queries the DICOM modality Worklist service class provider for orders. Returned orders are created or updated in the system orders database.



MUSE DICOM Gateway Services

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

MUSE Service Name	DICOM Function
MUSE DICOM Gateway DICOM Modality Worklist Client	DICOM Modality Worklist (MWL) Service Class User (SCU)
MUSE DICOM Gateway DICOM Storage User	DICOM Storage Service Class User (SCU)

In addition to the services listed in the table, the ***MUSE DICOM Gateway Normal*** service is used to normalize all inbound DICOM test data. The ***MUSE DICOM Gateway Format*** 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-DICOM services and devices.
- AE titles, IP addresses, and ports for all non-DICOM services and devices.

Configuring DICOM Communications

This section provides instructions to configure the system for DICOM communication. The procedures are:

- "Configuring the System to Send DICOM Tests" on page 111
- "Configuring the System to Query for DICOM Orders" on page 114

Configuring the System to Send DICOM Tests

To configure the system to send DICOM tests, you need to perform the following procedures:

1. Configure the DICOM storage user service.
2. Configure the outbound DICOM device in the system.
3. Configure the DICOM device(s) to receive DICOM test from the system.

Configure 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 MUSE DICOM storage user service:

1. Log on to the system application.
2. 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***.	Change the default if required, and type 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.	Change the default if required, and type a new port.
Maximum Wait Time	The maximum time the system waits for storage commitment responses. Default is 60.	Change the default if required, and type a new value.
Maximum retries	The number of storage commitment requests the system makes. Default is 3.	Change the default if required, and type a new value.

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, you need to restart the ***MUSE DICOM Gateway DICOM Storage User*** service on the system application server.

Configure 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.

Perform 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 on to the system application.
2. Go to ***System*** > ***Setup***.
3. Select ***Devices***.
4. Perform one of the following:
   a. To create a new device, go to ***Action*** > ***New*** and select one of the following device types.

      The device types are based on the compatibility or preference of the receiving DICOM storage service class provider.

      - ***DICOM IOD***

DICOM Information Object Definition

- ***DICOM PDF***
  DICOM Encapsulated PDF

b. 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 DICOM storage service class provider that is to receive tests from the system.	Type the IP address .
Port	The port number of the DICOM storage service class provider that is to receive tests from the system.	Type the port number.
Send Original IOD if available	If this option is enabled, the original data initially acquired is sent for export. **NOTE:** This option is only available for DICOM IOD device types. When used with the MUSE DICOM Gateway Pro, this option has no impact as the test will never be modified by the MUSE Editor.	Select the box to enable this option. Do not select the box to disable the option.
Supports Storage Commitment	If the DICOM storage service class provider supports storage commitment, this box can be checked to enable it. If storage commitment is enabled, the system sends storage commitment requests to the DICOM device storage commitment service using information configured here.	Select the box to enable this option. Do not select 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.

Field	Description	Action
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.

Configure 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.

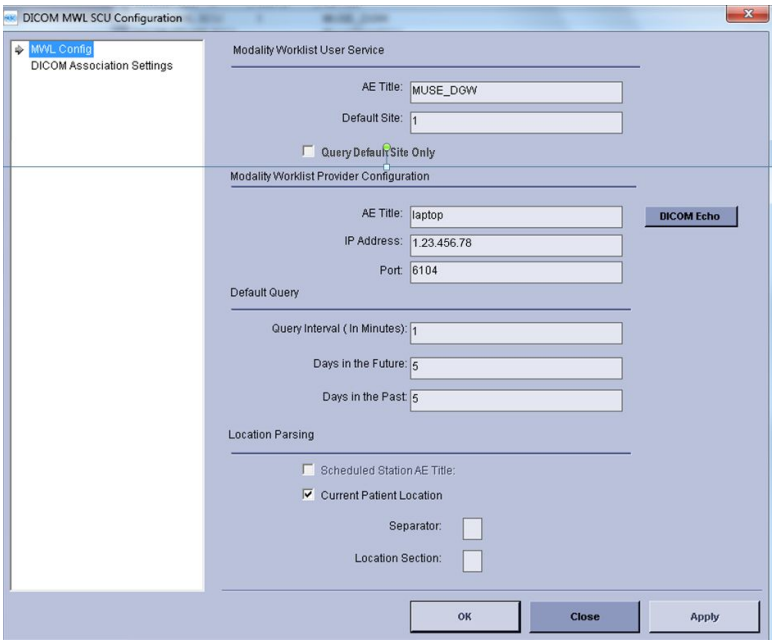
Configure the System DICOM Modality Worklist Client Service

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 with which 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: • Scheduled Station AE Title • Current Patient Location	Select the field from the Orders received through DMWL that should be usde 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. 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-Room 204-Bed 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***. If a match is not made to a MUSE ***HIS Location Full Name***, the order is not associated with any MUSE 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.	

6. 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.

7. 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.

10

System Checkout

Checking out the System

This checkout procedure should be performed after completing all configurations. Use this procedure to verify communication between the ECG cart and DICOM systems.

1. Confirm that the following services are started.
   - MUSE DICOM Gateway
   - MUSE DICOM Gateway DCP Inbound
   - MUSE DICOM Gateway DICOM Modality Worklist Client
   - MUSE DICOM Gateway DICOM Storage User
   - MUSE DICOM Gateway Format
   - MUSE DICOM Gateway Modem
   - MUSE DICOM Gateway MT Host
   - MUSE DICOM Gateway Normal
   - MUSE DICOM Gateway Scheduler
2. Check that the system application can be started and logged on to successfully.
3. Check that the ECG Cart is
   - Configured for use with the system
   - Receiving the patient and order information from the system.

   Perform a test at the ECG cart using the patient information retrieved from the system.
4. Check that the ECG cart can transmit tests to the system.
5. Check that the test was routed from the MUSE DICOM Gateway Pro system to the receiving DICOM Storage Service Class provider.

Transition to Technical Support

The following list should be used as a reference for the Installer Personnel to use when they have completed the installation of the system and are ready transition service of the system to the Remote Technical Support Team:

- Ensure the technical support remote access database and/or Customer Relationship Management (CRM) system has been updated with information on how to remotely access the system.
- Verify the systems can be successfully accessed remotely via InSite ExC.
- Provide the Technical Support team with server names, IP addresses, and InSite serial numbers.
- Provide the Technical Support team with user names, passwords, and domains for the remote systems as appropriate.

11

System Administration

This chapter provides system information and procedures for administrative functions to administer the system.

MUSE DICOM Gateway Pro Services

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

CAUTION:

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

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

MUSE DICOM Gateway Pro Services

Service Name	Description
MUSE DICOM Gateway	MUSE DICOM Gateway Pro Service Control Manager. When started, all MUSE DICOM Gateway services are started. When stopped, all MUSE DICOM Gateway services are stopped.
MUSE DICOM Gateway DCP Inbound	Listens for inbound DCP communication.
MUSE DICOM Gateway DICOM Modality Worklist Client	Used to communicate with DICOM Modality Worklist Service Class Provider to retrieve orders.
MUSE DICOM Gateway Storage User	Used by outbound DICOM Devices in the system.
MUSE DICOM Gateway Format	Formats all system output.
MUSE DICOM Gateway Modem	Supports CSI communication.

MUSE DICOM Gateway Pro Services (cont'd.)

Service Name	Description
MUSE DICOM Gateway MT Host	Handles Middle Tier communications.
MUSE DICOM Gateway Normal	Normalizes tests acquired into the system.
MUSE DICOM Gateway Scheduler	Runs system scheduled tasks.

Application Authentication

The system supports two different methods for application authentication:

- MUSE Authentication
- Windows Authentication

The following sections cover the different authentication method configurations.

MUSE Authentication

With this method, the user launches the system application after logging onto Windows. The system application opens an application logon screen, where the user needs to provide their system user name and password, and the site in the system that they want to log onto, if it is other than their default site.

Windows Authentication

With this method, when the user launches the system application after logging onto Windows, the system application recognizes the user's Windows logon and automatically logs the user into the system application as the appropriate system user.

This setup requires the Windows domain and user credentials be entered into the user's setup in the system application. No Windows password information is required for this setup

Mapping a System User Account to a Windows User Account for Window Authentication

Use the following steps to map a system user account to a Windows user account:

NOTE:
For information on creating system user accounts, see "Adding Users" on page 53.

1. Log on to the MUSE application.
2. Go to ***System*** > ***Setup***.
3. From the navigation panel, select ***Users***.
4. Right-click on the MUSE User to be mapped and choose ***Properties***.

   The ***User Properties*** window opens.

5. In the ***Windows User Name*** field, type the Windows user name to map to this MUSE user in the format ***<domain name>\<user name>***.
6. Click ***OK*** to save your changes.

Application Shortcuts

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

Using the System InstallShield Wizard to Create Shortcuts

During the initial installation of the system or when using the system Modify mode, you are presented with the ***MUSE DICOM Gateway Pro Client Configuration*** settings. The following procedure is for Modify mode, however the information is applicable to the installation of the system as well:

1. Log on to the MUSE application as administrator.
2. Go to ***Control Panel***>***Programs and Features***.
3. Select ***MUSE DICOM Gateway Pro*** and click ***Change***.

   The ***Welcome ...*** window opens.
4. Select ***Modify*** and click ***Next***.

   The ***Select Feature*** window opens.
5. Click ***Next***.

   The ***MUSE DICOM Gateway Pro Client Configuration*** window opens
6. Select the desired shortcuts options on the ***MUSE DICOM Gateway Pro Client Configuration*** window using the information in the following table:

Item	Description	Desktop Shortcut Name
Add Windows Authentication shortcuts	Select to add Windows Authentication shortcuts.	MUSE DICOM Gateway Pro Setup
Add MUSE DICOM Gateway Pro Authentication shortcuts	Select to add MUSE Authentication shortcuts.	MUSE DICOM Gateway Pro Setup (MUSE Logon)

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

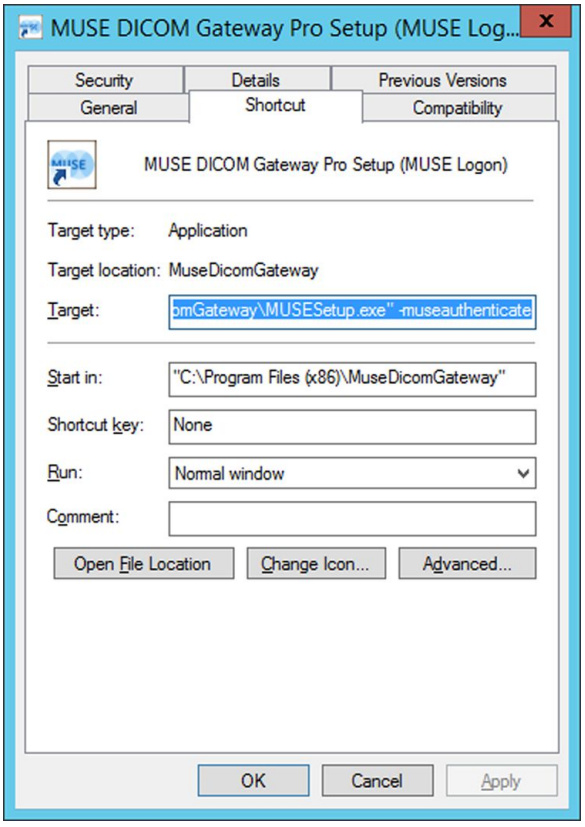
Manually Modify Shortcuts

The command line parameter of the Windows shortcut tells the system which authentication method to use. Rather than use the Modify mode to modify the shortcuts, shortcuts can be modified manually using the below information.

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

Authentication Method	Command-Line Parameter
Windows Authentication	None. No command-line parameter indicates the authentication method is Windows authentication.
MUSE Authentication	***-museauthenticate***

The following screen shows the parameters completed to configure a shortcut for MUSE authentication:



4. Click ***OK***.

Modifying System Installed Configuration

To view or change the current MUSE installed configuration, run the System Installer in Modify mode. Modify mode allows you to:

- Change the computer name of the application server
- Change the data base server
- Change the MUSE port number
- Change the Windows user accounts and passwords

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

CAUTION:

LOSS OF DATA:

Changing settings without knowing how they affect the system can result in data loss.

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

Use the following procedure to change an existing configuration:

1. Close the system application on the server.
2. Go to ***Control Panel*** > ***Programs and Features***.
3. Select ***MUSE DICOM Gateway Pro*** and click ***Change***.

   The ***MUSE InstallShield*** launches.
4. Select ***Modify*** and click ***Next***.
5. Go through the setup steps and make your configuration changes.

   NOTE:

   Click ***Cancel*** at any time to close the program and avoid saving any changes.
6. If no changes are required for a setup window, click ***Next*** on this window IMMEDIATELY to apply your changes.
7. Click ***Next***.

   The ***Maintenance Complete*** window opens.
8. Click ***Finish***.

   MUSE DICOM Gateway services restart.

12

Maintenance

This chapter covers maintenance information for the system.

Server Hardware Maintenance

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

Safe Shutdown Procedures

This section provides safe shutdown procedures for the system.

Shut Down the System Application Server

Use the following steps to shut down the system application server.

1. Before shutting down the server, notify all users of the scheduled shutdown.
2. Stop the MUSE DICOM Gateway services on the system application server.
3. After the MUSE DICOM Gateway services are shutdown, shut down the server following normal Windows shutdown procedures.

Shut Down a Remote Server

If a remove database server is used, use the following steps to shut it down.

1. Shut down the system application server using the instructions in "Shut Down the System Application Server" on page 129.
2. Shut down the remote database server following normal Windows shutdown procedures.

Disaster Recovery

This section covers system disaster recovery information.

System Backup and Recover

A backup and recovery plan is crucial to prevent data loss and to minimize service interruption in the event of system failure or disaster. All system installations are software-only, customer-supplied hardware configurations.

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

Windows Operating System and SQL Server

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

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

MUSE DICOM Gateway Pro System Software

Backing up system software and configurations is the responsibility of the customer.

The MUSE DICOM Gateway Pro and InSite ExC software can be reinstalled in the case of a disaster recovery situation.

Extra steps can be taken to backup the configuration files for each of these items to aid in restoration in a disaster recovery situation. The following table provides file names, default locations, and file descriptions for the system application and InSite ExC:

System Software	File	Default Location	Description
System application	Server.remoting.config	C:\Program Files(x86)\ MUSEDicomGateway	Contains the MUSE port information for the MUSE server; the default port number is 8001.
InSite ExC	Use the instructions in the *InSite ExC Installation Manual* to backup the InSite ExC configuration to a file.		

System Database Backup

System database backup is the responsibility of the customer.

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

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

Knowledge of the MUSE database helps you understand the backup requirements. The system uses the SQL Server database management system (DBMS) and includes the following default user databases:

- ***MUSE_Site0001***
- ***MUSE_SiteTemplate***
- ***MUSE_System***

If additional sites have been set up on the system, additional site databases exists: for example, ***MUSE_Site0002***, ***MUSE_Site0003***, and so on.

System Database Restoration

System database restoration is the responsibility of the customer.

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

System Application Server Disaster Recovery

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

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

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

1. Install physical server
2. Install operating system and SQL Server.
3. Restore system databases
4. Install system software
5. Restore system software configuration(s)
6. Reconnect device(s), as necessary

Multitech MT9324ZBA Modem

The Multitech MT9324ZBA modem is an optional hardware accessory for the system. This manual only references optional hardware that ships with the system at the time of its release.

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

Instructions for installing the modem drivers are located in the MultiTech Modem MT9234ZBA Driver Installation documentation.

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

LED Connectors

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

LED Indicator Name	Description
TD — Transmit Data	Flashes when the modem is transmitting data to another modem.
RD – Receive Data	Flashes when the modem is receiving data.
CD – Carrier Detect	Lights when the modem detects a valid carrier signal from another modem. It is on when the modem is communicating with the other modem and off when there is no connection.
OH – Off-Hook	Lights when the modem is off-hook, which occurs when the modem is dialing, online, or answering a call.
TR – Terminal Ready	Lights when a communication program is using the modem. It means the modem is ready for an outgoing or incoming call. It goes off when the communication program disconnects the serial port. When it goes off, a connected modem also disconnects.
Power	Lights when the system is applying power to the modem.

Replacement Parts

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

A

MUSE Service Users

This chapter describes the following items:

MUSE Service User Accounts

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

Account	Default Account Name	Description
MUSE Administrator	MuseAdmin	The MUSE Administrator account is used by GE Healthcare service personnel to • Log on to the MUSE system to perform initial setup and configuration • Provide ongoing service and support.
MUSE Background	MuseBkgnd	The MUSE Background account is used to • Start the MUSE related background services on the MUSE application server and MUSE client with the MUSE Modem feature • Create new MUSE site databases.

MUSE User Accounts

The default MUSE Administrator and MUSE Background accounts are automatically set up as users within the MUSE application. These accounts are critical to the internal working of the MUSE system and cannot be changed, with the exceptions of their passwords and Windows user names. The MUSE user service accounts are linked to the Windows user service accounts through the ***Windows User Name*** field in MUSE user setup. This linkage happens automatically by the MUSE installer and should only be changed by re-installing the MUSE system or using the MUSE Modify mode.

The MUSEAdmin and MUSEBkgnd user accounts in the MUSE system have known default passwords. The customer should change these passwords for these users. To change the MUSE system passwords for these accounts, see "Changing the MUSE Service Account Passwords in the MUSE System" on page 136.

Windows User Accounts

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

These user names and passwords must meet the following requirements:

- Must be a member of the local ***Administrators*** group on the MUSE application server.
- Must have appropriate access to the MUSE databases on the SQL Server instance where the MUSE databases are located. See the table in "SQL Server Role Requirements" on page 134.
- Should be a domain account whenever possible to avoid mismatches of local account user name and passwords.
- Set passwords to never expire, whenever possible. If the passwords change, GE Healthcare service personnel might not be able to log on to the system to provide support. Additionally, the background services can fail to start, causing the MUSE system to stop functioning.
- Allow the customer to determine both the account names and passwords. The passwords must be shared with GE Healthcare service personnel to use the account when they work on the MUSE system.
- The customer should not use the MUSE Administrator or MUSE Background accounts for accessing the MUSE application server or MUSE system. Instead, separate MUSE and/or Windows user accounts should be created for each individual user accessing the MUSE system.

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

NOTE:

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

SQL Server Role Requirements

The following table provides SQL Server role requirements for the MUSE Administrator and MUSE Background user. For detailed information on implementing these SQL Server roles, see "Configuring SQL Server Security" on page 138.

SQL Server Role Requirements

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

NOTE:

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

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

MUSE InstallShield Wizard Requirements

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

InstallShield Mode	Requirements
Initial Install or Upgrade Mode	• Must be a local administrator of the MUSE application server. • Must have SQL Server Login with the ***sysadmin server role*** on the SQL Server instance where the MUSE databases are created and reside. • Must have ***Master*** configured as the default database for the SQL Server login.
MUSE Modify Mode	SQL Server Login with the ***sysadmin server role*** on the SQL Server instance where the MUSE databases reside. This is the preferred configuration for a local database. OR SQL Server Login with the ***public server role*** on the SQL Server instance where the MUSE databases are located, and database user with ***db_owner database role*** for all of the MUSE databases. This configuration is more common for a remote database. **NOTE:** If the MUSE Administrator and MUSE Background requirements have been met, either user can be used to execute MUSE Modify mode.

Changing MUSE Service Accounts

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

Changing the MUSE Service Account Passwords in the MUSE System

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

1. Log on to the MUSE application.
2. Go to ***Setup*** > ***Users***.
3. Right-click on the account you want to change and select ***Properties***.

   The ***User Properties*** window opens.
4. Type a new password in the ***MUSE Password*** and ***Re-enter MUSE Password*** fields.
5. Click ***OK*** to save your change.

Changing the Windows Accounts and Passwords

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

1. Change or create the Windows accounts and passwords using Windows.
2. Verify SQL Server Logins and Roles.
3. Modify the MUSE installed configuration to:
   - Update the MUSE services with the new user name and password.
   - Update the Windows user name of the ***MUSE Administrator*** and ***MUSE Background*** user accounts.

Change or Create Windows Accounts

The hospital MUSE system and IT administrators are responsible for creating the Windows accounts and passwords. The Windows account user names and passwords used by the new MUSE Administrator and MUSE Background users must be set up and be ready to use before entering them into MUSE. Confirm that the user accounts to be used for the MUSE system meet the requirements specified in "Windows User Accounts" on page 134.

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

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

The hospital MUSE and IT administrators are responsible for ensuring the MUSE Service Users have appropriate SQL Server Logins and Roles. Confirm that the user accounts used for the MUSE system meet the requirements specified in "SQL Server Role Requirements" on page 134.

Modify the MUSE Installed Configuration

After changing or creating the Windows Accounts and Verifying SQL Logins, the MUSE installed configuration needs to be modified with the new accounts and/or passwords. Perform the following steps on the system application server:

1. Log on to Windows as the MUSE Administrator user.
2. Confirm the MUSE application is closed.
3. Go to ***Control Panel*** > ***Programs and Features***.
4. Select ***MUSE DICOM Gateway Pro*** and click ***Change***.

   The ***Welcome...*** window opens.
5. Select ***Modify*** and click ***Next***.

   The ***Select Feature*** windows opens.
6. Click ***Next***.
7. If the following prompt is displayed, ***SQL server 2008 or SQL server 2008 R2 or SQL server 2012 or SQL server 2014 is not installed. This warning can be ignored if you are installing the MUSE database on a different machine. Do you want to continue?***, click ***Yes***.

   The ***MUSE DICOM Gateway Pro Client Configuration*** window opens.

8. Click ***Next*** through each window until the ***MUSE DICOM Gateway Pro Services Configuration*** window opens.
9. Type the user name and password for the ***MUSE DICOM Gateway Pro Background*** account and the user name for the ***MUSE DICOM Gateway Pro Administrator*** account.
   - If you are using a domain account, type the user name in ***<domain name>\<user name>*** format.
   - If you are using a local account, type the user name in ***.\<user name>*** format.

   No password is required for the MUSE DICOM Gateway Pro Administrator user account.

   Using the ***MUSE DICOM Gateway Pro Background*** account and password that you entered in this step, the MUSE installer completes the installation of the MUSE DICOM Gateway services. The MUSE installer also populates the ***MUSE Background*** and ***MUSE Administrator*** accounts in the MUSE database with these same Windows user names and passwords.
10. Click ***Next***.

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

Configuring SQL Server Security

As indicated in the "SQL Server Role Requirements" on page 134, specific SQL Server security requirements must be met for the MUSE Administrator and the MUSE Background users. This section describes the process for configuring SQL Server security.

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

MUSE Background User Access Information

When the system databases are installed or upgraded, the MUSE Background user is made the owner of the databases. This ensures that the MUSE Background user has an SQL database user created for all the MUSE databases and that the user has the ***db_owner*** database role for all of the MUSE databases. If the databases are moved or reattached, the owner can change. In which case, the ***MUSE Background*** account may no longer have ***db_owner*** access to the database.

Create a SQL Server Login

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

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

   You can also use ***Search...*** to locate the user you want to add.
7. Click ***OK***.

Assign SQL Server Roles to a Login

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

1. Using ***SQL Server Management Studio***, log on to the appropriate SQL Server instance using a SQL Server login with ***sysadmin server role*** access.
2. In ***Object Explorer***, expand the database server.
3. Navigate to and expand ***Security*** > ***Logins***.
4. Right-click on the login you want to assign the SQL Server roles to and choose ***Properties***.
5. Select the ***Server Roles*** page.
6. Select any Server roles you want to assign to the SQL Server login.

   NOTE:
   The ***public server*** role is always selected and cannot be cleared.
7. Click ***OK***.

Creating SQL Server Database Users and Assigning Roles

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

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

1. Using ***SQL Server Management Studio***, log on to the appropriate SQL Server instance using a SQL Server login with ***sysadmin server role*** access.
2. In ***Object Explorer***, expand the database server.

3. Navigate to and expand ***Security*** > ***Logins***.
4. Right-click on the login you want to assign the SQL Server roles to and choose ***Properties***.
5. Select the ***User Mapping*** page.
6. In the ***Users mapped to this login*** section of the window, select ***MUSE_System***.
7. In the ***Database role membership for: MUSE_System*** section of the window, select ***db_owner***.
8. Repeat step 6 and step 7 for each of the rest of the MUSE databases (***MUSE_SiteTemplate***, ***MUSE_Site0002***, ***MUSE_Site0003***, etc.).
9. Click ***OK***.

B

Enhanced Patient Race List

Legacy Races

The following table provides the legacy race list that is displayed when ***Enhanced patient race list*** is **not** enabled in ***Setup***.

American Indian
Asian
Black
Caucasian
Eskimo
Hawaiian
Hispanic
Mongolian
Oriental
Other
Pacific Islander
Unknown

Enhanced Race List

The following table provides the race list that is displayed when ***Enhanced patient race list*** is enabled in ***Setup***.

<*blank*>
American Indian
Asian
Asian Indian
Bangladeshi
Black
Burmese

Cambodian
Chinese
Eskimo
Filipino
Hispanic or Latino
Indonesian
Japanese
Korean
Malaysian
Mixed Race
Native Hawaiian or Other Pacific Islander
Other Pacific Islander
Other Race
Pakistani
Polynesian
Singaporean
Sri Lankan
Thai
Vietnamese
White

Auto-mapped Races

Legacy races have been retired in the MUSE v9 system. The following table provides a cross-reference list showing how the legacy races are mapped to the enhanced race list when you enable ***Auto map legacy races*** in ***Setup***.

Retired Legacy Race	Mapped Race in Enhanced Race List when Auto map legacy races enabled
Caucasian	*White*
Hawaiian	*Native Hawaiian or Other Pacific Islander*
Hispanic	*Hispanic or Latino*
Mongolian	*Asian*
Oriental	*Asian*
Other	*Other Race*
Pacific Islander	*Other Pacific Islander*
Unknown	*<blank>*

C

Roles and Privileges

Definitions Table

Following is a list of privileges and the roles associated with them.

Role	Acq. Only	Site Manager	System Owner	MUSE Service	All Privileges
STATUS PRIVILEGES					
View System Status		Yes	Yes	Yes	Yes
View the Newly Acquired Queue		Yes	Yes	Yes	Yes
View the Format Queue		Yes	Yes	Yes	Yes
View the Print Queue		Yes	Yes	Yes	Yes
View the Discarded Data List		Yes	Yes	Yes	Yes
View List of Locked Tests		Yes	Yes	Yes	Yes
View the Acquisition Log		Yes	Yes	Yes	Yes
View the Discard Log		Yes	Yes	Yes	Yes
View the Print Log		Yes	Yes	Yes	Yes
View the Application Log		Yes	Yes	Yes	Yes
View the HIS Event Log		Yes	Yes	Yes	Yes
View the Process Log		Yes	Yes	Yes	Yes
View Configuration Change Log		Yes	Yes	Yes	Yes
View DICOM Log		Yes	Yes	Yes	Yes
Clear the Acquisition Log				Yes	Yes
Clear the Discard Log				Yes	Yes
Clear the Print Log			Yes	Yes	Yes

Role	Acq. Only	Site Manager	System Owner	MUSE Service	All Privileges
Clear the Application Log			Yes	Yes	Yes
Clear the HIS Event Log			Yes	Yes	Yes
Clear the Process Log			Yes	Yes	Yes
Clear Configuration Change Log			Yes	Yes	Yes
Clear DICOM Log			Yes	Yes	Yes
Reset a Device		Yes	Yes	Yes	Yes
Delete Newly Acquired Queue Entry(s)				Yes	Yes
Retry Newly Acquired Queue Entry(s)		Yes	Yes	Yes	Yes
Delete Format Queue Entry(s)		Yes	Yes	Yes	Yes
Retry Format Queue Entry(s)		Yes		Yes	Yes
Delete Print Queue Entry(s)		Yes	Yes	Yes	Yes
Retry Print Queue Entry(s)		Yes	Yes	Yes	Yes
Delete Discarded Data List Entry(s)		Yes	Yes	Yes	Yes
Recover Discarded Data List Entry(s)		Yes	Yes	Yes	Yes
Unlock Tests Locked by Users		Yes	Yes	Yes	Yes
Include option to View “Done" Records in Newly Acquired Queue				Yes	Yes
Include Option to View "Done" Records in Format Queue				Yes	Yes
Include Option to View "Done" Records in Print Queue				Yes	Yes
Include Option to View Binary File Data in Newly Acquired Queue		Yes		Yes	Yes
Include Option to View Binary File Data in Format Queue		Yes		Yes	Yes
Include Option to View Binary File Data in Print Queue				Yes	Yes

Role	Acq. Only	Site Manager	System Owner	MUSE Service	All Privileges
Include Option to View Binary File Data in Discarded Data List				Yes	Yes
SETUP PRIVILEGES					
View System Setup		Yes	Yes	Yes	Yes
Manage System			Yes	Yes	Yes
Manage Sites			Yes	Yes	Yes
Activate/ Deactivate Sites			Yes	Yes	Yes
Manage Users		Yes	Yes	Yes	Yes
Manage Roles		Yes	Yes	Yes	Yes
Manage Devices		Yes	Yes	Yes	Yes
Manage Formats		Yes	Yes	Yes	Yes
Manage Modems			Yes	Yes	Yes
Manage Locations		Yes	Yes	Yes	Yes
Manage HIS Locations		Yes	Yes	Yes	Yes
Manage Report Distribution		Yes	Yes	Yes	Yes
Manage Statement Library		Yes	Yes	Yes	Yes
Modify DICOM Services		Yes	Yes	Yes	Yes
Manage Scheduled Tasks		Yes	Yes	Yes	Yes

Role Description

Role Name	Role Description
Acquire Only	Acquire patient tests.
Site Manager	Manages the MUSE site level configuration.
System Owner	Manages the system level configuration.
MUSE Service	Manages the MUSE service level configuration.
All Privileges	All privileges.

Privilege Descriptions

Privilege Name	Privilege Description Allows the user to...
STATUS PRIVILEGES	
View System Status	View system status.

Privilege Name	Privilege Description Allows the user to...
View the ***Newly Acquired Queue***	View the ***Newly Acquired Queue***.
View the ***Format Queue***	View the ***Format Queue***.
View the ***Print Queue***	View the ***Print Queue***.
View the ***Discarded Data List***	View the ***Discarded Data List***.
View list of Locked Tests	View the list of currently locked tests.
View the ***Acquisition Log***	View the ***Acquisition Log***.
View the ***Discard Log***	View the ***Discard Log***.
View the ***Print Log***	View the ***Print Log***.
View the ***Application Log***	View the ***Application Log***.
View the ***HIS Event Log***	View the ***HIS Event Log***.
View the ***Process Log***	View the ***Process Log***
View ***Configuration Change Log***	View the ***Configuration Change Log***
View ***DICOM Log***	View the ***DICOM Log***
Clear the ***Acquisition Log***	Delete the entry(s) in the ***Acquisition Log***.
Clear the ***Discard Log***	Delete the entry(s) in the ***Discard Log***.
Clear the ***Print Log***	Delete the entry(s) in the ***Print Log.***
Clear the ***Application Log***	Delete the entry(s) in the ***Application Log***.
Clear the ***HIS Event Log***	Delete the entry(s) in the ***HIS Event Log***.
Clear the ***Process Log***	Delete the entry(s) in the ***Process Log***.
Clear ***Configuration Change Log***	Delete the entry(s) in the ***Configuration Change Log***
Clear ***DICOM Log***	Delete the entry(s) in the ***DICOM Log***
Reset a Device	Reset a device.
Delete ***Newly Acquired Queue*** entry(s)	Delete the entry(s) in the ***Newly Acquired Queue***.
Retry ***Newly Acquired Queue*** entry(s)	Retry the entries in the ***Newly Acquired Queue***.
Delete ***Format Queue*** entry(s)	Delete the entries in the ***Format Queue***.
Retry ***Format Queue*** entry(s)	Retry the entries in the ***Format Queue***.
Delete ***Print Queue*** entry(s)	Delete the entries in the ***Print Queue***.
Retry ***Print Queue*** entry(s)	Retry the entries in the ***Print Queue***.
Delete ***Discarded Data List*** entry(s)	Delete the entries in the ***Discarded Data List***.
Recover ***Discarded Data List*** entry(s)	Recover the entries in the ***Discarded Data List***.
Unlock Tests Locked by Users	Unlock tests that are currently locked by other users.
Include Option to View "Done" Records in ***Newly Acquired Queue***	Display "Done" records under ***Status > Options*** for the ***Newly Acquired Queue***.
Include Option to View "Done" Records in ***Format Queue***	Display "Done" records under ***Status > Options*** for the ***Format Queue***.

Privilege Name	Privilege Description Allows the user to...
Include Option to View "Done" Records in ***Print Queue***	Display "Done" records under ***Status > Options*** for the ***Print Queue***.
Include Option to View Binary File Data in ***Newly Acquired Queue***	Display the file data property page under ***Status > Options*** for the ***Newly Acquired Queue***.
Include Option to View Binary File Data in ***Format Queue***	Allows the user to display the file data property page under ***Status > Options*** for the ***Format Queue***.
Include Option to View Binary File Data in ***Print Queue***	Display the file data property page under ***Status > Options*** for the ***Print Queue***.
Include Option to View Binary File Data in the ***Discarded Data List***	Display the file data property page under ***Status > Options*** for the ***Discarded Data List***.
SETUP PRIVILEGES	
View ***System Setup***	View the ***System Setup***.
Manage System	Manage the MUSE system.
Manage Sites	Manage MUSE sites.
Activate/Deactivate Sites	Activate or deactivate MUSE sites.
Manage Users	Manage other users.
Manage Roles	Manage roles.
Manage Devices	Manage devices.
Manage Formats	Manage formats.
Manage Modems	Manage modems.
Manage Locations	Manage locations.
Manage HIS Locations	Manage HIS locations.
Manage Report Distribution	Manage report distribution.
Modify DICOM Services	Modify the DICOM services.
Manage Scheduled Tasks	Manage Scheduled Tasks.

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)

EC REP

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

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

www.gehealthcare.com