



# **VistA Imaging System**

## **Security Guide**

July 2019 – Revision 25  
MAG\*3.0\*204

Department of Veterans Affairs  
Product Development  
Healthcare Provider Systems

## VistA Imaging System Security Guide

MAG\*3.0\*34, MAG\*3.0\*116, MAG\*3.0\*118, MAG\*3.0\*119, MAG\*3.0\*127, MAG\*3.0\*129, MAG\*3.0\*204

July 2019

### Property of the US Government

This is a controlled document. No changes to this document may be made without the express written consent of the VistA Imaging Product Development Group.

While every effort has been made to assure the accuracy of the information provided, this document may include technical inaccuracies and/or typographical errors. Changes are periodically made to the information herein and incorporated into new editions of this document.

Product names mentioned in this document may be trademarks or registered trademarks of their respective companies, and are hereby acknowledged.

VistA Imaging Product Development  
Department of Veterans Affairs

[REDACTED](#)

### Revision History

16 July 2019	Updates for MAG*3.0*204 <a href="#">REDACTED</a> --Updated section 1.3 to include new Windows versions, title page, footers, revision history, and TOC.
2 August 2013	Updates for MAG*3.0*34, MAG*3.0*116, MAG*3.0*118, MAG*3.0*119, MAG*3.0*127, MAG*3.0*129 <a href="#">REDACTED</a> (rev 24). --Added new sections 2.85 <i>Security Keys for DICOM Importer II</i> and 2.14 <i>HDIG Security 2.14</i> (and all its sub-sections) Updated sections 1.1, 1.3, 1.3.2.5, 2.9, 2.11.1, 2.11.2, 2.12, 2.13, 2.13.2, 2.15.
15 Mar 2013	Updates for MAG*3.0*124 (Rev. 23). <a href="#">REDACTED</a> --Updated sections 2.2.5; added section 2.2.5.1 AWIV Web Application (new); 2.2.5.2 Security Keys for AWIV)
26 Nov 2012	Updates for MAG*3.0*122. <a href="#">REDACTED</a> . --Updated sections 2.2.1, 2.8.1, 2.9, 2.12.
09 Nov 2011	Updates for MAG*3.0*104 (rev 21). <a href="#">REDACTED</a> . --Updated Appendix A and A.11; removed obsolete subsections under A.11.
01 Sep 2011	Updates for MAG*3.0*117 (rev 20). <a href="#">REDACTED</a> . --Updated sections 2.8.2 and 2.9; added Glossary entries
31 May 2011	Updates for MAG*3.0*39 (rev 19). <a href="#">REDACTED</a> --Updated sections 2.3, 2.7, 2.9; added new section 2.14 --Made global text corrections listed on p.1 of the Change Pages document
04 May 2011	Updates for MAG*3.0*106 (rev 18). <a href="#">REDACTED</a> --Updated sections 2.8.3 and 2.9
21 Mar 2011	Update For MAG*3.0*115 (rev 17). <a href="#">REDACTED</a>
01 Feb 2011	Updates for MAG*3.0*105 and 98 (rev 16). <a href="#">REDACTED</a> --Added new section 2.2.4 for Patch 105.

	--Updated section 2.8.1 for Patch 98.
	--non-patch update. Section 2.11, IPRM replaces OCIS.
1 Dec 2010	Updates for MAG*3.0*53 and MAG*3.0*66 (rev 15). <a href="#">REDACTED</a> --Updated section 2.9 for Patch 53. --Updated sections 1.1, 1.2, 2.2.3 and 2.1.2 for Patch 66.
21 Sep 2010	Updates for MAG*3.0*111, MAG*3.0*90, and MAG*3.0*94 (rev 14). <a href="#">REDACTED</a> y. --Updated sections 2.2.1, 2.6, and 2.8.2 for Patches 111 and 94. --Updated section 2.8.4 for Patch 90.
09 Jul 2010	Updates for MAG*3.0*83 (rev 13). <a href="#">REDACTED</a> . --Updated sections 1.2, 2.2.1, and 2.8.1; correct typos in section 2.8.4; added new appendix for VIX.
10 Feb 2010	Updates for Patch 93 and Patch 101 (rev 12) <a href="#">REDACTED</a> -- Updated sections 1.1, 2.6, 2.8.2, 2.9 for Patch 93 -- Updated sections 2.2.3, 2.8.4, 2.9 for Patch 101
20 Oct 2009	Updates for Patch 72 and applied change pages for Patch 54 (rev 11), <a href="#">REDACTED</a> For Patch 72: updates to section 2.8.1. General cleanup and corrections for sections: 1.1, 2.2.2 2.13.3 29 Feb 2008 Patch 59 revisions (rev 10): Updates to section 2.8.3. <a href="#">REDACTED</a> .
14 Jan 2008	Patch 76 revisions (rev 9): Updates to sections 1.3, 2.8.4, and 2.11.2. <a href="#">REDACTED</a>
04 May 2007	Patch 46 and 65 revisions (rev 8): Updates to section 2.9. <a href="#">REDACTED</a> .
20 July 2006	Patch 50 revisions (rev 7): Updated section 2.9. <a href="#">REDACTED</a>
30 June 2006	Patch 18 revisions (rev 6): Updated sections 1.2, 2.8, 2.9, and 2.11.2. Removed obsolete sections 2.11.2.1 and 2.11.2.2. <a href="#">REDACTED</a>
05 Dec 2005	Patch 57 revisions (rev 5): Added 2 keys released with patch 30 to section 2.8. Removed obsolete information from sections 2.10 and 2.11. Incorporated p45 changes to sections 2.2 and 2.12. <a href="#">REDACTED</a>
8 Feb 2005	Updated information for Patch 48 (rev 4). <a href="#">REDACTED</a>
27 April 2004	Changed "Revision 1" references" to "Revision 2"
23 April 2004	Updated information for Patch 8 (rev 3)
16 April 2004	Updated information for Patch 11
5 Nov 2003	Updated Security Features section

# Preface

This manual is provided to control the release of sensitive information related to VistA Imaging V. 3.0 software (**Note:** The Security Guide will not be included in any Freedom of Information Act (FOIA) request releases.) This document shall not be distributed outside the VA Intranet.

Since certain keys and authorization must be delegated for proper management of the VistA Imaging System, information about these items also may be found in the technical and user manuals.

# Table of Contents

<b>Chapter 1</b>	<b>Security Management .....</b>	<b>1</b>
1.1	Introduction .....	1
1.2	Software Application and User Interface.....	1
1.3	Security Measures.....	1
<b>Chapter 2</b>	<b>Security Features .....</b>	<b>3</b>
2.1	Mail Group and Alerts.....	3
2.2	Remote Systems.....	3
2.2.1	Remote Image Views .....	3
2.2.2	Routing to DICOM Storage SCPs (Service Class Providers).....	4
2.2.3	Query/Retrieve.....	4
2.2.4	Images Posted to MIRC .....	4
2.2.5	AWIV with CVIX.....	4
2.3	Archiving/Purging.....	5
2.4	Contingency Planning .....	6
2.4.1	Magnetic Share.....	6
2.4.2	Optical Disk Jukebox .....	6
2.4.3	Network.....	6
2.4.4	Workstations Used During Medical Care Procedures.....	6
2.5	Interfacing .....	7
2.6	Electronic Signature.....	8
2.7	Menus .....	9
2.8	Security Keys .....	9
2.8.1	General Security Keys.....	9
2.8.2	Security Keys for Clinical Display .....	10
2.8.3	Security Keys for Clinical Capture.....	11
2.8.4	Security Keys for VistARad .....	12
2.8.5	Security Keys for the DICOM Importer II.....	13
2.9	File Security .....	14
2.10	Windows Security .....	25
2.11	Workstation Security.....	25
2.11.1	SMS Software, DICOM Gateways and Background Processors .....	26
2.11.2	SMS Software and VistARad.....	26
2.12	Audit Trails .....	26
2.13	VistA DICOM Gateway .....	27
2.13.1	Modality Worklist.....	27
2.13.2	DICOM Gateway Service Account.....	27
2.13.3	Kernel RPC Broker Routines .....	28
2.14	HDIG Security.....	28
2.14.1	HDIG Service Account.....	29
2.14.2	Apache Tomcat Administrator Account.....	29
2.14.3	DICOM AE Security Matrix .....	30
2.14.4	Security Keys Required for Deleting a Study by Accession Number.....	30

## Table of Contents

2.14.5	Security Mechanisms for the Logs in that Record HDIG Activities .....	30
2.14.6	Patient Security Logging for Sensitive Patients.....	31
2.15	Background Processor Servers.....	31
2.16	References.....	32
<b>Appendix A</b>	<b>VIX Security Information .....</b>	<b>35</b>
	The VIX and CVIX are described in detail in the <i>VIX Administrator's Guide</i> .....	35
A.1	Mail Groups, Alerts, and Bulletins.....	35
A.2	Remote Systems.....	35
A.3	Archiving .....	35
A.4	Contingency Planning .....	35
A.5	Interfacing .....	35
A.6	Electronic Signatures .....	35
A.7	Menus .....	35
A.8	Security Keys .....	36
A.9	File Security .....	36
A.10	Software Pushes and the VIX .....	36
A.11	VistA Account for BHIE Framework Access .....	36
A.12	References.....	36
A.13	Official Policies.....	36
<b>Glossary</b> .....		<b>37</b>

# Chapter 1 Security Management

## 1.1 Introduction

The VistA Imaging System captures, stores, displays, and distributes medical images. These medical images are part of a patient's medical record and are protected by the Federal Privacy Act and by HIPAA (the Health Insurance Portability and Accountability Act). Images are stored on magnetic servers that are backed up on optical disk jukebox servers. The hardware configurations should include a high-capacity tape backup unit. Additionally, backups (copies) of the optical platters can be created. Those backups should be taken off site. Security keys are required for use of the package and special features such as image deletion. An electronic signature is required for copying and printing images. The Joint Commission on Accreditation of Health Organizations (JCAHO) has been very interested in image storage during their visits to the VistA Imaging sites and has recommended guidelines in these areas.

## 1.2 Software Application and User Interface

The VistA Imaging System is a suite of Windows applications with user interfaces written predominately in Delphi. Certain components are written in C++ (VistARad), Java (the VIX) and M (the DICOM Gateway), and Java (the Query/Retrieve application).

Client components in the Imaging System make calls to the Veterans Health Information Systems and Technology Architecture (VistA) hospital information system using the Remote Procedure Call (RPC) Broker.

***The Food and Drug Administration classifies this software as a medical device. As such, it may not be changed in any way. Modifications to this software may result in an adulterated medical device under 21CFR820, the use of which is considered to be a violation of US Federal Statutes.***

## 1.3 Security Measures

The VistA Imaging servers and workstations are protected by several security measures. Security protection is built into the software for Windows XP, Windows 7, Windows 2008 Server, Windows 2010 Server, and Windows 2012 Server. The use of other versions of Windows is not permitted. If a site has a requirement to use an unpermitted operating system version, then the site's administrator should contact the VistA Imaging National Project Office (NPO). The Food and Drug Administration (FDA) Quality System Regulation (QSR) permits the use of the VistA Imaging software only on approved hardware and operating systems. Only the NPO can determine compliance with QSR (not Customer Support or any other party), elect to test a new platform, or authorize any changes.

This page intentionally left blank.



# Chapter 2 Security Features

## 2.1 Mail Group and Alerts

The MAG SERVER mail group is created during the VistA Imaging KIDS software installation. This mail group is used for messages related to system configuration and usage based on information collected by the software. The VistA Imaging KIDS installer and the remote imaging development mail group are added as initial members.

There are no alerts that are created, required, or used by this application.

## 2.2 Remote Systems

### 2.2.1 Remote Image Views

When the remote image viewing functionality is used without a VistA Image Exchange (VIX) service, the VistA Imaging system logs image access information at remote sites. User accounts are also created on the remote system when the user logs into their local system and accesses remote images. Images from remote sites are transmitted to the local site for viewing with the Clinical Display client or VistARad client on an as-requested basis. No encryption is used for the images or the data. Verification of the image integrity is done visually by the user.

For information about VIX-supported remote image views, see *Appendix A VIX Security Information*.

Patch 111 provides the availability of the Broker Security Enhancement (BSE) for VistA Imaging clients. BSE is a token based authentication method that provides enhanced security over the previously used CAPRI login method.

Patch 94 modifies remote image view functionality in Display and TeleReader to make use of BSE. The client will first use BSE when attempting to connect to remote sites. If BSE fails, the client will use the CAPRI remote site login. When CAPRI is used, the system will generate a log entry to track the usage of the CAPRI authentication method. Using the BSE or CAPRI remote login method does not affect the usability of the applications, and it is transparent to the user.

The Kernel Team will release a patch to disable the CAPRI authentication method after Patch 94 is released. When the Kernel Team disables the CAPRI authentication method, only clients 94 and later will be able to connect to sites for remote image viewing.

Users with the annotation permission at the remote site can make annotations to remote VA images. Remote annotating is intended to assist in remote interpretation of images.

#### Notes:

1. Users cannot annotate images from the Department of Defense (DoD).
2. Users cannot save permanent annotations to VistARad-annotated radiology images.
3. Radiology image annotations can only be saved in the VistARad application.

### **2.2.2 Routing to DICOM Storage SCPs (Service Class Providers)**

Studies and associated header data may be pushed to DICOM Storage SCPs on an ad hoc basis. Site-configurable rules-based routing may also be used to push newly acquired studies and associated header data to DICOM Storage SCPs without human intervention.

Confirmation and acknowledgement is provided via the methods inherent in a DICOM data exchange.

Transmitted data is not encrypted; US Federal regulations and VA internal policy prohibit unencrypted transmission of patient information outside the VA's intranet.

### **2.2.3 Query/Retrieve**

Studies and associated header data may be retrieved by validated DICOM Query/Retrieve SCUs (Service Class Users) on an ad hoc basis. To receive the data, DICOM Query/Retrieve SCUs must provide valid patient and study attributes.

Confirmation and acknowledgement is provided via the methods inherent in a DICOM data exchange.

Transmitted data is not encrypted; US Federal regulations and VA internal policy prohibit unencrypted transmission of patient information outside the VA's intranet.

### **2.2.4 Images Posted to MIRC**

VistARad can be used to post images, series, or exams of broader interest (a.k.a. "teaching files") to local or offsite Medical Imaging Resource Center (MIRC) servers. It is imperative that images posted to such servers contain no personally identifiable information (PII). Ensuring that images contain no PII is the user's responsibility. VistARad will have already removed any PII from text data. However, burned-in pixel data cannot be removed. Therefore, the user must ensure that there is no PII in the burned-in pixel data of any image, series, or exam uploaded to the MIRC.

### **2.2.5 AWIV with CVIX**

The VistA Imaging Advanced Web Image Viewer (AWIV) retrieves all image information from the Centralized VistA Imaging Exchange (CVIX) service. Access to the AWIV is available only from within VistAWeb and requires the user to authenticate against a VistA system. User credentials from VistAWeb are passed to the AWIV using 256-bit AES encryption and are used to connect to remote VA systems through the CVIX. Access to VA data through the CVIX shares the same functionality as VIX-supported remote image views, described in Appendix A.

#### **2.2.5.1 AWIV Web Application**

The AWIV Web Application, hosted on the CVIX, is independent of VistAWeb and VistA Imaging Clinical Display, and enables use of the AWIV via Microsoft Edge/Google Chrome.

The AWIV Web Application is hosted on the CVIX because it is not feasible to acquire secure socket layer (SSL) certificates for each VA VIX service. SSL certificates are used to encrypt the communication of data between web browsers and the CVIX.

#### **2.2.5.2 Security Keys for AWIV**

Users of the AWIV Web Application are required to be authenticated to the claims system or have security keys that allow them access to view images. During the log-in process users will

select what site they wish to authenticate against. The user must have a valid account at that site to view log-in. Patient lookup is then done against this selected site. Only patients seen at this site can be viewed.

Users authenticated against VHA facilities (non-claims users) will have access to images based on the security keys the user has at that facility. Enforcement of security keys is handled by the AWIV Web Application, with the exception of the MAG REVIEW NCAT key. The AWIV Web Application passes a parameter to the AWIV component which indicates if the user has the MAG REVIEW NCAT key. The enforcement of the MAG REVIEW NCAT key is handled by the AWIV component.

### Security Keys Supported by AWIV Web Application

Security Key	Function
MAGDISP ADMIN	Enables the holder to display administrative images/documents.
MAGDISP CLIN	Enables the holder to display clinical images/documents.
MAG PAT PHOTO ONLY	Enables a user to view the patient photo only and gives the user no other functionality.
MAG REVIEW NCAT	User can view NCAT Report.
MAG ROI	Users with this key need not enter an electronic signature when printing images.

**Note:** NCAT reports are available if NCAT is available and online.

### 2.3 Archiving/Purging

All images acquired using the VistA Imaging System are archived immediately to the optical disk jukebox. This provides two copies of the image on site for an initial period of time. In addition, the magnetic server should be backed up regularly as specified by site system administrator. The tapes and/or optical media copies should be moved to an offsite location.

**Note:** See the Installation Guide for details on backup types and frequency.

Images are periodically purged from the magnetic server to free up disk space. A purge can be started manually by the VistA Imaging coordinator. Typically, the process is either triggered automatically when the available free space is less than a site-specified threshold or scheduled to manage space and backup activities. Images on the jukebox are never deleted. The coordinator specifies the date criteria for the purge: the Date Accessed, the Date Created, or the Date Modified, which are attributes of an image on the RAID. Keep Days are specified by the type of image.

The Purge operation checks for pointers to network locations on the jukebox, and then verifies that the database references to the images are correct and that the files referenced are on the jukebox before it purges them.

After the magnetic copy of an image is purged, the only copy of the image will be the one on the jukebox. This is why it is critical to create backups of optical disk platters.

## **2.4 Contingency Planning**

The VistA Imaging System relies on a number of devices for its operation, including magnetic file servers, one or more optical disk jukebox servers, network components and workstations.

Sites should have procedures defined for use in case of a system outage.

### **2.4.1 Magnetic Share**

Image management software within the VistA Imaging package allows a site with a magnetic share that is down, to indicate that it is “offline”. When a share is set to “offline”, all images will be retrieved directly from the jukebox.

In many cases, sites have chosen to purchase “clustered” Microsoft Windows™ file servers. This adds an extra layer of redundancy that allows the image shares to be accessible even if a server is down.

Read/write access to image shares is limited to restricted accounts.

### **2.4.2 Optical Disk Jukebox**

The jukebox is used for long-term storage. Most of the time images that are requested will reside on the magnetic server. Access to jukebox shares is also restricted.

### **2.4.3 Network**

The VistA Imaging System is dependent on a properly operating network. Network problems will cause users to be unable to view images or to access data within VistA. Some DICOM image capture capability is available even under conditions where VistA, the servers, or the hospital network is not operational. However, the network should be repaired as quickly as possible, as there is no workstation access to images. Sites should maintain equipment for detecting problems in their network and spare switches and devices for rapid maintenance and repair. It is very important that sites have proper documentation of their networks. These documents should be available for review by your Regional Information Security Officer (RISO).

### **2.4.4 Workstations Used During Medical Care Procedures**

If a workstation malfunctions, it is necessary that the workstation be repaired or replaced immediately. In many cases the patient is in the operating room or having a procedure performed at the time of the failure. It is recommended that medical centers keep “hot spare” workstations available so that when a trouble call is placed, the new workstation can immediately replace the problem workstation. Subsequently, the failed workstation can be repaired as time permits.

## 2.5 Interfacing

VistA Imaging interfaces to a number of image capture devices and to other systems. The following is a list of devices and systems that have been used by the application:

<b>Product</b>	<b>Connection type</b>	<b>Used in (Medical Center) Service/Section</b>	<b>Restriction</b>
Electron Microscope with JVC video camera mounted with an adapter	Video output	Pathology Lab	Imaging procedure keys
Multi-headed microscope with JVC video camera mounted with an adapter	RGB analog output	Hematology (can also be used for live conferencing)	Imaging procedure keys
Document Scanners - HP Desktop - Microtek – Fujitsu	TWAIN/ SCSI inter- face	Tumor Registry, Medical Libraries, Scanned Advance Directives, Consent Forms	Imaging procedure keys
Siemens Cardiac Catheterization system	RGB (may require a composite to RGB converter)	Cath Lab	Imaging procedure keys
Echocardiograph Ultra Sound unit	RGB analog output	Echo Lab	Imaging procedure keys
Video Endoscopy Unit via probe (Fuji & Olympus)	RGB analog output	GI Lab	Imaging procedure keys
Pulmonary Endoscope	RGB analog output	Bronc Lab	Imaging procedure keys
Endoscopic retrograde cholangiopancreatography (ERCP) procedure to C-ARM	Import to floppy disk	Radiology equipment used during endoscopic procedure	Imaging procedure keys
Regular VCR viewer with calibration	Video output	Neurology for sleep studies	Imaging procedure keys
Arthroscope	Video output	Orthopedics	Imaging procedure keys

<b>Product</b>	<b>Connection type</b>	<b>Used in (Medical Center) Service/Section</b>	<b>Restriction</b>
Laparoscope	Video output	Vascular, Surgery	Imaging procedure keys
SLIT Lamp	Video output	Ophthalmology	Imaging procedure keys
Cystoscope	RGB analog output	Urology	Imaging procedure keys
Digitized scanners: Lumisys 75, Lumisys 100, 150	SCSI port or TWAIN interface	Radiology	Imaging procedure keys
Portable hand held cameras: Olympus, Polaroid, Kodak	Via import function from USB 2.0 or higher, FireWire, or Thunderbolt	Dermatology, Plastic Surgery, operating rooms, Orthopedics, emergency rooms, wards, clinics (Example of types of images: lesions, bedsores, skin pigmentation, etc.)	Imaging procedure keys

Please note the security of the equipment will depend on the Medical Center's policies and/or the medical area supervision.

All equipment purchased for interfacing with the VistA Imaging System must first be tested by the VistA Imaging development team.

## 2.6 Electronic Signature

The VistA Imaging System requires an electronic signature when an image is copied or printed from the image database. The signature is required of the person obtaining the image to indicate that privacy and security will be properly protected for that image and that the image is being copied or printed for an authorized purpose.

Only one electronic signature is required when attaching image groups to a signed TIU note. Prior to Patch 94, users were required to electronically sign each image in a group, individually.

## 2.7 Menus

On the workstations, there is a menu option that allows users with the MAG DELETE key to delete images that have been collected in error. A record is kept of all deleted images.

## 2.8 Security Keys

There are a number of security keys associated with the VistA Imaging system. The following tables summarize security keys and their function.

### 2.8.1 General Security Keys

**Note:** Please be cautious when assigning the following keys; the keys are intended for Imaging Support personnel. Review the descriptions before assigning these keys.

General Security Keys	
MAG ANNOTATE MGR	User can add, edit, and delete annotations. Permissions provided by this key apply only to images at the site where the user has the key. This key also allows users to create annotations regardless of the settings of the user's account in the PARAMETER DEFINITION (MAG IMAGE ALLOW ANNOTATE) specified at a given site.
MAGDFIX ALL	Allows the holder to perform DICOM CORRECT functions on any entry in the DICOM FAILED IMAGES file (#2006.575). Users who do not hold this key will only be able to correct entries that were captured on their own site's gateway.
MAG DELETE	This key allows the holder to delete images from the IMAGE file (#2005). Pointers in parent packages such as Medicine, Surgery, Lab, Radiology, and TIU will also be deleted.
MAG DOD FIX	This key gives the holder permission to run the MagKat utility.
MAG PREFETCH	This key allows a user to 'PreFetch' or Queue all images for a patient. This means that all images for a patient that are on the jukebox will be copied from the jukebox to the magnetic server cache.
MAG SYSTEM	Given to person(s) managing VistA Imaging Systems. Required to modify site parameters via the Background Processor or to modify workstation parameters via the MAGSYS application. Also enables the display of DICOM header data for radiology images on Clinical Display workstations.

General Security Keys	
MAG VIX ADMIN	This key grants access to the VIX transaction log and HDIG administration parameters (HDIG server accounts access/verify code and email addresses). This key should be assigned to VIX and HDIG administrators. For more information, see the <i>VIX Administrator's Guide</i> .

### 2.8.2 Security Keys for Clinical Display

The following keys are used for display of images and should be limited to appropriate personnel.

Display-related Security Keys	
MAG RAD SETTINGS	User can edit the CT Presets in the Clinical Imaging Display Radiology Viewer window.
MAG ROI	User can print (single or multiple) images or copy images without having to enter an electronic signature. This key should only be assigned to the HIMS Release of Information Officer.
MAGDISP ADMIN	User can display administrative images/documents.
MAGDISP CLIN	User can display clinical images/documents.
MAG EDIT	The MAG EDIT key is used to correct an image field when an index field is incorrect or incomplete, such as correction of a wrongly selected specialty. Only users assigned the MAG EDIT key can edit an image. The MAG EDIT key is also required to access the QA Review Utility when performing quality assurance reviews of the scanned images. Only the Chief, HIM or authorized designated personnel (e.g., VistA Imaging Coordinator, Scanning Supervisor) should be assigned this key.
MAG PAT PHOTO ONLY	User can view only the patient photo.
MAG QA REVIEW	User can access QA Review and QA Review Report from Clinical Display Utilities Menu.
MAG REVIEW NCAT	User can view NCAT reports.
MAG VIEW DOD IMAGES	In Patch 72 and 93 versions of Clinical Display, users must have this key to display DoD images.  In newer versions of Clinical Display, this key is not checked.



### 2.8.3 Security Keys for Clinical Capture

**Note:** If the 'CAPTURE KEYS' site parameter has been initialized, the following keys will need to be assigned appropriately.

Capture-related Security Keys	
MAG CAPTURE	Allow capture of images without an associated specialty (e.g., 'NONE' on the Imaging Capture configuration window).
MAG NOTE EFILE	User can electronically file notes without an electronic signature from the Imaging Capture workstation.
MAGCAP ADMIN	Allow capture of images associated with the 'Admin Document' specialty.
MAGCAP CP	Allow capture of Clinical Procedure images.
MAGCAP LAB	User can capture Laboratory images from the Imaging Capture workstation.
MAGCAP MED C	User can capture Cardiology images from the Imaging Capture workstation.
MAGCAP MED G	User can capture GI images from the Imaging Capture workstation.
MAGCAP MED GEN	User can capture Generic Medicine images from the Imaging Capture workstation.
MAGCAP MED H	User can capture Hematology images from the Imaging Capture workstation.
MAGCAP MED HI	User can capture Internal Medicine / Hematology images from the Imaging Capture workstation.
MAGCAP MED I	User can capture Internal Medicine images from the Imaging Capture workstation.
MAGCAP MED N	User can capture Neurology images from the Imaging Capture workstation.
MAGCAP MED P	User can capture Pulmonary / Endoscopy images from the Imaging Capture workstation.
MAGCAP MED PF	User can capture Pulmonary Function Test images from the Imaging Capture workstation.
MAGCAP MED R	User can capture Rheumatology images from the Imaging Capture workstation.
MAGCAP MED Z	User can capture Consult images from the Imaging Capture workstation.
MAGCAP PHOTOID	User can capture Photo ID images from the Imaging Capture workstation.

<b>Capture-related Security Keys</b>	
MAGCAP RAD	User can capture Radiology images from the Imaging Capture workstation.
MAGCAP SUR	User can capture Surgery images from the Imaging Capture workstation.
MAGCAP TIU	User can capture TIU images from the Imaging Capture workstation.
MAGCAP TRC	A user with this key can capture images associated with a "TeleReader Consult" from the Imaging Capture workstation.

#### 2.8.4 Security Keys for VistARad

The following keys are related to VistARad and should be limited to appropriate personnel.

<b>VistARad-related Security Keys</b>	
MAGJ DEMAND ROUTE	User can access VistARad's on-demand routing capability. On-demand routing can be used to manually send exams to remote sites. For more information, refer to the VistARad or Routing User Guides.
MAGJ DEMAND ROUTE DICOM	Allows the user to use the on-demand routing function to queue exam images to be routed to selected remote DICOM destinations. This function only works for sites that have been configured for routing of images. An updated Routing agreement needs to be submitted and approved by the VistA Imaging Group before this function can be used.
MAGJ OVERRIDE ANNOTATIONS	Grants to a radiologist user of VistARad access to the menu option Override Annotations when viewing an exam whose status is "Complete." This functionality is detailed in the VistARad User Guide and Vista Imaging Technical Manual.
MAGJ REMOTE ACCESS CONTROL	Allows a VistARad user to access the Monitored Sites configuration subset of the VIX Configuration settings tab, and to view exam list data in the Monitored Sites tab of the Manager.
MAGJ SEE BAD IMAGES	User can view images in VistARad that are associated with an exam that has failed the "Patient Safety" database checks.
MAGJ STORE IMAGES	Allows VistARad users to save Voxar images as secondary captures to VistA.

VistARad-related Security Keys	
MAGJ SYSTEM MANAGER	Allows access to Voxar-related settings in the VistARad Settings dialog. Grants access to additional data in the Imaging Internal Data display window. This functionality is detailed in the <i>VistARad User Guide</i> and <i>VistA Imaging Technical Manual</i> . Assigned only to VistARad administrators. Grants access to the Local Site VIX configuration subset of the VIX Configuration tab.
MAGJ SYSTEM USER	Allows a user to create and delete site-level hanging protocols, templates, and image presets associated with the VistARad 'sysAdmin' user.
MAGJ VOXAR COPYIMAGE	Allows VistARad users to copy images using Voxar (Enables the <b>Copy to Clipboard</b> button in the Voxar Reading manager window; refer to Voxar documentation for more information.)
MAGJ VOXAR EXPORTCAPTURE	Allows VistARad users to export images using Voxar (Enables the three <b>Export</b> -related buttons in the Voxar Reading manager window; refer to Voxar documentation for more information.)
MAGJ VOXAR PRINTCOMPOSER	Allows VistARad users to print images using Voxar (Enables the <b>Print Composer</b> button in the Voxar Reading manager window; refer to Voxar documentation for more information.)

### 2.8.5 Security Keys for the DICOM Importer II

The DICOM Importer II is a role-based application. The tasks that users can perform are linked to the role of the user. This allows Imaging System Managers and Imaging System Administrators to define different types of user accounts and thus limit access to the functions that the DICOM Importer II provides.

For more information about the roles, see the *DICOM Importer II User Manual*.

All users of the DICOM Importer II client application must have the MAG DICOM VISA menu assigned as a secondary menu option. In addition to this, each user must have one of the following security keys, depending on their role.

Security Keys for the DICOM Importer II	
MAGV IMPORT MEDIA STAGER	Allows DICOM Importer II users to stage (copy) from media to staging persistent storage, where it waits for reconciliation processing.

<b>Security Keys for the DICOM Importer II</b>	
<b>MAGV IMPORT STAGE MEDIA ADV</b>	<p>Allows DICOM Importer II users to:</p> <ul style="list-style-type: none"> <li>• Stage (copy) studies from media to staging persistent storage and</li> <li>• View images on the media.</li> </ul> <p>This key extends security key MAGV IMPORT MEDIA STAGER.</p>
<b>MAGV IMPORT RECON CONTRACT</b>	<p>Allows DICOM Importer II users to:</p> <ul style="list-style-type: none"> <li>• Stage media at the study level</li> <li>• View images on the media</li> <li>• Associate study DICOM objects with an existing Radiology or Consult order for reconciliation.</li> </ul>
<b>MAGV IMPORT RECON ARTIFACT</b>	<p>Allows DICOM Importer II users to:</p> <ul style="list-style-type: none"> <li>• Stage media at the study level</li> <li>• View images on the media</li> <li>• Associate study DICOM objects with an existing Radiology or Consult order for reconciliation.</li> <li>• Place new Radiology orders using the Importer II user interface.</li> <li>• Use DICOM Correct to fix errors in studies in the DICOM Correct queue.</li> <li>• Manage the DICOM Importer II queue</li> <li>• Run, view, print and save DICOM Importer II reports</li> </ul>
<b>MAGV IMPORT REPORTS</b>	<p>Allows DICOM Importer II users to view, print, and save reports to a text file.</p>

## 2.9 File Security

The following table lists all files associated with the VistA Imaging application and the default VA FileMan security for each.

<b>File Security</b>							
<b>File Number</b>	<b>File Name</b>	<b>DD Access</b>	<b>RD Access</b>	<b>WR Access</b>	<b>DEL Access</b>	<b>LAYGO Access</b>	<b>Audit Access</b>
2005	IMAGE	@	@	@	@	@	
2005.001	IMAGING STUDY	@	@	@	@	@	@
2005.002	IMAGING ANNOTATION FILE	@	@	@	@	@	

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2005.02	OBJECT TYPE	@	@	@	@	@	
2005.021	IMAGE FILE TYPES	@	@	@	@	@	@
2005.03	PARENT DATA FILE	@	@	@	@	@	
2005.1	IMAGE AUDIT	@	@	@	@	@	
2005.2	NETWORK LOCATION	@	@	@	@	@	
2005.4	IMAGE HISTOLOGICAL STAIN	@	@	@	@	@	
2005.41	MICROSCOPIC OBJECTIVE	@	@	@	@	@	
2005.6	IMAGING PATIENT REFERENCE	@	@	@	@	@	@
2005.61	IMAGING PROCEDURE REFERENCE	@	@	@	@	@	@
2005.62	IMAGE STUDY	@	@	@	@	@	@
2005.63	IMAGE SERIES	@	@	@	@	@	@
2005.64	IMAGE SOP INSTANCE	@	@	@	@	@	@
2005.65	IMAGE INSTANCE FILE	@	@	@	@	@	@
2005.66	IMAGING DUPLICATE UID LOG	@	@	@	@	@	@
2005.71	IMAGING DICOM FIELDS	@	@	@	@	@	@

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2005.8	IMAGING SERVICE INSTITUTION	@	@	@	@	@	
2005.81	MAG DESCRIPTIVE CATEGORIES	@	@	@	@	@	
2005.82	IMAGE INDEX FOR CLASS	@	@	@	@	@	@
2005.83	IMAGE INDEX FOR TYPES	@	@	@	@	@	@
2005.84	IMAGE INDEX FOR SPECIALTY/SUBSPECIALTY	@	@	@	@	@	@
2005.85	IMAGE INDEX FOR PROCEDURE/EVENT	@	@	@	@	@	@
2005.86	IMAGE ACTIONS	@	@	@	@	@	@
2005.87	IMAGE LIST FILTERS	@	@	@	@	@	@
2005.872	DICOM INDEX MAPPING	@	@	@	@	@	@
2005.88	MAG REASON FILE	@	@	@	@	@	@
2005.99	IMAGE INDEX FOR BODY PART	@	@	@	@	@	@
2006.03	IMAGE BACKGROUND QUEUE	@	@	@	@	@	
2006.031	IMAGE BACKGROUND QUEUE POINTER	@	@	@	@	@	
2006.033	OFFLINE IMAGES	@	@	@	@	@	

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.034	IMPORT QUEUE	@	@	@	@	@	@
2006.035	SEND QUEUE	@	@	@	@	@	@
2006.036	ROUTING STATISTICS	@	@	@	@	@	@
2006.04	ACQUISITION DEVICE	@	@	@	@	@	@
2006.041	ACQUISITION SESSION FILE	@	@	@	@	@	@
2006.1	IMAGING SITE PARAMETERS	@	@	@	@	@	
2006.15	DICOM UID ROOT	@	@	@	@	@	@
2006.17	MUSE VERSIONS	@	@	@	@	@	@
2006.18	IMAGING USER PREFERENCE	@	@	@	@	@	
2006.19	IMAGING USERS	@	@	@	@	@	
2006.5	PACS MESSAGE	@	@	@	@	@	@
2006.51	DICOM DATA ELEMENT DICTIONARY	@	@	@	@	@	@
2006.511	DIAGNOSTIC INFO FIELD	@	@	@	@	@	@
2006.52	DICOM MESSAGE TEMPLATE DICTIONARY	@	@	@	@	@	@
2006.53	DICOM UID DICTIONARY	@	@	@	@	@	@
2006.531	EXTENDED SOP NEGOTIATION	@	@	@	@	@	@

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.532	DICOM SOP CLASS	@	@	@	@	@	@
2006.539	DICOM UID SPECIFIC ACTION	@	@	@	@	@	@
2006.54	PDU TYPE	@	@	@	@	@	@
2006.55	DICOM WORKLIST PATIENT	@	@	@	@	@	@
2006.56	DICOM WORKLIST STUDY	@	@	@	@	@	@
2006.563	DICOM GATEWAY PARAMETER	@	@	@	@	@	@
2006.564	DICOM QUEUE	@	@	@	@	@	@
2006.5641	DICOM GATEWAY MACHINE ID	@	@	@	@	@	@
2005.565	EXPORT DICOM RUN FILE	@	@	@	@	@	@
2006.57	DICOM HL7 SEGMENT	@	@	@	@	@	@
2006.571	DICOM RAW IMAGE	@	@	@	@	@	@
2006.5711	DICOM M2MB RPC QUEUE	@	@	@	@	@	@
2006.5712	DICOM FIXED QUEUE	@	@	@	@	@	@
2006.5713	DICOM UNKNOWN MODALITY	@	@	@	@	@	@
2006.5714	DICOM INCOMPLETE OBJECT	@	@	@	@	@	@



File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.5715	CURRENT IMAGE	@	@	@	@	@	@
2006.5719	DICOM ERROR LOG	@	@	@	@	@	@
2006.572	EXAMINATION COMPLETE	@	@	@	@	@	@
2006.573	GE PACS QUERY/RETRIEVE	@	@	@	@	@	@
2006.5732	DICOM QUERY RETRIEVE RESULT	@	@	@	@	@	@
2006.5733	QUERY/RETRIEVE STATISTICS	@	@	@	@	@	@
2006.574	DICOM IMAGE OUTPUT	@	@	@	@	@	@
2006.575	DICOM FAILED IMAGES	@	@	@	@	@	@
2006.5751	DICOM OBJECTS TO BE IMPORTED	@	@	@	@	@	@
2006.5752	IMPORTABLE DICOM OBJECTS	@	@	@	@	@	@
2006.5757	DICOM RADIOLOGY PROCEDURE MODIFIERS	@	@	@	@	@	@
2006.5758	DICOM RADIOLOGY PROCEDURES	@	@	@	@	@	@
2006.5759	OUTSIDE IMAGING LOCATION	@	@	@	@	@	@
2006.5761	DICOM MESSAGE STATISTICS	@	@	@	@	@	@

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.5762	DICOM INSTRUMENT STATISTICS	@	@	@	@	@	@
2006.5763	DICOM PACS STATISTICS	@	@	@	@	@	@
2006.5764	DICOM LOCAL INSTRUMENT STATISTICS	@	@	@	@	@	@
2006.577	DICOM FIFO QUEUE	@	@	@	@	@	@
2006.58	DICOM LOG	@	@	@	@	@	@
2006.581	INSTRUMENT DICTIONARY	@	@	@	@	@	@
2006.582	MODALITY TYPE DICTIONARY	@	@	@	@	@	@
2006.5821	CT CONVERSION PARAMETERS	@	@	@	@	@	@
2006.583	MODALITY WORKLIST DICTIONARY	@	@	@	@	@	@
2006.5831	DICOM HEALTHCARE PROVIDER SERVICE	@	@	@	@	@	@
2006.5839	DICOM GMRC TEMP LIST	@	@	@	@	@	@
2006.584	TCP/IP PROVIDER PORT LIST	@	@	@	@	@	@
2006.5841	TELEREADER ACQUISITION SERVICE	@	@	@	@	@	@

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.5842	TELEREADER ACQUISITION SITE	@	@	@	@	@	@
2006.5843	TELEREADER READER	@	@	@	@	@	@
2006.5849	TELEREADER READ/UNREAD LIST	@	@	@	@	@	@
2006.585	USER APPLICATION	@	@	@	@	@	@
2006.586	PROVIDER APPLICATION	@	@	@	@	@	@
2006.587	DICOM TRANSMIT DESTINATION	@	@	@	@	@	@
2006.588	APPLICATION ENTITY TITLE	@	@	@	@	@	@
2006.59	ROUTING RULE	@	@	@	@	@	@
2006.5906	ROUTE LOAD BALANCE	@	@	@	@	@	@
2006.596	ACTION QUEUE STATUS	@	@	@	@	@	@
2006.598	DICOM ERROR MESSAGE QUEUE	@	@	@	@	@	@
2006.599	DICOM Error Log	@	@	@	@	@	@
2006.61	MAG RAD EXAM STATUS CATEGORIES						
2006.621	MAG CT PARAMETER	@	@	@	@	@	@

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.623	MAG CR PARAMETER	@	@	@	@	@	@
2006.63	MAG RAD LIST DATA ELEMENTS	@	@	@	@	@	@
2006.631	MAG RAD LISTS DEFINITION	@	@	@	@		@
2006.634	MAGJ ZLIST SEARCH	@	@	@	@	@	@
2006.65	MAG RAD PRIOR EXAMS LOGIC	@	@	@	@	@	@
2006.67	MAG RAD CPT MATCHING	@	@	@	@	@	@
2006.671	MAG RAD BODY PART	@	@	@	@	@	@
2006.672	MAG RAD BODY REGION	@	@	@	@	@	@
2006.68	MAGJ USER DATA	@	@	@	@	@	@
2006.69	MAG VISTARAD SITE PARAMETERS	@	@	@	@	@	@
2006.8	BP WORKSTATIONS	@	@	@	@	@	
2006.81	IMAGING WINDOWS WORKSTATIONS	@	@	@	@	@	@
2006.82	IMAGING WINDOWS SESSIONS	@	@	@	@	@	
2006.83	DICOM WORKSTATION	@	@	@	@	@	@

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.87	DICOM GATEWAY INFORMATION	@	@	@	@	@	@
2006.911	DICOM GATEWAY INSTRUMENT DICTIONARY	@	@	@	@	@	
2006.912	DICOM GATEWAY MODALITY DICTIONARY	@	@	@	@	@	
2006.913	ARTIFACT KEYLIST	@	@	@	@	@	
2006.914	RETENTION POLICY	@	@	@	@	@	
2006.915	ARTIFACT DESCRIPTOR	@	@	@	@	@	
2006.916	ARTIFACT	@	@	@	@	@	
2006.917	STORAGE PROVIDER	@	@	@	@	@	
2006.918	ARTIFACT INSTANCE	@	@	@	@	@	
2006.9191	MAGV GATEWAY CONFIGURATION	@	@	@	@	@	
2006.9192	DICOM AE SECURITY MATRIX	@	@	@	@	@	
2006.9193	IMAGING APPLICATION SERVICE	@	@	@	@	@	
2006.921	ARTIFACT RETENTION POLICY	@	@	@	@	@	

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.922	RETENTION POLICY FULFILLMENT	@	@	@	@	@	
2006.923	RETENTION POLICY STORAGE PROVIDER MAP	@	@	@	@	@	
2006.924	STORAGE PROVIDER AVAILABILITY	@	@	@	@	@	
2006.925	TRANSFER STATISTICS	@	@	@	@	@	
2006.926	STORAGE TRANSACTION	@	@	@	@	@	
2006.927	QUEUE	@	@	@	@	@	
2006.928	QUEUE MESSAGE	@	@	@	@	@	
2006.93	IMAGING EVENT AUDIT LOG	@	@	@	@	@	
2006.931	IMAGING EVENT AUDITABLE ACTION	@	@	@	@	@	
2006.941	MAG WORK ITEM	@	@	@	@	@	
2006.9411	MAG WORK ITEM HISTORY	@	@	@	@	@	
2006.9412	WORKLIST	@	@	@	@	@	
2006.9413	MAG WORK ITEM STATUS	@	@	@	@	@	
2006.9414	MAG WORK ITEM SUBTYPE	@	@	@	@	@	

File Security							
File Number	File Name	DD Access	RD Access	WR Access	DEL Access	LAYGO Access	Audit Access
2006.9421	MAGV IMPORT STUDY LOG	@	@	@	@	@	
2006.9422	MAGV IMPORT MEDIA LOG	@	@	@	@	@	
2006.95	IMAGE ACCESS LOG	@	@	@	@	@	@
2006.96	IMAGE INDEX CONVERSION	@	@	@	@	@	@
2006.961	MULTI IMAGE PRINT	@	@	@	@	@	@

## 2.10 Windows Security

Windows provides security through the use of user profiles, policies/rights, directory/share permissions and domain configuration. VistA Imaging file servers should be configured as a member servers of the VISN domain. The *VistA Imaging Installation Guide* also defines recommended user profiles, groups and policies to be administered.

## 2.11 Workstation Security

Security of an Imaging workstation is the same as any other personal computer located within the Medical Center and should be covered by the Medical Center's Equipment Security Guidelines and/or policies.

Restricting access to the VistA Imaging workstation by placing the workstation in a secure area (such as a locked office) would be optimal. However, the use of the workstation would be limited to only those assigned to the office. Placing the workstation in an open area accessible by all clinical staff would be beneficial to all but can present a problem of theft or tampering. Physical security of the PC to prevent theft or altering of internal electronic boards is recommended; a cable lock can prevent the opening of the case of the PC box unit.

Security software is required, such as virus detection software and desktop configuration restriction software. Virus protection software must be installed on the servers to protect imaging file servers against viruses. The VA has validated McAfee VirusScan for use on Imaging File Servers and other Imaging components. For guidance in locating security software information, contact the Information Protection and Risk Management (IPRM) office at their web site at [REDACTED](#). For additional assistance, contact the VA Help Desk. Commercial products are available for controlling access to system setup and files. Policies and profiles can be used to restrict access in a Microsoft Windows workstation environment. The BIOS of all VistA Imaging workstations should be password protected.

### 2.11.1 SMS Software, DICOM Gateways and Background Processors

VA Security Policy requires that, on many computers, specific software is installed to ensure that the machines are running the most up-to-date virus protection software.

DICOM Gateway Systems and Background Processors must be able to operate continually, without unplanned interruption. While it is acknowledged that any computer that is connected to the network must have adequate virus protection, the provision of this protection cannot interrupt the processing of essential medical data.

VA's SMS and EPO software distribution mechanism can trigger a safety problem because it causes the system to reboot while it might be processing essential data. As a result, the VA's SMS and EPO software cannot be installed on any VistA DICOM Gateway or Background Processor.

Each site must appoint a person who is responsible for applying Microsoft updates to the DICOM Gateways when Microsoft makes mandatory patches (also known as "Critical Updates and Service Packs") available. The responsible person should check at least once per week whether any critical updates are available, and make certain that they are installed while the medical software is not active.

The virus protection software should be configured such that it automatically downloads and applies new updates for the virus definition files on a daily basis.

### 2.11.2 SMS Software and VistARad

Because software distribution/inventory management tools can be used to install inappropriate or unapproved software without an administrator's knowledge, VistARad workstations must be excluded from Microsoft's Systems Management Server (SMS) server or similar systems.

**Note:** The installation of unapproved components onto a VistARad diagnostic workstation will result in an adulterated medical device. The use of adulterated medical devices violates US Federal Law (21CFR820).

Information about exclusion and removal of SMS can be found at: [REDACTED](#).

If there are any questions about the contents of these documents, refer to the EIE (VA Enterprise Infrastructure Engineering) portal at: [REDACTED](#) /.

## 2.12 Audit Trails

The VistA Imaging software has several files that can be used to audit usage of VistA Imaging workstations and access to image files.

- The IMAGING WINDOWS WORKSTATIONS file (#2006.81) can be used to review the date and time the Display, Capture, or VistARAD application was installed, the last access date/time the workstation was used, and who last signed onto the workstation. This information is vital for the Imaging system manager to audit workstation usage.
- The IMAGE AUDIT file (#2005.1) records data from deleted image records of the IMAGE file (#2005) and serves as an audit trail for deleted images. When image deletion takes place, the image is deleted off of the magnetic server (if it exists), and the associated specialty package pointer to the image file is deleted. The data from the IMAGE file (#2005) is copied over to the IMAGE AUDIT file (#2005.1) using the same



internal entry number. The image residing on the optical jukebox is not deleted, so it can be retrieved (if necessary) by the system manager.

- The IMAGE ACCESS LOG file (#2006.95) tracks users' access to images and patient records, as well as the copying and deleting of image files. Entries are added to the local IMAGE ACCESS LOG file (#2006.95) by remote users when accessing remote images. Actions of remote users are logged in the same manner as local image access.
- The QUERY/RETRIEVE STATISTICS file (#2006.5733) records requests for and delivery of data to Query/Retrieve SCU
- IMAGING ANNOTATION FILE (#2005.002). This file can be used to view annotation (audit) history for an image. When users with Annotations permission add and save annotations during a session, the log file tracks each annotation added and stores the following user information: name, date and time, and the user's service. The log file also tracks changes (such as modifications and deletions) that a user with the MAG ANNOTATE MGR key makes to annotations.

### 2.13 VistA DICOM Gateway

A VistA DICOM Gateway connects to a VistA system using the M2M RPC Broker. Access to the physical equipment of the DICOM Gateway itself is protected using the features of the Windows™ operating system, and access from the DICOM Gateway to the VistA Hospital Information System is protected using the standard VA Kernel security features.

There are two special cases (see following sections) where automated processes will use these standard security features in a specific fashion.

#### 2.13.1 Modality Worklist

Modality Worklist queries are processed by DICOM Gateways. Such requests are issued by Imaging equipment ("modalities") when they need patient scheduling information. Under normal circumstances, a DICOM Gateway is able to respond to a Modality Worklist query using only information that is stored locally on the DICOM Gateway. In some special cases, the DICOM Gateway needs to query its VistA Hospital Information System for details that the DICOM Gateway does not store locally. Since "modalities" are lab-equipment that connects to a DICOM Gateway directly through TCP/IP, using the standard DICOM protocol, a DICOM Gateway has no concept of a "VistA user context" for these Modality Worklist queries. In the exception that a DICOM Gateway needs to query its VistA system for old Radiology case information, it will use a special access and verify code that is configured on that DICOM Gateway (stored in encrypted form).

#### 2.13.2 DICOM Gateway Service Account

Some processes on a DICOM Gateway are executed in typical "user oriented" sessions: the user logs in, performs a task, and logs out. However, the tasks that embody the main purpose of the DICOM Gateway run for a long time, typically weeks or months on end, and are intended to keep functioning in an automated fashion, that is: without any human interaction.

Since these tasks need to be started at some point in time, a (fully privileged) user will login, and request the menu option that starts the long-running task. From that point on, the task will run and will continue to run until stopped by a system manager.

When the network connection between the DICOM Gateway and the VistA Hospital Information System is interrupted, the DICOM Gateway will recover from this situation, and will periodically attempt to reconnect (at 5 minute intervals). Once the connection is re-established, the DICOM Gateway will continue processing where it left off when the connection was interrupted.

The situation may arise that:

1. A user logs in with valid credentials.
2. Start a long-running task on a DICOM Gateway.
3. Several weeks later change his/her access or verify code on VistA.
4. Sometime after that, the DICOM Gateway loses its connection with VistA and starts making attempts to reconnect.

At this point in time, the credentials that the user provided to the DICOM Gateway (and that the DICOM Gateway will continue to use when attempting to reconnect to the VistA system) will no longer be valid, and attempts to reconnect will fail.

Since it is essential that the DICOM Gateway should be capable of continuing to perform its function, without human interaction, a site can establish a special “service account” for which the access and verify codes will not expire. When a DICOM Gateway cannot re-establish a network connection as a result of the scenario described above, the DICOM Gateway will:

1. Send an e-mail message to a local mail group warning site management that valid credentials need to be re-established
2. Use the “service account” to continue processing, until a human is available to re-establish valid credentials on the DICOM Gateway.

The DICOM Gateway service account must have the following:

- MAG VIX ADMIN security key assigned to it
- MAG DICOM VISA assigned to it as a secondary menu option
- OR CPRS GUI CHART assigned to it as a secondary menu option

### 2.13.3 Kernel RPC Broker Routines

Two RPC Broker routines are incorporated into the DICOM Gateway software:

<b>Routine</b>	<b>Used For</b>
XLFDI	Date and time formatting
XUSRB1	Encrypt/decrypt access and verify codes

### 2.14 HDIG Security

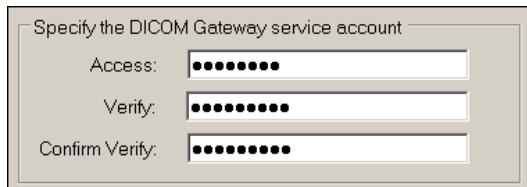
The Hybrid Image DICOM Gateway (HDIG) uses a set of security mechanisms to protect the integrity of the VistA system and the data that it stores:

- HDIG Service account
- Apache Tomcat administrator account
- AE Security Matrix

### 2.14.1 HDIG Service Account

The Hybrid Image DICOM Gateway (HDIG) uses the DICOM Gateway service account to connect to VistA and to run the services that it provides. This account is also used by the (legacy) DICOM Gateway and is described in section 2.13.2 *DICOM Gateway Service Account*.

The service account that the HDIG uses to connect to VistA is configured when the HDIG is installed for the first time. Users set the account credentials when they run the HDIG Service Installation Wizard as illustrated in the following screenshot.



For more information about the HDIG Service Installation Wizard and the requirements for the accounts whose credentials are set when the HDIG is installed for the first time, see the *VistA Imaging DICOM Gateway Installation Guide*.

The credentials for the DICOM Gateway service account are stored in an XML configuration file. The passwords for the HDIG service account are encrypted. When the DICOM Gateway service account credentials expire or when they are changed and the HDIG can no longer connect to VistA, it sends a notification that the credentials of the DICOM Gateway service account are invalid. The email addresses to which the HDIG sends notifications for invalid service account credentials are also specified when the HDIG is installed for the first time.

After initial installation, authorized users can change the password for the HDIG service account and the email addresses to which the HDIG sends notifications when it detects invalid service account credentials through the HDIG statistics page.

To change the password of the DICOM Gateway service account and the email address (or addresses) for notifications of invalid DICOM Gateway service account credentials and error in the processing flow, users must have:

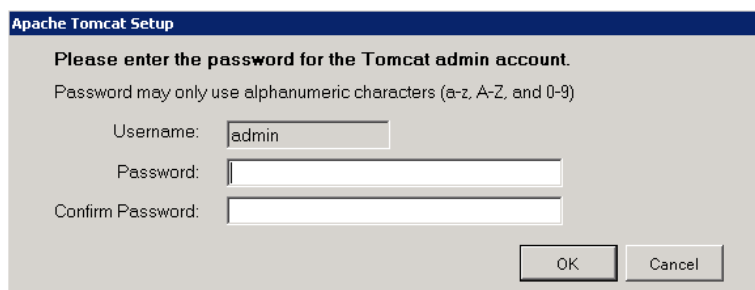
- MAG VIX ADMIN security key
- MAG DICOM VISA secondary menu option
- OR CPRS GUI CHART secondary menu option

For more information about accessing the HDIG statistics page and changing the password or the email addresses for notification for invalid credentials, see the *VistA Imaging DICOM Gateway User Guide*.

### 2.14.2 Apache Tomcat Administrator Account

The Apache Tomcat administrator account is used to run the HDIG service in the Tomcat environment on the local system. This account and its credentials are also configured when the HDIG is installed for the first time.

The following image shows the prompts to specify the credentials of the Apache Tomcat administrator account that appears when users install the HDIG for the first time.



For more information about the Apache Tomcat administrator account, see the *VistA Imaging DICOM Gateway Installation Guide*.

### 2.14.3 DICOM AE Security Matrix

Authorized users can control access to the VistA system and the services the HDIG supports through the DICOM AE Security Matrix. The DICOM AE Security Matrix is the file DICOM AE SECURITY MATRIX (#2006.9192). It includes the configuration settings of all remote device that use the DICOM services the HDIG provides to connect to the VistA system. Only devices listed in the file can access the VistA system. Each device can only use the service or services specified for the device in the DICOM AE SECURITY MATRIX.

To configure the DICOM AE SECURITY MATRIX, users must have:

- MAG SYSTEM security key
- Access to the Imaging System Manager menu [MAG SYS MENU]

For more information about the DICOM AE Security Matrix, see the *VistA Imaging DICOM Gateway Installation Guide*.

### 2.14.4 Security Keys Required for Deleting a Study by Accession Number

Authorized users can delete studies stored in VistA by accession number.

To delete a study by accession number users must have:

- MAG SYSTEM security key
- MAG DELETE security key
- Access to the Imaging System Manager menu [MAG SYS MENU]

For more information about deleting studies by accession number, see the *VistA Imaging Technical Manual*.

### 2.14.5 Security Mechanisms for the Logs in that Record HDIG Activities

The HDIG logs its activities in several logs.

- Application log

The Application log is encrypted because it may contain protected health information. Access to the Application log is restricted to authorized users. Users need the following to access the Application log:

- MAG VIX ADMIN security key
- MAG DICOM VISA VistA menu

Users must be authenticated to access the application log. For information about accessing the Application log, see the *VistA Imaging DICOM Gateway User Guide*.

- **HDIG Summary log**

The HDIG Summary log is one of the logs of the Hybrid DICOM Image Gateway (HDIG). It is useful for detecting and correcting errors in the operation of the HDIG, because it contains troubleshooting information in plain language – a format that is simple and easy to read and understand. In addition to this, the log is not encrypted and it can be accessed by authorized support and administrative personnel. For information about accessing the Application log, see the *VistA Imaging DICOM Gateway User Guide*.

- **Audit log**

The Audit log records system level events, such as HDIG startup and shutdown. It does not contain protected health information (PHI) or any other type of patient information.

Access to the Audit log is restricted to authorized VA personnel (typically the VistA administrator and the Security Officer).

All events written to the Audit log are also written to the Application log. This enables VistA Imaging coordinators and administrators to access information when troubleshooting the HDIG or trying to identify causes of problems in its operation.

#### **2.14.6 Patient Security Logging for Sensitive Patients**

The Security log records all attempts to access and retrieve the records of sensitive patients based on the user account credentials (DUZ).

For more information about the Security log, see the *PIMS V5.3 ADT Module User Manual Security Officer Menu*.

### **2.15 Background Processor Servers**

The Background Processor (BP) applications manage the storage and distribution of Clinical images both within the local area network (LAN) and remote storage within the VA wide area network (WAN). It is a requirement of the VistA Imaging system that the applications operate 24/7. The BP Queue Processor is responsible not only for file transmissions, but also network grooming by way of purges to ensure that adequate space is available for newly acquired images.

Since these tasks need to be started at some point in time, a (fully privileged) user will log in and start the Queue Processor. From that point on, the task will run and will continue to run until stopped by a system manager.

When the network connection between the BP Server(s) and the VistA Hospital Information System is interrupted, the BP Server(s) will recover from this situation, and will periodically attempt to reconnect (at 3 minute intervals). This reconnection will be attempted, without human interaction. A site can establish a special “service account” for which the access and verify codes will not expire.

Once the connection is re-established, the BP Server(s) will continue processing where it left off when the connection was interrupted.

## **2.16 References**

The following references for the VistA Imaging System are available through the VistA Imaging website [REDACTED](#) .

- Installation manuals, technical manual, user manuals, release notes, planning document, and DICOM conformance statements.
- References for Windows can be obtained from the Microsoft Corporation.

This page intentionally left blank.





# Appendix A VIX Security Information

This appendix contains security information specific to the VistA Imaging Exchange (VIX) service. Information in this appendix applies only to VA sites that have implemented a VIX.

The VIX is an optional VistA Imaging component used to exchange images between VA sites and the Department of Defense (DoD). In the case of VIX-supported VA-VA image sharing, a VIX can be at the requesting site only, the responding site only, or at both sites. In the case of VA-DoD image sharing, a VIX must be at the applicable VA site and must also be able to communicate with the CVIX (the centralized VistA Imaging Exchange service).

After a VA site implements a VIX, the VIX handles all local requests for remotely stored images (including Clinical Display remote image views). The VIX also serves copies of locally stored images to remote requestors (other VA sites and DoD clinicians via the CVIX).

The VIX and CVIX are described in detail in the *VIX Administrator's Guide*.

## A.1 Mail Groups, Alerts, and Bulletins

The VIX will automatically notify the VistA Imaging development group when it starts or restarts.

## A.2 Remote Systems

When the VIX processes data requests from a remote system, the VIX uses web services for metadata and HTTP 'get' commands for images and image-like artifacts.

Transmission frequency is dependent on the requesting party.

Data transfers can be synchronous or asynchronous depending on the nature of the request; the VIX uses HTTP response codes to acknowledge requests.

## A.3 Archiving

The VIX does not archive data. The VIX temporarily caches data and does not replace the existing Imaging archive.

## A.4 Contingency Planning

As defined for VistA Imaging in general (see section 2.4).

## A.5 Interfacing

The VIX incorporates the Laurel Bridge DCF DICOM Toolkit and the Aware JPEG2000 Toolkit. For details about these toolkits, refer to the *VIX Administrator's Guide*.

## A.6 Electronic Signatures

The VIX does not implement any new electronic signatures.

## A.7 Menus

The VIX does not have any security-related menu options on VistA.

## **A.8 Security Keys**

The MAG VIX ADMIN key gives the holder access to the web-based VIX transactions log. For more information, see the *VIX Administrator's Guide*.

## **A.9 File Security**

As defined for VistA Imaging in general (see section 2.9).

## **A.10 Software Pushes and the VIX**

The VIX server is an Imaging component, and Imaging components are FDA-regulated medical devices that cannot be modified by unauthorized parties in a production environment. Because software distribution/inventory management tools can install inappropriate or unapproved software without a local administrator's knowledge, sites must exclude the VIX server from automated update systems.

## **A.11 VistA Account for BHIE Framework Access**

With the release of the MAG\*3.0\*104 VIX, the VistA account needed to support DoD image accesses is no longer needed. Credentialing is now handled using Station 200 data and the CVIX (Centralized VistA Imaging Exchange) service.

Sites that have previously established a VistA account to support DoD image access may disable the account after updating their VIX to MAG\*3.0\*104.

## **A.12 References**

VIX documentation is available at [REDACTED](#).

## **A.13 Official Policies**

As defined for VistA Imaging in general (see section 2.16).

# Glossary

Architecture	The design of the components of a computer, network, or software system.
Archive	The long-term storage of data or images.
Audit trail	Record of activity on a particular file or computer.
BHIE	Bidirectional Health Information Exchange
DoD	Department of Defense
DICOM	Digital Imaging and Communications in Medicine. A medical imaging standard, DICOM is standard for Radiology equipment and is being adopted by the other members of the medical imaging community.
File	All the data that describes a document or image.
File protection	Techniques for preventing files from being erased.
File server	A machine where shared software and data files are stored.
Frame grabber	A device that translates a frame from a video image into a still digitized image.
High resolution	An image or a display that has more pixels per inch than a conventional display.
HDIG	Hybrid DICOM Image Gateway: An image gateway that combines the legacy DICOM Gateway and the new VISA Gateway. It implements DICOM services.
Image	The computerized representation of a picture, or graphic.
Image abstract	A “thumbnail” version of an image, which requires less computer processing resources to display than the actual image.
Image group	A group of images associated with a medical examination.
Image processing	The translation of an image into a digital computer language so that it may be manipulated in size, color, clarity, or to enhance portions of it.
Image resolution	The fineness or coarseness of an image.

## Glossary

Imaging system	Collection of units that work together to capture and recreate images.
JCAHO	Joint Commission on Accreditation of Health Organizations
Jukebox	A device that holds multiple optical discs and can swap them in and out of the drive as needed.
Login (Logon)	Procedure for gaining access to the system or program.
Multimedia	Combining more than one medium for the dissemination of information (e.g., text, graphics, full video motion, audio).
MUMPS	Massachusetts General Hospital Utility Multi-Programming System
NCAT	Neurocognitive Assessment Tool
Off-line	Something that is not available for access on the system.
On-line	Something that is available for access on the system.
Resolution	Measure of output quality (dpi—dots per inch) or halftone quality (lpi—lines per inch).
Retrieval	The ability to search for, select, and display an image or other data from storage.
RGB	Red, Green, Blue. The colors used in varying combinations and intensities on monitors, TV screens, and other color displays.
RPC	Remote Procedure Call
Server	A computer that is dedicated to a task (generally data storage).
Storage media	The physical device onto which data is recorded.
User preferences	The preferences that each user sets in the User Preferences window that control the circumstances and ways in which the Imaging package displays images.
VistA	<u>V</u> eterans Health <u>I</u> nformation <u>S</u> ystem <u>T</u> echnology <u>A</u> rchitecture. VistA replaces DHCP.