GE Healthcare

AMX Navigate
Product Privacy & Security Manual

Product Name	**AMX Navigate**
Language	**English**
Revision Information	**Revision 1**

Table of Contents

1.0 Introduction

This manual describes Privacy & Security considerations of the use of AMX Navigate. This manual describes the expected intended use, the Privacy & Security capabilities, and how they are configured.

This manual assumes that the reader understands the concepts of Privacy & Security. Privacy is the property of protecting the personal private interests of patients. Security protects both system and information from risks to confidentiality, integrity, and availability. Security and Privacy work together to help reduce risk to an acceptable level. In Healthcare one must balance privacy, security, and safety as it relates to the intended use of the device.

The Healthcare Delivery Organization (HDO) is encouraged to use risk management procedures to assess and prioritize privacy, security, and safety risks. Using the risk management, HDO's can determine how to best leverage the capabilities provided within the product.

Privacy & Security relevant information can be found at https://securityupdate.gehealthcare.com.

1.1 Product Description

The AMX Navigate is intended to take exposures utilizing film, computed radiography (CR), or wireless detectors, which are intended to replace radiographic film screen systems in all general purpose diagnostic procedures, for digital radiography (DR).

AMX Navigate is a self-contained, battery-operated mobile radiographic imaging system designed to generate diagnostic radiographic images (medical X-rays) that may increase the ability to detect disease or injury early enough for a medical problem to be managed, treated, or cured. Medical X-rays are used in many types of examinations and procedures, some examples include: X-ray radiography (to find orthopedic damage, tumors, pneumonias, foreign objects).

AMX Navigate is indicated for use on adult and pediatric patients for general-purpose diagnostic radiographic examinations and procedures. Its mobility enables general-purpose radiographic procedures throughout the clinical environment, or as needed within the emergency, intensive care, premature birth ward, cardiac and operating departments, for patients that may not be able to be moved or in cases where it is unsafe or impractical to move them to a traditional RAD room.

The system is indicated for taking radiographic exposures of the skull, spinal column, chest, abdomen, extremities, and other body parts with the patient sitting, standing, or lying in the prone or supine position.

This device is not intended for mammographic applications.

The AMX Navigate incorporates AutoGrid, which is an optional image processing software installed as a part of the system's Helix image processing software. AutoGrid can be used in lieu of an anti-scatter grid to improve image contrast in general radiographic images by reducing the effects of scatter radiation.

2.0 Abbreviations and Definitions

2.1 Abbreviations

AIDE	*Advanced Intrusion Detection Environment*
CCS	*Critical Care Suite*
CSV	*Comma Separated Value*
DHCP	*Dynamic Host Configuration Protocol*
DICOM	*Digital Imaging and Communication in Medicine*
DNS	*Domain Name System*
FDA	*Food and Drug Administration*
HDO	*Healthcare Delivery Organization (i.e. Hospital, Clinic, etc.)*
ID	*Identity*
LAN	*Local Area Network*
LDAP	*Lightweight Directory Access Protocol*
MDS2	*Manufacturer Disclosure Statement for Medical Device Security*
PACS	*Picture archiving and communication system*
PHI	*Protected Health Information*
PI	*Personal Information*
QCS	*Quality Care Suite*
SBOM	*Software Bill of Materials*
SOP	*Service-Object Pair (DICOM)*
SSL	*Secure Socket Layer*
TLS	*Transport Layer Security*
UID	*Unique Identifier (DICOM)*
USB	*Universal Serial Bus*
VPN	*Virtual Private Network*
XML	*Extensible Markup Language*

2.2 Definitions

Class A	*A user access level with the most limited access to configurations and settings. This access level has all the privileges and capabilities needed to setup the system and configure it for day-to-day clinical use.*
Class C	*A user access level with limitations on access to configurations and settings, Class C is a purchasable option by the customer of a 3rd party service provider. GE may subcontract some servicing duties.*
Class M	*A user access level that has access to all the configuration settings and servicing features on the system. This is reserved for GE personnel (GE Service/Engineers).*
Locale Archive	*Archive containing images and patient information, residing locally on the AMX Navigate.*
InSite Agent	*The client part of the InSite ExC platform. The Agent is integrated in the AMX Navigate.*
InSite ExC	*A GE Healthcare remote service platform.*
InSite Server	*The server part of the InSite ExC platform.*
Online Center	*GE Healthcare Online Support Center*

3.0 Privacy & Security Environment

The GE Healthcare AMX Navigate has been designed for an intended use with the following expectations of Privacy & Security protections included in the environment where this product will be used:

- The AMX Navigate should be connected to a secured hospital network via ethernet cable or a Wi-Fi network.
- The AMX Navigate should be physically secured such that the system is inaccessible to unintended users.
- The default application users and passwords should be replaced with customized users and passwords. See Section 4.2.2 “Management of Application User Accounts”.
- External media containing images, patient data, reports, and logs should be secured. When no longer in use, the data should be securely erased and/or the media should be securely deleted.

4.0 Authentication, Authorization and Audit Logging

The GE Healthcare AMX Navigate incorporates a broad assortment of capabilities to enable Privacy & Security. This section describes the capability and use of these Privacy & Security capabilities.

4.1 Access Controls

The access control features of AMX Navigate may be used to help control access to sensitive information. Access control includes user account creation, assigning privileges

4.2 Identity Provisioning

The provisioning of user/badge accounts includes the steps of account creation, maintenance, and suspension of the account when it is no longer needed. A user account is created for the use by a specific individual. This user account is associated with access rights and is recorded in security audit logging.

4.2.1. Management of Operating System User Accounts

The operating system is delivered from the factory with several predefined operating system user accounts.

The intended use of the system does not require a user to interact with the Operating System (OS). Hence, the system provides no User Interface (UI) mechanisms for the OS user accounts or passwords to be changed. The OS account passwords, however, are unique to each system.

It is recommended to establish operational procedures to monitor appropriate system usage such as periodically reviewing system and audit logs.

4.2.2. Management of Application User Accounts

This section describes privacy and security aspects of account management. For specific instructions on how to operate the UI, please refer to Appendix A of the *AMX Navigate Operator Manual, 5845272.*

The AMX Navigate system is delivered from the factory with two predefined user accounts:

- **admin**: the default administrator user account
- **geservice**: a GE user account for Class M servicing

When receiving the AMX Navigate or after installing, it is recommended that the customer takes the following steps to ensure control of the user accounts:

- Create user accounts for each user of the system or use the Enterprise Access Authorization and Audit (EA3) feature to connect with an Enterprise user database. See Appendix A of the *AMX Navigate Operator Manual, 5845272.*
  - It is recommended to create individual user accounts for each person who will use the system. This is required to associate actions performed on the system with individual persons in the audit records.
  - Give each user the privilege they need to perform their required tasks.
  - Only provide administrative rights to those users intended to perform administrative tasks on the system.
- Maintain user accounts
  - It is recommended to establish a routine for removal of user accounts that are no longer in use.

The AMX Navigate allows the customer to set the following password policies:

- Maximum logon attempts before lock
- Lock duration
- Minimum password length (6-255 characters)
- Maximum password length (6-255 characters)
- Minimum Password Retention Period (0 – 1 days)
- Password Expiry Period (0 – 1024 days)
- Advanced password rules
  - 1 Number
  - 1 Lowercase
  - 1 Uppercase
  - 1 Non-alphanumeric
  - Cannot contain 3 consecutive identical characters
  - Cannot contain whitespace character

In addition, the password cannot include the logon name of the user account, and cannot be a palindrome.

4.3 User Authentication

The User Authentication step is verifying that the user attempting to use the system is indeed the user associated with the account given. This section covers the administration of the authentication system to be used.

For specific instructions on how to operate the UI, please refer to the Appendix A of the *AMX Navigate Operator Manual, 5845272.*

4.3.1. Secure Login

A user authenticated by a valid username and password will be granted access to the AMX Navigate. The product supports the following authentication methods:

- Username and password login via local login management
- RFID badge reader login via local login management
- Username and password login via an Enterprise LDAP solution through the Enterprise Access Authorization and Audit (EA3) feature

Secure Login is enabled by default, but can be disabled or reenabled by a GE service engineer upon request.

4.3.2. Emergency Login

The AMX Navigate allows users to login without user credentials via an Emergency Login mode. This mode is provided to support medical emergencies in which logging in normally can jeopardize a patient's wellbeing

Emergency login does not require the user to input valid authentication credentials. The system will prompt the user to enter a name into the dialog box for auditing purposes.

Emergence login will allow exposures, but does not allow connection to the HIS/RIS or PACs hosts and does not allow for configuration of system preference or administrative access. This feature is disabled by default.

4.4 Assigning Access Rights

4.4.1. User Access Rights

The Assigning of Access Rights is the administrative process to associate permissions with user accounts.

A user defined on the system will be assigned with a set of operator rights. This is done by granting the user account membership to a specific role-based group in the system. User accounts and user badges may be individually disabled to prohibit the logins of specific users. Only users with administrator privileges have access to manage user accounts.

User accounts and user badges may be individually disabled to prohibit the logins of specific users.

The following group access roles are supported:

- Limited User
- Standard User
- Administrator User

For details, see Appendix A of the *AMX Navigate Operator Manual, 5845272.*

4.4.2. Service Access Rights

Service access provides the service engineer with greater access to the system than the clinical user. Class C users may configure additional settings than those provided by administrator user accounts. The Class M user has access to all configuration capabilities.

A user can initiate remote service by placing a call to the GE back office or through the iLinq button on the user interface. In response for this service request, a GE representative may log in remotely. Only GE representatives can establish a remote service session. See Remote Service Section 7.2. A user can terminate the remote connection by power the system off or an administrator user can turn off the connectivity in the service user interface.

4.5 Audit Logging and Accountability Controls

Privacy & Security Audit Logging and Accountability Controls support Security surveillance and Privacy investigations and reporting. With this feature, one can audit user's activities, detect instances of non-compliant behavior, determine compliance with security policies, and assist with detecting improper creation, access, modification, and or deletion of protected health information by collecting usage data. The data itself constitutes the audit trail while the collection and review of data is called security auditing.

The AMX Navigate provides integrated functionality for audit logging including audit logging of privacy and security related events. The system also provides support of a local log viewer and the capability to transfer audit logs to a customer’s remote system log server.

4.5.1. Scope of Audit Trail Event logging

Event	Event Type
System Start	Application Activity
Shutdown System	Application Activity

Patient/Study Create	DICOM Instances Accessed
Patient/Study Read(Worklist)	Patient Record
Patient/Study Read(IM)	DICOM Instances Accessed
Patient Update Browser	Patient Record
Copy exam	DICOM Instances Accessed
Auto Push Start	Begin Transferring DICOM Instances
MPPS Start(N-CREATE and N-SET)	Begin Transferring DICOM Instances
Auto Push Complete	DICOM Instances Transferred
MPPS Complete (N-CREATE and N-SET)	DICOM Instances Transferred
Manual Push Start Image	Begin Transferring DICOM Instances
Manual Push Start Dose SR	Begin Transferring DICOM Instances
Manual Push Complete Image	DICOM Instances Transferred
Manual Push Complete Dose SR	DICOM Instances Transferred
Auto Print Start	Begin Transferring DICOM Instances
Manual Print Start	Begin Transferring DICOM Instances
Auto Print Completed	DICOM Instances Transferred
Manual Print Completed	DICOM Instances Transferred
Study Delete	DICOM Study Deleted
Series Delete	DICOM Instances Accessed
Image Created	DICOM Instances Accessed
Image Review (Manual)	DICOM Instances Accessed
Image Update (Manual)	DICOM Instances Accessed
Image Delete	DICOM Instances Accessed
Login Clinical User	User Authentication
Logout Clinical User	User Authentication
System Auto-Lock	Security Alert
Worklist Query (Auto)	Query
Worklist Query (Manual)	Query
Local Service Session Start	Security Alert
Local Service Session Stopped	Security Alert
Image Host/Dose Host Added	Security Alert
MPPS Host Added	Security Alert
Worklist Host Added	Security Alert
Storage Commitment Host Added	Security Alert
Image Host/DoseSR Host Update	Security Alert
MPPS Host Update	Security Alert
MPPS Host Update	Security Alert
Worklist Host Update	Security Alert
Storage Commitment Host Update	Security Alert
DICOM Verification Association Failure (DICOM TLS)	Security Alert
DICOM Verification Association Failure (DICOM NonTLS)	Security Alert
DICOM Image Push Association Failure (DICOM TLS)	Security Alert

DICOM Image Push Association Failure (DICOM Non TLS)	Security Alert
DICOM Image Print Association Failure (DICOM TLS)	Security Alert
DICOM Image Print Association Failure (DICOM Non TLS)	Security Alert
DICOM Dose SR Push Association Failure(DICOM TLS)	Security Alert
DICOM Dose SR Push Association Failure(DICOM Non TLS)	Security Alert
DICOM MPPS N-CREATE Association Failure(DICOM TLS)	Security Alert
DICOM MPPS N-CREATE Association Failure(DICOM Non TLS)	Security Alert
DICOM MPPS N-SET Association Failure (DICOM TLS)	Security Alert
DICOM MPPS N-SET Association Failure (DICOM Non TLS)	Security Alert
DICOM Worklist Query Association Failure(DICOM TLS)	Security Alert
DICOM Worklist Query Association Failure(DICOM Non TLS)	Security Alert
Change User Password	Security Alert
Update User Name	Security Alert
Adding Group	Security Alert
Removing Group	Security Alert
Adding User	Security Alert
Removing User	Security Alert
Add User To Group	Security Alert
Remove User From Group	Security Alert
Group Roles Changed	Security Alert
SUIF Firewall Configuration	Security Alert
Manual Change Of time Or Date Or Timezone	Security Alert
Enterprise Authentication Enabled	Security Alert
Enterprise Authentication Disabled	Security Alert
Enterprise Authentication Successful	User Authentication
Enterprise Authentication Failed	User Authentication
Enterprise Authentication With Invalid User	Security Alert
Enterprise Cache Authentication Successful	User Authentication
User Updated	Security Alert
Enterprise Cache Authentication Failed	User Authentication
Login Emergency User	Security Alert
Logout Emergency User	User Authentication
User Lock Flag Enabled	Security Alert
User Lock Flag Disabled	Security Alert
User Password Reset On Next Logon Enabled	Security Alert
User Password Reset On Next Logon Disabled	Security Alert
Emergency Login Enabled	Security Alert
Emergency Login Disabled	Security Alert
Enterprise Server Connection Configuration Changed	Security Alert
Bad Connection To Enterprise Server	Security Alert
Good Connection To Enterprise Server	Security Alert
NTP Sync Re-Established	Security Alert

NTP Sync lost	Security Alert
NTP Server Changed	Security Alert
Service Key Insert	Security Alert
Service Key Remove	Security Alert
USB Insert	Security Alert
USB Remove	Security Alert
Remote Service : Service event enabled	Security Alert
Remote Service : Service event disabled	Security Alert
Antivirus enabled	Security Alert
Antvirus disabled	Security Alert
Image Host/DoseSR Host Deletion	Security Alert
MPPS Host Deletion	Security Alert
MWL Host Deletion	Security Alert
Storage Commitment Host Deletion	Security Alert

4.5.2. Audit Log Configuration

4.5.2.1.1 GE Service Prerequisites

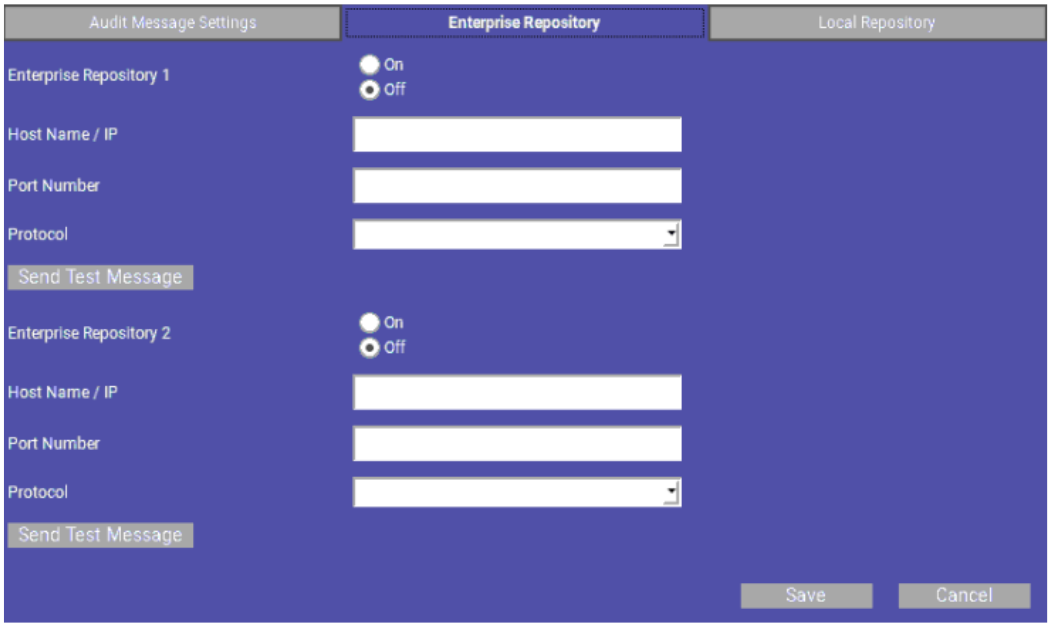
Audit Logs options must be enabled by GE Service personnel

4.5.2.1.2 Configuration

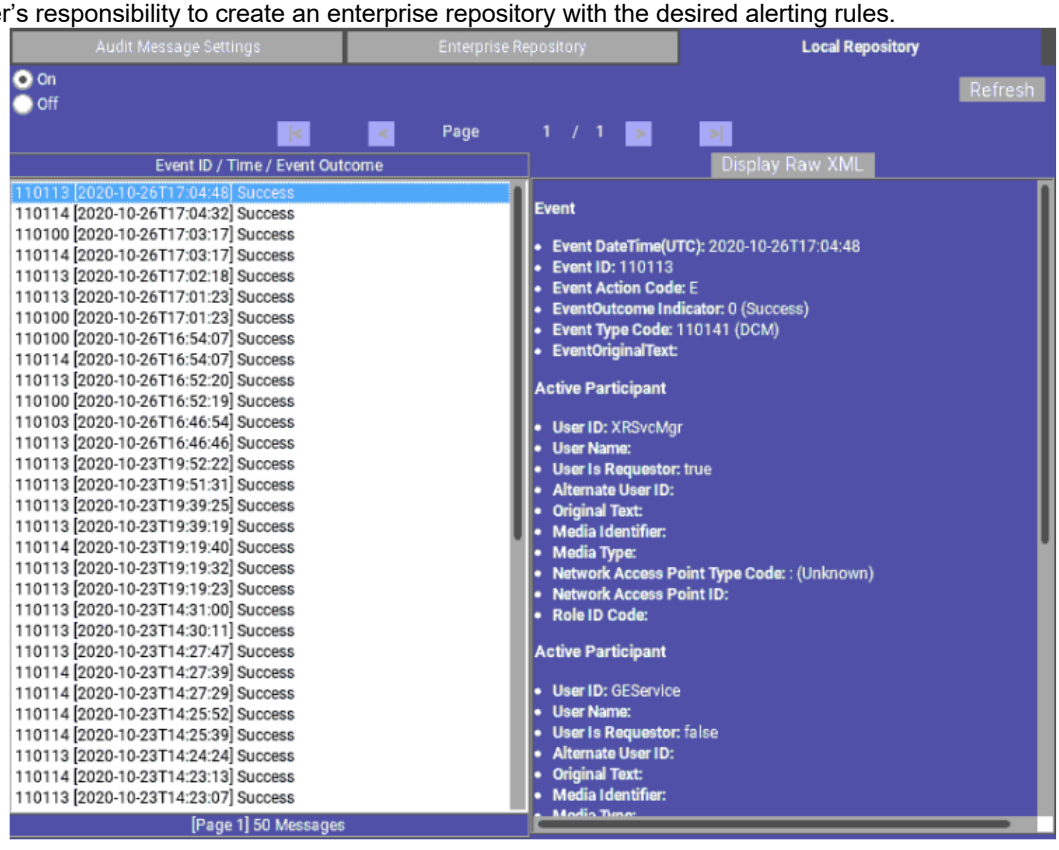
An administrator user can view and configure Audit settings in the service user interface:
(Service → Configuration → Audit Logs)

Configuration options include setting a unique audit source ID for the system and anonymizing patient names through the Audit Message Settings:

The system can also be configured to write audit logs to an enterprise repository, such as a syslog server. Up to two enterprise repositories can be configured. The administrator user must provide the target IP address and port number of the repository and select the protocol from the drop-down menu.



Finally, the system also provides a local log viewer if an enterprise repository is not available. The system itself does not provide any customizable audit controls and does not provide any alerting capabilities. It is the customer's responsibility to create an enterprise repository with the desired alerting rules.



4.6 Patient Privacy Consent Management

Patient Privacy Consent Management is the process of supporting the patient expressing their privacy requirements. This is distinct from other forms of consent such as the consent to treat.

There is no integrated functionality in the system for patient privacy consent management. If needed, operational routines must be established by the customer facility.

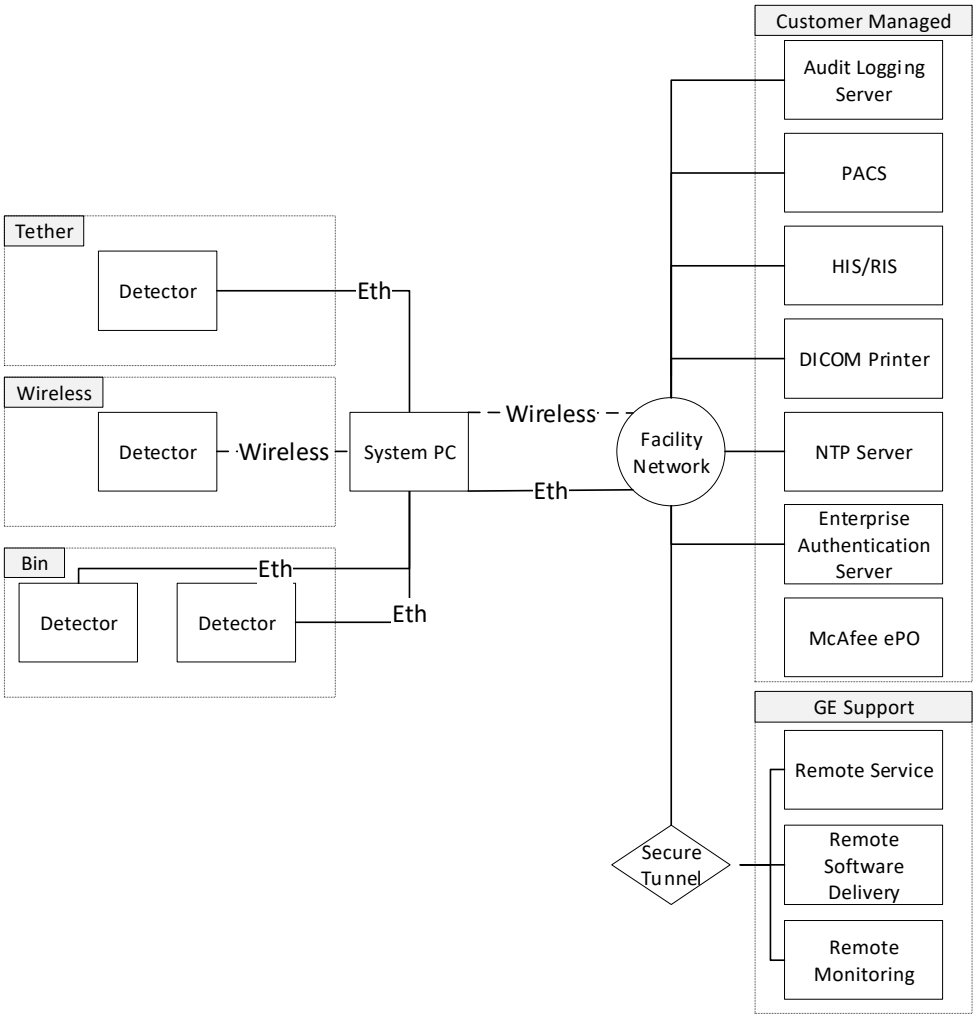
5.0 Information Protection

This section of the manual focuses on Privacy & Security operations and contains information to guide in the preparation of a secure environment for the GE Healthcare AMX Navigate.

Security operations is best implemented as part of an overall “defense in depth” information assurance strategy is used throughout an Information Technology system that addresses personnel, physical security, and technology. The layered approach of defense in depth limits the risk that the failure of a single security safeguard will allow compromise of the system.

5.1 System Interconnections

The AMX Navigate system interconnections are shown below. For a particular installation a subset of the interconnections may be utilized.



Source / Destination	Network Service	Description
PACS	DICOM	DICOM storage of patient images
HIS/RIS	DICOM	DICOM worklist query/retrieve
DICOM Printer	DICOM	DICOM print of patient images
Audit Logging Server	Syslog	Transfer of audit logs from system to facility
NTP Server	NTP	Time synchronization between system and facility
Enterprise Authentication Server	LDAP	Enterprise authentication of users
Remote Service	SSH	Remote service connection session
Remote Software Delivery	SSH	Electronic delivery of OS and software patches
Remote Monitoring	SSH	Monitoring of system status

5.2 Network Security

GE Healthcare strongly recommends that medical devices are operated in a network environment that is separate from an organization's general-purpose computing network. There are many effective techniques for isolating medical devices on a secure sub network, including implementing firewall protection, demilitarized zones (DMZs), Virtual Local Area Networks (VLANs) and network enclaves.

To assist in secure network design, the following network profile outlines the required network services for the AMX Navigate.

Port	*Protocol*	*Direction*	*Network Service*	*Source/Destination*
22	*tcp*	*Outbound / inbound*	*ssh*	*GE VPN tunnel for remote administration*
4010 (configurable)	*tcp*	*outbound / inbound*	*DICOM*	*HIS/RIS, PACS, DICOM Printer, AMX Navigate*
514	*tcp,udp*	*outbound*	*rsyslog*	*Audit logging of system services and audit log capture of logs generated by*
443	*tcp*	*outbound*	*https*	*Insite 2.0 Server*
123	*udp*	*outbound / inbound*	*ntp*	*The system may be configured to sync with an NTP time source.*
389, 636	*tcp*	*outbound / inbound*	*LDAP*	*The system may be connected to the customer's LDAP server for enterprise user authentication*
80, 443	*tcp*	outbound / inbound	McAfee Agent	The system may be connected to the customer's McAfee ePO server for enterprise antivirus management.

5.2.1. Remote Software Control

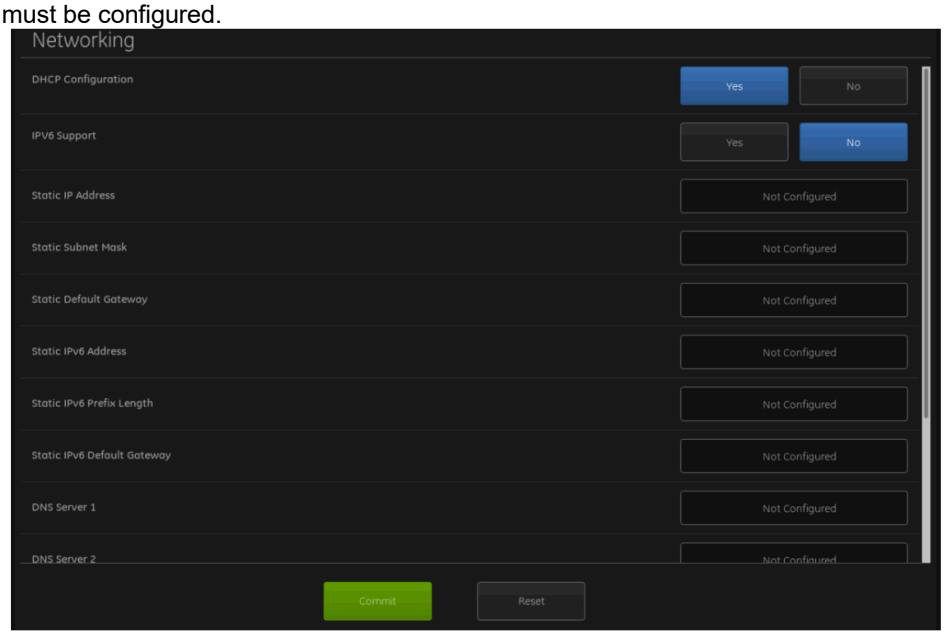
The system has the ability for remote desktop viewing by GE Healthcare applications and service personnel. When VNC is initiated, a remote operator can view the system UI, can make selections and navigate different workflows, or can view exactly what the user is doing. Remote operators cannot initiate any x-rays. Remote desktop viewing is to be utilized for service troubleshooting, guidance, issue investigation, or for applications training purposes.

5.2.2. Network Requirements and Protocols

The AMX Navigate supports both DHCP and static IP address allocation on both IPv4 and IPv6 for its network interfaces. Up to two manual DNS servers can be configured as well. An administrator user can configure these settings in the service user interface:

(Service → Configuration → Networking)

By default, the system is configured to only use DHCP with IPv4. If static IP address and IPv6 support is required, this must be configured.



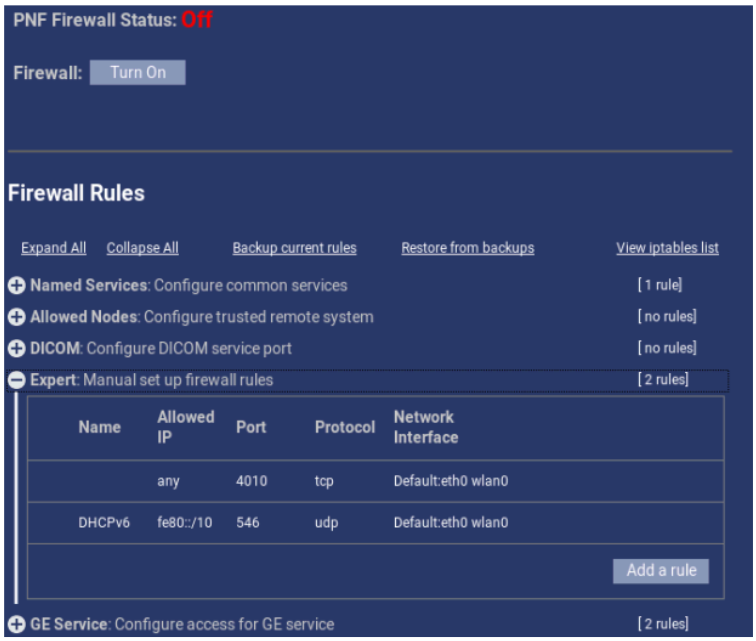
5.2.3. Product Network Filter (PNF)

The AMX Navigate is protected by a software-based product network filter, a network firewall. By default, it is turned on for every network interface. It only permits traffic through port 4010 to support interoperability with DICOM. Note that if DICOM over TLS is enabled, the DICOM listening port is 2762.

GE recommends that firewall be turned on at all times, that only port 4010 is left unblocked, and that you check your firewall settings periodically.

An administrator user can configure the product network filter in the service user interface:
(Service → Configuration → Product Network Filter)

The following options can be configured: firewall rules for named services, allowed nodes, DICOM services, manual firewall rules, and GE service rules. The firewall rules can also be backed up to local system and restored from backup files on the local system. In addition, the firewall can be paused or disabled completely.

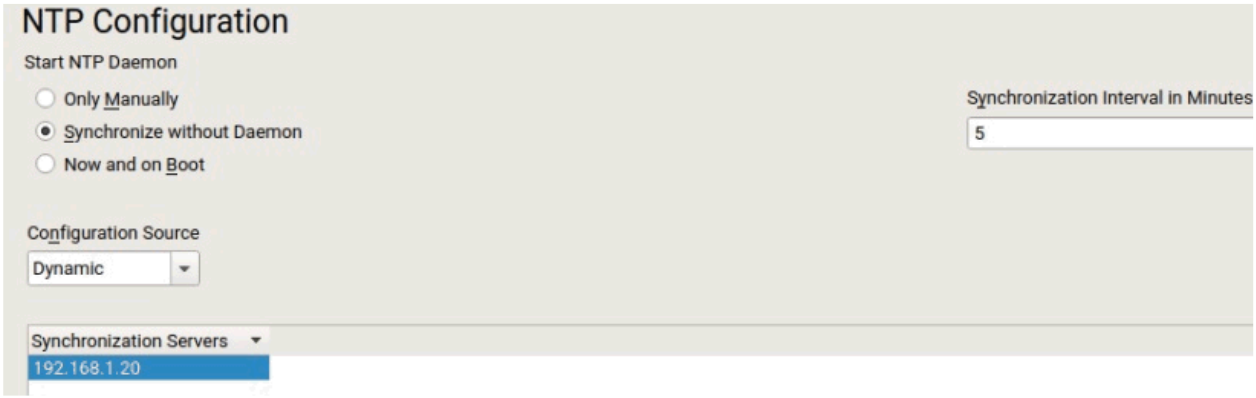


5.2.4. Time Synchronization (NTP)

The AMX Navigate supports the ability to synchronize its clock with an NTP server. An administrator user may configure this in the service user interface:

(Service → Configuration → Time Server)

Either an NTP server hosted locally by the customer site or a public server can be configured. The source can either by Static or Dynamic and the NTP daemon can be configured to be a one-time manual synchronization, automatically on system boot, or automatically at specific configurable time intervals.



5.2.5. Federal Information Processing Standard (FIPS) 140-2

The AMX Navigate supports an optional ability to configure the system in a FIPS 140-2 compliant operating mode.

This will limit communication and encryption protocols to those that are only permitted by the FIPS 140-2 standard and may affect the ability to transmit data over wired and wireless networks if the site infrastructure does not support FIPS 140-2 compliant configurations.

5.3 Wireless Security

Due to the broadcast nature of wireless communication, wireless devices require special security consideration. There are effective techniques and tools for improving the security of wireless communication devices.

5.3.1. Wireless Protocols

The AMX Navigate supports two wireless networks utilizing Wi-Fi technology. One is dedicated for communication with the wireless detectors and is completely managed by the system. Its behaviors can be tuned with configuration settings. The second wireless network is for connectivity with the facility wireless network.

5.3.1.1 Detector Wireless Network

The AMX Navigate broadcasts a wireless network for wireless detectors to connect with over a WPA2-PSK wireless local area network secured with AES-CCMP encryption. The network is disabled by default and is automatically configured with the system country is selected and committed at product installation.

The wireless network is secured by a passphrase that is automatically computed upon configuration of the site country selection. Hence there is no display of or user interaction necessary for selection. If a new country is selected, the system will reconfigure the detector wireless network and all registered detectors will be unregistered.

The first time the system boots after being configured, all registered wireless detectors will need to be re-registered with the system. This is done by connecting the detector to the system via tether or charging bin and following the detector registration process.

By default, this network will broadcast on a 40MHz channel in the UNII-1 and UNII-3 band (if supported for the selected country) in the 5 GHz spectrum with a maximum transmit power of 21 dBm (or lower if restricted by the selected country). The UNII-2 band and other DFS channels are not used for this network.

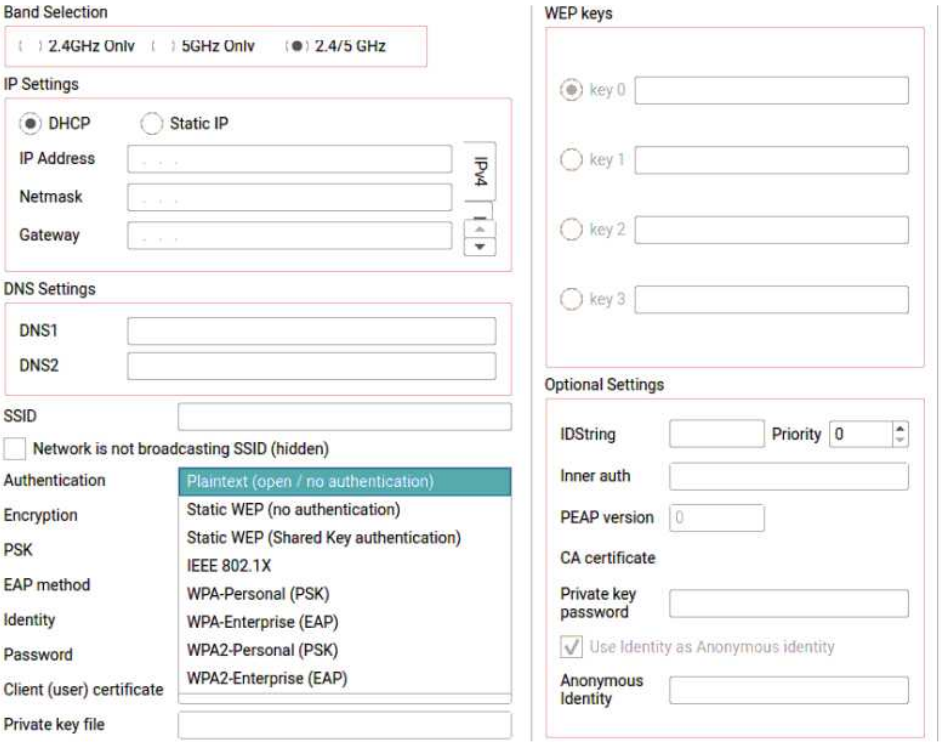
Customers with Class C licenses are able configure the network to broadcast on specific 20 MHz and 40MHz channels in the UNII-1 and UNII-3 as allowed by the selected country. In addition, Class C license users can reduce the maximum allowed transmit power in 3 dBm increments from a maximum of 21 dBm.

5.3.1.2 Hospital Wireless Network

The AMX Navigate can connect to the hospital network via Wi-Fi as well as Ethernet cable. If you are connecting AMX Navigate to the hospital network wirelessly, GE recommends a minimum of a WPA2 protocol with AES-CCMP encryption.

If the AMX Navigate system is using the hospital wireless network, then it is exchanging protected health information (PHI) with RIS and PACS servers over this network connection. If your network is improperly secured, sensitive patient information may be intercepted.

An administrator user can configure Wi-Fi network settings in the service user interface:
(Service → Configuration → Wireless Hospital Network)



Multiple network configurations can be supported at one time and can be selected to operate in either the 2.4 GHz spectrum, the 5 GHz spectrum, or both spectrums. DHCP and Static IP address are supported for both IPv4 and IPv6, however IPv6 is disabled by default and must be enabled for use.

If the facility makes use of hidden Wi-Fi networks, this must be specifically configured by enabling the checkbox in the network profile configuration.

Note: Hidden networks provide no additional security benefit and can cause compatibility problems for certain devices or devices operating in the Dynamic Frequency Selection (DFS) channel spectrum. If your facility uses Hidden networks, consider unhiding them and using at least WPA2 with AES-CCMP.

The following authentication methods are supported by the AMX Navigate:

- Plaintext (Open / No Authentication)

Note: Plaintext Authentication is not secure. GE recommends that at minimum WPA2 with AES-CCMP be used.

- Static WEP (No Authentication)
- Static WEP (Shared Key Authentication
- IEEE 802.1X

Note: WEP has been compromised. If your facility uses WEP, consider upgrading to WPA2.

- WPA-Personal (PSK)
- WPA-Enterprise (EAP)

Note: WPA has been replaced by WPA2. WPA can support TKIP, which has known vulnerabilities. Whenever possible use WPA2 with AES-CCMP.

- WPA2-Personal (PSK)
- WPA2-Enterprise (EAP)

Note: WPA2 can support TKIP, which has known vulnerabilities. Whenever possible use WPA2 with AES-CCMP.

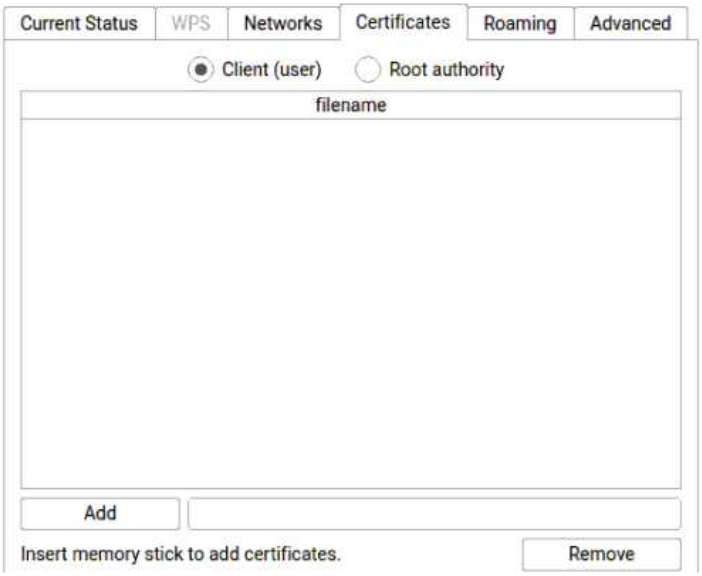
WPA-Enterprise and WPA2-Enterprise support additional protocols and encryption methods:

- MD5

- TLS
- MSCHAPv2
- PEAP
  - Inner Authentication Methods:
    - EAP-MD5, EAP-TLS, EAP-MSCHAPv2, EAP-GTC, EAP-OTP
- TTLS
  - Inner Authentication Methods:
    - PAP, CHAP, MSCHAP, MSCAHPv2, EAP-MD5, EAP-TLS, EAP-MSCHAPv2, EAP-GTC, EAP-OTP
- GTC
- OTP
- LEAP

These methods can support either an Identity and Password combination for authentication, or it can support the use of Client (User) certificate as well as a private key file and password if this is required by the facility.

Certificates (Client and Root) and private key files must by uploaded manually via a USB stick and the Certificate configuration tab:



5.4 Removable Media Security

The AMX Navigate supports removable media storage via USB drives as well as USB mounted CD and DVD drives. Using removable media is required for various tasks:

- Exporting and importing acquired data and images
- System back-up and restore
- Upgrading system and application software
- Storing service logs during service sessions

GE recommends USB drives be stored in a secure place, where unauthorized personnel cannot easily access them.

GE also recommends that you secure medical data exported from AMX Navigate systems. These data exports contain protected health information (PHI).

5.4.1. Booting from Removable Media

Booting from USB removable media is disabled in BIOS. The BIOS boots directly to the internal hard disk drive.

5.4.2. Removable Media

Data stored on removable media is stored unencrypted. As this data could contain personal information (PI)/protected health information (PHI), removable media and the content on removable media must be handled according to applicable regulations and guidelines for such.

5.4.3. Data Destruction for Portable Media

The AMX Navigate system does not have an internal functionality for secure deletion of data stored on the removable devices.

Approved procedures and tools should be used for secure removal of data stored on removable media, according to applicable regulations and guidelines for handling patient information, personal information (PI), and protected health information (PHI).

5.5 Data Encryption

5.5.1. Encryption of Data at Rest

Patient Information (PHI) data stored on the system is stored encrypted on the system's internal hard disk. Access to the file system is prevented for users without service privileges.

The AMX Navigate system provides features to limit damage from accidental data disclosures via its auto-delete capability.

Data	Description
Local Archive	Database contain personal information (PI) and protected health information (PHI)
Debug Log Files	Logs for debugging purposes, potentially containing personal information (PI) and protected health information (PHI)

5.5.1.1 Auto-Delete

The AMX Navigate is capable of automatically deleting examination information stored on the system based on disk usage. This is a configurable setting that can be set in the user interface configuration screens. It is recommended that you configure auto-delete to start when the disk is 9% full and to delete images older than 2 days.

When the system is shipped, auto-delete is turned off.

When auto-delete is first enabled, the system is configured to delete images older than 14 days.

The AMX Navigate is not intended to be used for long-term storage of exam information. It is recommended that the system be connected to an archival device.

5.5.1.2 Backup

The AMX Navigate system stores data unencrypted to the back-up target. This includes back-up of images and patient info.

The target for the back-up, either removable media or servers, must be secured to ensure the required security of the backed-up data from the AMX Navigate system.

Please refer to the *AMX Navigate Operator Manual, 5845272* for instructions on how to perform backups.

5.5.2. Data in Transit Security

The GE Healthcare AMX Navigate provides TLS over DICOM connections.

5.5.2.1 Introduction

The successor of Secure Socket Layer (SSL), DICOM Transport Layer Security (TLS) is a cryptographic protocol that provides confidentiality and integrity between two data sources. Its specific purpose for the system is to protect data in DICOM traffic. It relies on public-key cryptography (PKI). The connection is private because the transmitted data is encrypted, and machine identity can be authorized before transmission to ensure the recipient of the data is authorized. The most current version of TLS on the system is TLS 1.2, but it also supports TLS 1.1 and TLS 1.0.

5.5.2.2 GE Service Prerequisites

Security and TLS options must be enabled by GE service personnel.

5.5.2.3 Certificate Configuration

Certificates must be configured and distributed for successful DICOM over TLS operation. There are two supported configurations. Choose configuration based off whether IT architecture support a certificate authority (CA) server and other DICOM host (PACS, RIS) TLS support.

5.5.2.4 Identity files for use in DICOM TLS configurations

Private Key
The private key must be generated before any other certificate is generated, or an error will occur. It is kept secret and is only known by the system. The private key will only work with the corresponding public key. It can be imported via USB to the system; however, one must know the passphrase to decrypt it.

Host Certificate
The Host Certificate is a digital file that contains the public key of the system. It is shareable via USB export and generated on the system; however, only one of these is supported at a time. If the system generates the private key, the system must also generate the host certificate.

Trusted Certificates
Trusted Certificates can be certificates of other systems or a CA certificate. Many of these can be loaded onto the system, but they must be loaded via USB. If the system does not have the CA Certificate, one must have the PACS's certificate to make TLS work on the system.

Certificate Signing Request (CSR)
The CSR exports a file that allows the signing of a host certificate by the CA server.

5.5.2.4.1 Direct Comparison (Self-signed)

The AMX navigate support creation and installation of its own self-signed X.509 certificate as well as the installation of trusted host certificates. To successfully configure the AMX Navigate for secure DICOM transport in a self-signed certificate environment, the following steps must be completed:

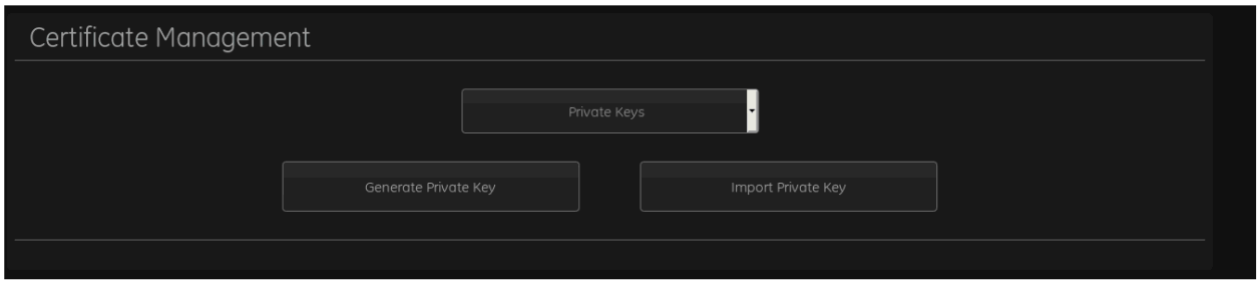
1. Generation or import of private key **Section 5.5.2.4.1.1**
2. Creation, installation, and export of the AMX Navigate system certificate. **Section 5.5.2.4.1.2**
3. Import of configured (trusted) DICOM hosts intended for TLS communication. **Section 5.5.2.4.1.3**

5.5.2.4.1.1 Private Key Configuration

The system’s private key can be self-generated or imported.

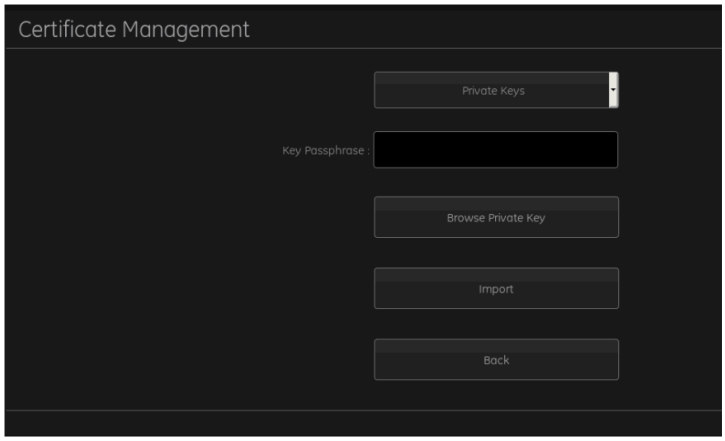
5.5.2.4.1.1.1 Private Key Generation

In Certificate Management, under “Private Keys” drop-down, click “Generate Private Key” to generate a private Key.



5.5.2.4.1.1.2 Private Key Import

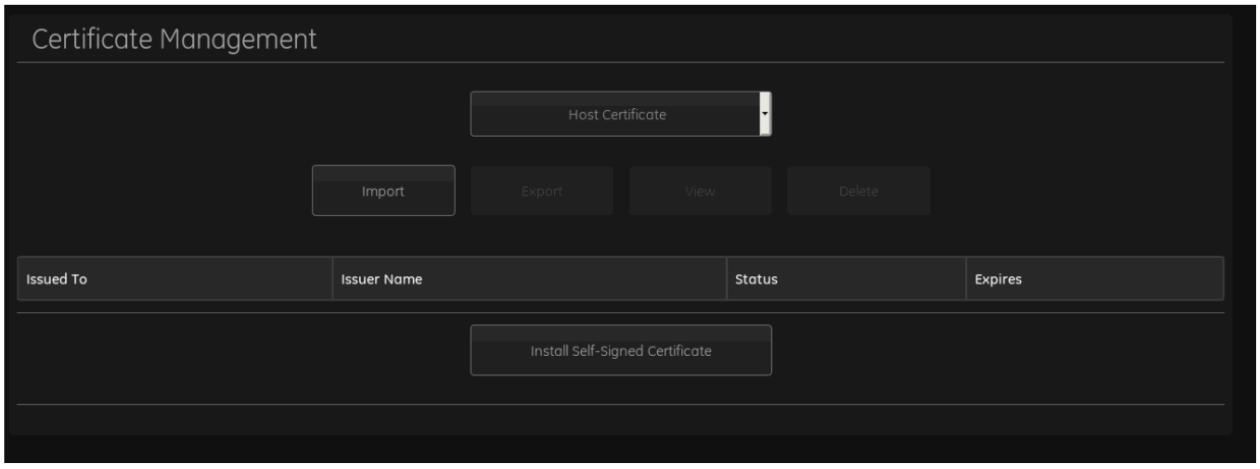
Click “Import Private Key” to import a private key from USB media. A file browser will open, where user can select private key. A passphrase can be entered if the private key is encrypted.



5.5.2.4.1.2 Host Certificate Configuration

5.5.2.4.1.2.1 Host certificate installation

For self-singed certificate configuration, the certificate will be self-generated and installed. Click Install Self-signed Certificate button to complete this process.

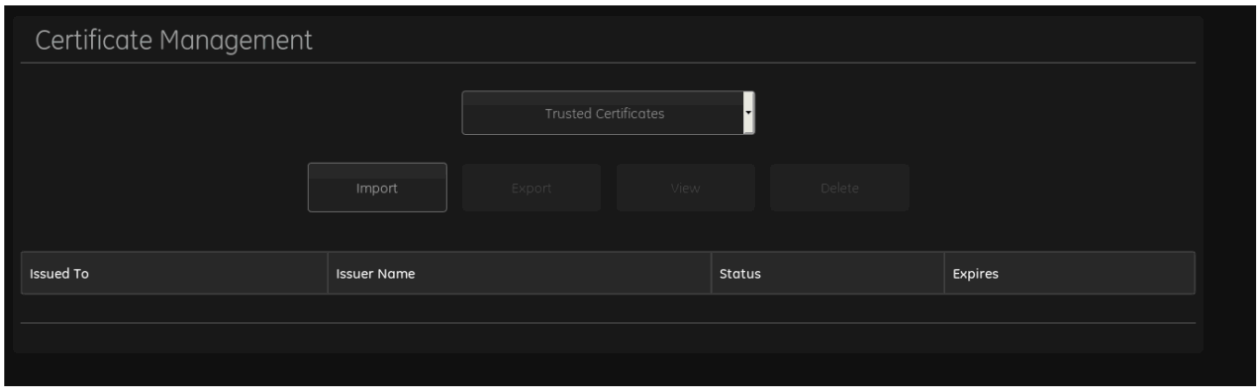


5.5.2.4.1.2.2 Host certificate export

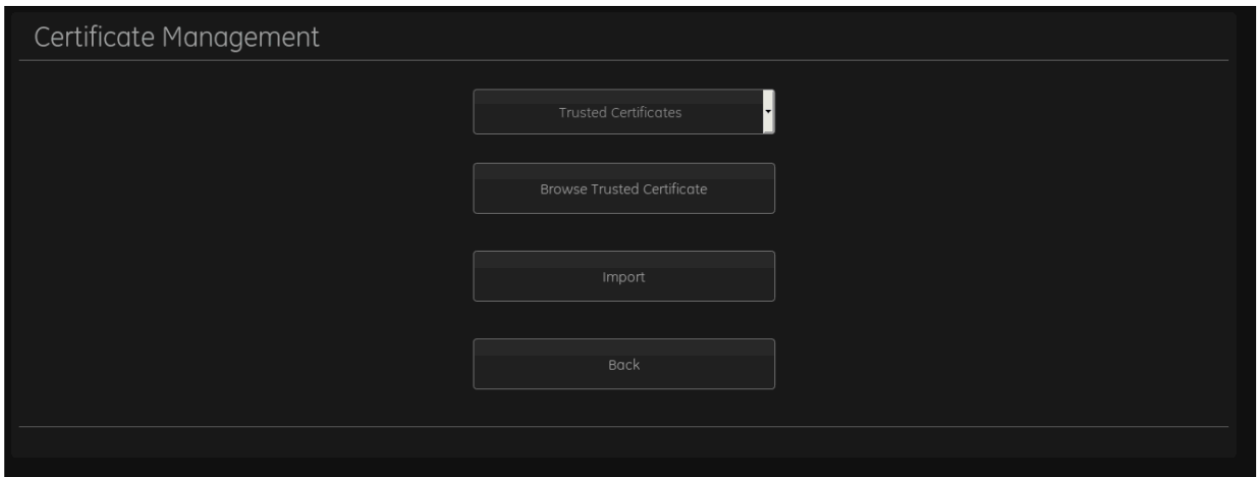
For self-singed certificate configuration, the certificate will need to be exported to USB media for installation on DICOM over TLS capable hosts intended for communication. With USB media mounted to the system, click “export.” This certificate will need to be loaded on DICOM capable hosts per process outlined by the vendor.

5.5.2.4.1.3 Trusted Certificate Configuration

For self-singed certificate configuration, the trusted certificates of TLS capable DICOM hosts (PACS, RIS, etc.) will need to be imported.



Click Import to complete this process.



5.5.2.4.2 Trusted Signature Chain Comparison (CA-signed)

The AMX Navigate supports creation and installation of a Certificate Signing Request (CSR) as well as installation of a CA or intermediate-CA certificate.

The AMX Navigate supports creation of a certificate signing request, import of system certificate that has been signed by the CA and installation of a CA or intermediate CA certificate as the trust anchor. To successfully configure the AMX Navigate for secure DICOM transport in an environment that uses a certificate authority (CA) server, the following steps must be completed:

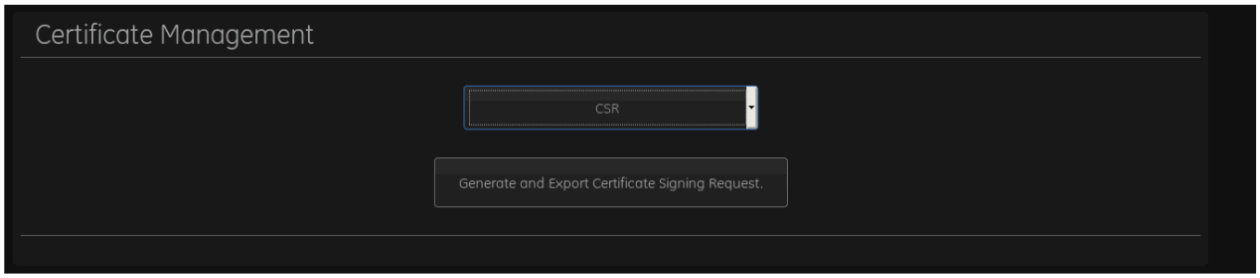
1. Generation or import of private key **Section 5.5.2.4.2.1**
2. Creation and export of the CSR (Certificate Signing Request) **Section 5.5.2.4.2.2**
3. Import of CA as trust anchor. **Section 5.5.2.4.1.3**

5.5.2.4.2.1 Private Key configuration

See Section 5.5.2.14.1.1

5.5.2.4.2.2 Certificate Signing Request

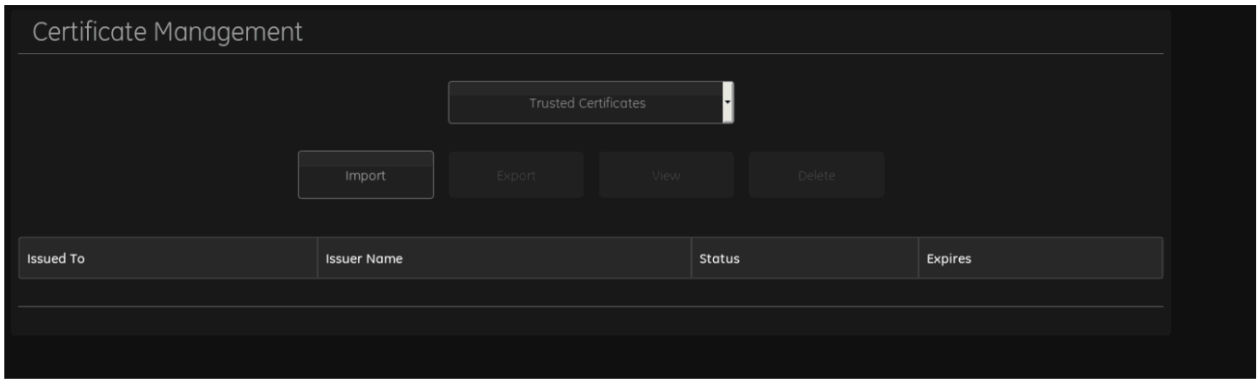
With USB mounted, click “Generate and export Certificate Signing Request” to export a CSR to USB media.



This certificate signing request will need to be imported to CA where a certificate can be generated for the AMX Navigate.

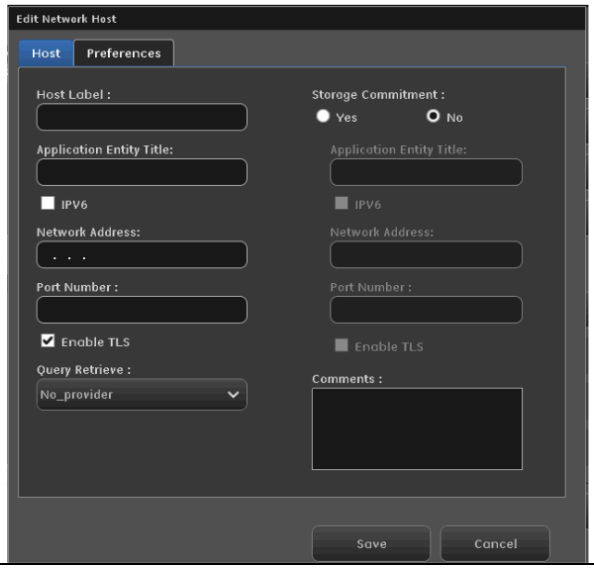
5.5.2.4.2.3 Import of CA or intermediate CA certificate as trust anchor

Per local IT process, obtain the appropriate CA certificate and save to a USB media. Import that certificate by clicking “Import” from “Trusted Certificates” page.



5.5.2.4.3 DICOM TLS configuration

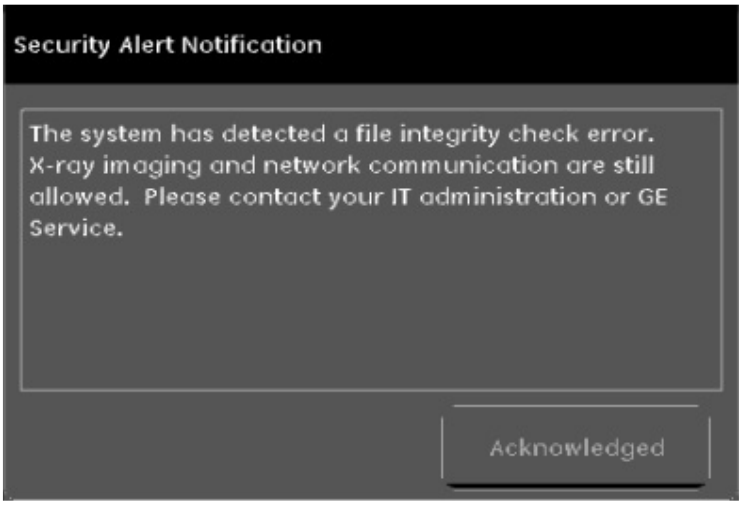
Once the certificates are configured, TLS must be enabled for all configured DICOM network hosts. Click the “Enable TLS” box to check mark.



5.6 Data Integrity Capabilities

The GE Healthcare AMX Navigate provides optional capabilities to assure that data are not inappropriately modified accidently or maliciously.

The Linux Advanced Intrusion Detection Environment (AIDE) is used to determine if files have been inappropriately modified. If this occurs, a blinking red bell icon will be displayed in the user interface and an error will be logged. Clicking on the red bell icon will display a popup with further instructions to the user.



5.7 De-Identification Capabilities

The GE Healthcare AMX Navigate contains de-identification (anonymization and pseudonymization) capabilities to limit Privacy & Security risks to sensitive information.

When exporting patient information, the de-identification option may be selected.

The de-identification option is also available for transferring the data to remote service. PI/PHI data is removed when pulled from remote service. De-identification is done by clearing or overwriting all information in the image containing PI/PHI.

5.8 Backup Considerations

The AMX Navigate is not intended to be used for long term data storage.

5.8.1. Patient Archive Solutions

DICOM data from the AMX Navigate is intended to be archived to DICOM/PACS servers for long-term storage. The business contingency planning and security of data stored on DICOM/PACS servers are outside the scope of this document.

5.8.2. System Configuration Backup and Restore

The AMX Navigate provides the capability to back up the system configuration. Refer to the *AMX Navigate Operator Manual, 5845272* for details.

A back-up of the system configuration is not encrypted. The backup media should be properly secured as it contains information that an attacker can leverage to help attack the hospital network or AMX Navigate system.

5.8.3. DICOM Exports

DICOM data on the system may be exported to removable media. This feature is not intended to be used as a substitute for archival on DICOM/PACS servers.

However, these exports do not interfere with archival on the servers; data that has been exported will be treated like any other data when archiving to servers. Because these exports are stored on removable media, the removable media must be properly secured.

5.9 Security Controls provided by the Cloud Provider

Not Applicable. This product is not a cloud-based application and as such there is no cloud provider.

6.0 System Protection

The System needs to be configured and maintained in a way that continually protects Privacy & Security.

6.1 Malicious Software Protection

The computing environment is increasingly hostile, and threats continue to grow from malicious software, including computer viruses, worms, Trojan horses, denial of service attacks, and other malware. Vigilant defense on many levels is required to keep systems free from compromise by malicious software. In most cases, effective protection requires cooperation and partnership between GE Healthcare and our customers.

Commercial Anti-Malware software is commonly used on general-purpose computers to detect the presence of malicious software (virus, Trojan horse, worm, etc.). Anti-Malware software is useful on general-purpose computers as they typically cannot be sufficiently hardened against the attack vectors used by malicious software. A Medical Device however is a single purpose (dedicated) device that has controlled intended use, and thus often can be well hardened. GE Healthcare employs a hardening approach on medical devices to maximize both security and patient safety. For medical devices, the patient safety risk introduced by using commercial Anti-Malware software needs to be carefully considered. Considerations Such risks include:

- Misconfigured Anti-Malware software.
- Real-time scanning affecting system performance.
- Introducing false positives.
- Quarantining of clinical data that randomly appear to match a virus signature.
- The Anti-Malware software itself is another popular attack vector.
- Support of the Anti-Malware software throughout the life cycle of the medical device (Operating System support and virus signatures/libraries)

Due to the cited risks, the use of anti-malware software needs to be carefully configured when used with this product. The following configuration guidance has been developed to effectively balance the risks vs the benefit of using Anti-Malware.

The AMX Navigate provides optional antivirus (AV) through McAfee Endpoint Security for Linux Threat Prevention (ENSL) to protect against malicious software.

The anti-virus software monitors files (read or execute) and reports errors to user. The system also provides local capability to complete full system scan. Latest scan reports can be viewed on the system. Virus signature version is displayed in the UI and can be updated through local USB update.

An administrator user can access the antivirus configuration and usage tools in the service user interface:
(Service → Configuration → Security → Antivirus)

If malicious files are detected on the system a blinking red bell icon will be displayed in the user interface and an error will be logged. Clicking on the red bell icon will display a popup with further instructions to the user.

6.1.1. User Interface – Antivirus Scan

The antivirus version, engine version, and MEDDAT file version are all displayed at the top of the screen.

On-access scanning is enabled by default, this feature will scan files and directories in real-time as read, write, and execute operations are performed by the AMX Navigate. There is no configuration needed for this.

In addition, a detailed full system on-demand scan can be started by clicking on the “Start Scan” button. System performance may be slowed while an on-demand scan is in progress. Clinical operations are still permitted while this scan is in progress.

A summary for both on-demand and on-access results are displayed on this page and detailed scan results can be viewed by clicking on the links provided in the user interface.

6.1.2. User Interface – Antivirus ePO Setup

If the customer site has a McAfee ePolicy Orchestrator (ePO) server deployed, virus reporting, initiation of full system scan, and updates of signature file can be completed from the ePO server.

In order to connect to an ePO server, the following information must be entered and applied:

- ePO Server IP Address
- ePO Port Number
- ePO Username
- ePO Password

Once configured the connection status of the system to the ePO server will be displayed in the upper-right of the user interface.

Please note that GE ePO policies can override the locally configured policies. The following section provide instructions on how to implement the GE Healthcare approved configuration policies for an ePO server. GE Healthcare cannot guarantee system performance if there is any deviation to this approved configuration.

This configuration will allow for on-access scanning as well as Engine and MEDDAT file update policies.

6.1.2.1 McAfee ePolicy Orchestrator Server Console Configuration

This configuration assumes a McAfee ePO 5.10.0 with Update 9 or newer. Older configurations may have different UI display and workflow, but all of the configuration options apply.

6.1.2.1.1 Create a New Subgroup

1. Login to the McAfee ePolicy Orchestrator Console.

2. Click **Menu** → **Systems** → **System Tree**

3. Expand the drop-down menu in the **Systems Tree** and click on the Group you wish to add to the system Subgroup.

4. Click on the **New Subgroup** button and enter the desired name.

6.1.2.1.2 Configure Product Deployment Rules for New Subgroup

1. Expand the drop-down menu in the **Systems Tree** and click on the newly created Subgroup for the system.

2. Click on the **Assigned Client Tasks** tab.

3. Click on the **Edit Assignment** link of the product update task.

4. Click on the **Break Inheritance** radio button in the **Inheritance** section.

5. Click on the **Disabled** button in the **Schedule Status** section.

6. Click on the **Save** button.

6.1.2.1.3 Configure Product Update Rules for New Subgroup

Please note that if the MEDDAT and Engine product deployment task is locked, the following steps in this section will not be possible.

1. Expand the drop-down menu in the **Systems Tree** and click on the newly created Subgroup for the system.

2. Click on the **Assigned Client Tasks** tab.

3. Click on the **Edit Assignment** link of the product deployment task.

4. Click on the **Break Inheritance** radio button.

5. Click on the **Create New Task** button.

6. Enter a desired **Task Name** and add a **Description**.

7. Click on the **Selected packages** radio button.

8. Under **Package types**, ensure that only the check boxes for **MEDDAT** and **Linux Engine** are checked.

9. Click on the **Save** button.

10. Click on the **Save** button.

6.1.2.1.4 Create New On-Access Policy

1. Click **Menu** → **Policy** → **Policy Catalog**
2. Select **Endpoint Security Threat Prevention** in the Product options.
3. Select **On-Access Scan** in the Category drop-down menu.
4. Click on the **New Policy** button. Name the policy and click on the **OK** button.
5. Click on the newly created policy in the catalog window to open the configuration page.
6. Scroll down to **McAfee GTI** window and uncheck the box for **Enable McAfee GTI**.
7. Click on **Show Advanced**.
8. Scroll down to the **Exclusions** window and add the following exclusions:

File Name or Path	Also Exclude Subfolders	When To Exclude
/magichome/	Yes	Read / Write
/database/	Yes	Read / Write
/enggdata/	Yes	Read / Write
/usr/share/gehc_security/	Yes	Read / Write
/export/	Yes	Read / Write
/var/log/	Yes	Read / Write
/_adming/Manage_NSS/	Yes	Read / Write
/media/nss/	Yes	Read / Write
/mnt/system/log/	Yes	Read / Write
/cgroup/	Yes	Read / Write
/dev/	Yes	Read / Write
/proc/	Yes	Read / Write
/selinux/	Yes	Read / Write
/sys/	Yes	Read / Write
/tmp/	Yes	Read / Write
/configDB/	Yes	Read / Write
/xrayDigital/	Yes	Read / Write

File Type	When To Exclude
Vmdk	Read / Write
Dbl	Read / Write
Ctl	Read / Write
Log	Read / Write
Jar	Read / Write
War	Read / Write
Dtx	Read / Write
Dbf	Read / Write
Frm	Read / Write
Myd	Read / Write
Myi	Read / Write
Rdo	Read / Write
Arc	Read / Write

9. Click on the **Save** button.

6.1.2.1.5 Create New Tag

1. Click **Menu** → **Systems** → **Tag Catalog**
2. Click on the **New Tag** button.
3. Enter a name for the new tag.
4. Under **Criteria**, click on **the** Add button. Select **System Name** and **OS OEM Identifier** from the **Available Properties** list.

5. For the **System Name** property, create the following setting:

Property	Comparison	Value (case sensitive)
System Name	Equals	Magic

6. For the **OS OEM Identifier** property, create the following settings:

Property	Comparison	Value
OS OEM Identifier	Contains	SUSE Linux Enterprise Server 15

7. Click the **Next** button.

8. Under **System**, select the **Apply tag now to systems that match the tag criteria** check box.

9. Under **Evaluation**, select the **Also evaluate on each agent-server communication** check box.

10. Click on the **Save** button.

6.1.2.1.6 Create New Assignment Policy Rule

1. Click **Menu** → **Policy** → **Policy Assignment Rules**

2. Click on the **New Assessment Rule** button.

3. Enter a name for the new assignment policy rule and click the **Next** button.

4. Click on the **Add** policy button. Select **Endpoint Security Threat Prevention** from the Product drop-down menu. Select **On-Access Scan** from the Category drop-down menu. Select the newly created policy from the Policy drop-down menu.

5. Click on the **Next** button.

6. Click on the **Tag** option in the Available Properties window. Select **Has Tag** in the Comparison drop-down menu. Click the **[…]** button and select the newly created Tag in the Value drop-down menu. Click the **OK** button.

7. Click on the **Next** button.

8. Click on the **Save** button.

6.1.2.1.7 Assign Assignment Policy Rule to Client Device and Move to New Subgroup

1. Click **Menu** → **Systems** → **System Tree**

2. Click on the top-level group in the **Systems Tree**.

3. Click on the preset drop-down menu and select **This Group and All Subgroups**.

4. In the Quickfind field, enter the IP address of the system and click **Apply**. If the system includes any tags in addition to the one just created, complete the following action. If not, skip to step 8.

5. Click on the checkbox next to the desired system.

6. Click on the **Actions** button in the lower left of the **Systems** list. Click the **Clear Tag** action.

7. Select one of the tags that is not the one just created and click **OK**. Do this for all tags except for the one that was just created.

8. If the system already contains the tag that was just created, skip to step 10. Click on the checkbox next to the desired client system. Click on the **Actions** button in the lower left of the **Systems** list. Highlight **Tag** and click on the **Apply Tag** action.

9. Select the newly created tag and click **OK**.

10. Click on the checkbox next to the desired client system. Click on the **Actions** button in the lower left of the **Systems** list. Highlight **Directory Management** and click on the **Move Systems** action.

11. Select the desired Subgroup for the AMX Navigate system and click on the **OK** button in the lower left.

6.1.3. User Interface – Antivirus Non-ePO Setup

The AMX Navigate provides manual Engine and MEDDAT file update capabilities for customer sites that do not have an ePO server deployed.

The following instructions are used to procure the most recent Engine and MEDDAT files from the McAfee website, extract the appropriate files onto a USB stick, and upload the new files to the system.

Download DAT File

1. Navigate to https://www.mcafee.com/enterprise/en-us/downloads/security-updates.html
2. Click on the tab titled "**.DATs**"
3. Scroll down to the section titled "**Download MEDDAT Updates**"
4. Click on the link to download the MEDDAT file. The file that will be downloaded will contain a name with the following format: "**mediumepoXXXXdat.zip**"
5. Extract the downloaded "**mediumepoXXXXdat.zip**" file and copy the file titled "**mediumdat-XXXX.zip**" to a USB.

Download Engine File

1. Navigate to https://www.mcafee.com/enterprise/en-us/downloads/security-updates.html
2. Click on the tab titled "**Engines**"
3. Scroll down to the section titled "**Linux Engine Package for Use with ePO**"
4. Click on the link to download the MEDDAT file. The file that will be downloaded will contain a name with the following format: "**epoXXXXlnx.zip**"
5. Extract the downloaded "**epoXXXXlnx.zip**" file and copy the file titled "**avengine64.zip**" to a USB.

Updating DAT and Engine Files

1. Plug the USB where the files are copied to into the system.
2. Under the dropdown menu titled "**Select USB**" select the USB that is inserted into the system.
3. To Update the DAT file, select "**mediumepoXXXXdat.zip**" in the "**Select DAT/Engine File**" dropdown menu. Click the "**Update DAT**" button.
4. To Update the Engine file, select "**avengine64.zip**" in the "**Select DAT/Engine File**" dropdown menu. Click the "**Update Engine**" button.

Confirmation of DAT and Engine File Update

When updates are complete, check that the DAT and/or Engine file version in the "**Antivirus Details**" section of this page have been updated to the versions downloaded from the McAfee website.

6.2 System Security

The GE Healthcare *AMX Navigate* contains additional features to improve local operational security.

6.2.1. No Linux Desktop Access

System operators do not have access to the OS terminal or to the Linux file system. Therefore, the users will have no access to Internet web-browsing, e-mail clients, installing any software on the system nor adding files (except for application related files through the application).

6.2.2. Linux Services Disabled

Unused Linux services are disabled on the AMX Navigate system.

6.2.3. GE Healthcare Service Access

To access the AMX Navigate system in service mode, an encrypted USB service key and a service password are required. The service key is a secure device and its features are discussed in greater detail in Section 7.1

When in service mode, the field engineer will have access to the operating system and to the file system.

6.2.4. Firewall

See Section 5.2.3.

6.2.5. Drive Lock

As a mobile device, the AMX Navigate is capable of being driven throughout the hospital. To assist with physical security of the device, a drive lock code and idle time can be configured. While drive lock is enable, a user will not be able to engage the wheels of the device. The drive login code must be entered to unlock the wheels. The wheels will lock once again when the configured idle timeout has been reached. The drive lock is independent of and in addition to user authentication.

6.1 Patch Management Practices

6.1.1. Operating System

The AMX Navigate uses the Suse Linux Enterprise Server (SLES) 15 operating system.

6.1.2. Security Updates

GE Healthcare is constantly monitoring for security vulnerabilities applicable to its products. This includes vulnerabilities in the application software, third party components and the underlying operating system. Announced vulnerabilities in the operating system or other third-party components are assessed based on the AMX Navigate system's configuration and use.

When needed, GE Healthcare will make product security updates/patches available to customers. When applicable, these updates will include patches for the operating system and third-party components.

For privacy and security concerns regarding GE products, please refer to http://www.ge.com/security

6.1.3. eDelivery

E-Delivery is a broad term used to describe the electronic delivery of files from a secure server to a target device. The remote software download feature on the AMX Navigate product will utilize the e-Delivery network ecosystem to transfer system operating system and/or applications level software to the target device. GE Healthcare will build and manage software packages and load to the secure Flexera server upon release. The target device can then recognize when an update is available and alert the user to take action. The target device will be capable of installing the updates with an integrated user workflow. A standard user will only have access to view that an update is available; a privileged user (GE service or site admin) will have the access to initiate both a download and an installation.

For more information and detailed instructions on using the eDelivery feature, please refer to the *AMX Navigate System Manual Class, 5871434*.

7.0 Servicing

7.1 Local Servicing

AMX Navigate supports local servicing through a factory-installed service user account, *GEService*. A fully authenticated login with *GEService* has Class M privileges, which means he or she has access to all of the same configuration screens as the admin user as well as several others reserved for Class M users. *GEService* also has the ability to open a terminal.

The *GEService* account's password is unique to each system. When GE field engineers need to access to a Class M feature, their Class M service key must be inserted into the system. Class M service keys are SSA hard keys that are protected by an individualized PIN and encryption. Also, Class M service keys expire and must be renewed periodically.

If you find a Class M service key left on a system, please contact GE.

GE field engineers may access the system via a terminal. As such files containing PHI will be exposed to field engineers. GE field engineers are explicitly prohibited from retrieving any files containing PHI unless the immediate service request cannot be accomplished without those files. Even so, they are trained to use anonymization tools present on the system to remove PHI information.

7.2 Remote Servicing

Often the most efficient and cost-effective manner for GE Healthcare to provide service is to connect to AMX Navigate remotely. Every effort is made to ensure that this connection is as secure as possible.

The GE Healthcare remote service platform is integrated in the AMX Navigate system. This platform enables real-time application support, problem diagnosis, and repair.

Please refer to the *AMX Navigate Operator Manual, 5845272* for instructions on how to use the remote servicing capability

7.2.1. Remote Service Platform

The two major technical components of the remote service platform are the Agent and the Server. The Agent is installed on the AMX Navigate system, while the Server resides within GE Healthcare. The Agent establishes secure communications via an encrypted VPN initiated from the AMX Navigate.

7.2.2. Key Security Features

The key security features of the remote service platform include the following:

- Communication from the Agent to the Server is initiated by the on-site user securely via an encrypted FIPS 140-2 VPN. No fixed IP address is required on the device.
- The Server which the agent connects to is predefined. This ensures that remote connections can only be made to GE Healthcare systems.
- The Agent communicates with the Server via transmissions that require password authentication. Data transmission occurs over the encrypted VPN.
- Inbound firewall on the AMX Navigate system is not compromised. Because the connection is made from the Agent, the firewall does not need to support an additional open port.
- On the server end, the trained GE Service Representative is authenticated through single sign-on.

8.0 Personal Information Collected by the Product

In some cases, GE Healthcare may encounter personal information (PI)/protected health information (PHI) as part of the troubleshooting procedures or under data access rights granted to GE Healthcare. Access to this data

is limited to GE Healthcare authorized personnel only. PI/PHI encountered as part of remote service sessions will be handled according to GE Healthcare's standards for handling PI/PHI.

To support facilities that operate in the Eurozone, GE operates a remote service facility in that same region. As a result, PI and PHI information remains within the Eurozone.

9.0 Additional Privacy & Security Considerations

The GE Healthcare AMX Navigate has been designed with Privacy & Security functionality integrated into the core design. However, there exist Privacy & Security residual risks that must be mitigated once the GE Healthcare AMX Navigate is integrated into the work environment. This section contains some risks that should be imported into the Risk Assessment of the deployment of the GE Healthcare AMX Navigate for proper mitigation.

9.1 Advanced Applications

9.1.1. Quality Care Suite and Critical Care Suite

The Quality and Critical Care Suites (QCS and CCS) is a clinical decision support function that identifies potential critical findings in a radiographic exam and provides notification for prioritized review. Intended users includes technologist, clinical care team and radiologist.

QCS and CCS are a software module that can be deployed on several computing and X-ray imaging platforms; the Optima XR240amx with the Helix image processing software is one such reference platform that QCS and CCS can be deployed on and serves as an example of device integration on an imaging platform. The Optima XR240amx intended use remains
unchanged in that the system is used for general purpose diagnostic radiographic imaging.

All the privacy and security mitigations the Optima 240 platform has implemented are still effective even with QCS and CCS applications. There are no new privacy or security unmitigated risks with the integration of QCS and CCS applications.

9.1.2. HIS/RIS Link Application

The HIS/RIS Link Application is compatible with the AMX Navigate. For Privacy and Security information, please see *HIS RIS Link Application on Optima XR240amx Privacy and Security Manual, 5816166*.

10.0 Product Security Supplemental Documents

- **The Manufacturer Disclosure Statement for Medical Device Security (MDS2):** The MDS2 is available for the product AMX Navigate upon request by contacting sales representative or via the GE Healthcare Product Security Portal, https://securityupdate.gehealthcare.com.

- **The Software Bill of Materials (SBOM)**: SBOM is available upon request for the product AMX Navigate. Please reach out to sales representative for a copy of the SBOM.