IMAGING SYSTEM
SECURITY GUIDE

Version 3.0 - Revision 3

September 2004

Department of Veterans Affairs
System Design and Development
V*IST***A** Imaging

Preface

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

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

Revision History

5 November 2003	Updated Security Features section
16 April 2004	Updated information for Patch 11
27 April 2004	Changed “Revision 1” references” to “Revision 2”
23 April 2004	Updated information for Patch 8

Table of Contents

Preface ..... **i**

Chapter 1 Security Management **1**

1.1 Introduction 1
1.2 Software Application and User Interface 1
1.3 Security Measures 1

Chapter 2 Security Features **3**

2.1 Mail Group and Alerts 3
2.2 Remote Systems 3
2.3 Archiving/Purging 3
2.4 Contingency Planning 4
2.4.1 Magnetic Servers 4
2.4.2 Optical Disk Jukebox 4
2.4.3 Network 4
2.4.4 Workstations used during medical care procedures 4
2.5 Interfacing 4
2.6 Electronic signature 6
2.7 Menus 6
2.8 Security Keys 7
2.9 File Security 9
2.10 Windows™ Security 14
2.11 Workstation Security 14
2.11.1 SMS Software and DICOM Gateways and Background Processors 15
2.11.2 SMS Software and VistARad 15
2.11.2.1 SMS(tm) Exclusion 16
2.11.2.1.1 Excluding Workstations from SMS 16
2.11.2.1.2 Removing SMS Client Software 16
2.12 Audit Trails 16
2.13 V*IST*A DICOM Gateway 17
2.13.1 Modality Worklist 17
2.13.2 Service Account 17
2.14 References 18

Glossary **19**

Chapter 1 Security Management

1.1 Introduction

The **V***IST***A** Imaging System captures, stores, and displays medical images. These medical images are part of a patient's medical record and are protected by the Federal Privacy Act. Images are stored on magnetic servers that are properly backed up on optical disk jukebox servers. The hardware configurations should include a tape backup unit that has the capacity to handle large volume. 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 of images. The Joint Commission of Accreditation of Health Organizations (JCAHO) has been very interested in image storage during their visits to the **V***IST***A** Imaging Test Sites and has recommended guidelines in these areas.

1.2 Software Application and User Interface

The **V***IST***A** Imaging System is a Windows application with a user interface written predominately with the Delphi development language. It makes calls to the Veterans Health Information Systems and Technology Architecture (**V***IST***A**) hospital information system using the Remote Procedure Call (RPC) Broker. The VistARad Diagnostic Display workstation component of **V***IST***A** Imaging also uses the RPC Broker to make calls to **V***IST***A.** VistARad was written using Visual Basic and C++.

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.

Please contact the **V***IST***A** Imaging Development Team with any requests or feedback on the user interface.

1.3 Security Measures

The **V***IST***A** Imaging servers are protected by several security measures. Security protection is built into the software for Windows XP and Windows 2000. The use of Windows 95, Windows 98 and Windows NT stations is no longer permitted. At the time of publication of this document, newer operating systems have not yet been approved for usage. If a site has a requirement to use other than approved operating systems, they should contact the **V***IST***A** Imaging Support team to determine if the site can be configured for secure access to images.

Chapter 2 Security Features

2.1 Mail Group and Alerts

The MAG SERVER mail group is created during the **V*IST*A** 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 user that performs the **V*IST*A** Imaging installation, as well as 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

The **V*IST*A** Imaging System currently does not transmit data to any remote system or database for storage. Users may log into a remote system on the VA wide area network if they have an access and verify code supplied by the remote medical facility. In this case, security software on the workstation is activated. No encryption is used for the images or data. Verification of the image integrity is done visually by the user.

2.3 Archiving/Purging

All images acquired using the **V*IST*A** 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 to a tape or optical media regularly as specified by site system administrator. A backup should also be made of the jukebox SQL database or of the OTG Extended Drive (OTG Disk Extender; check with Support and/or Legato for the most current release). The tapes and/or optical media copies should be moved to an off site location.

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

Images are periodically purged from the magnetic server to free disk space. Images on the jukebox are never deleted. Purging is controlled by the *last access date* of the image file. It is compared with the purge site parameters to determine if the file is a candidate for purging. The fields in the site parameters file specify the number of days an image is kept on the server.

The image purge job checks for the existence of pointer-to-jukebox images before purging. The Image file (2005) contains all information about the images and their locations.

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 backup tapes or optical disk platters containing all images.

2.4 Contingency Planning

The **V*IST*A** 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 Servers

Image management software within the **V*IST*A** Imaging package allows a site with a magnetic server that is down, to indicate that it is "offline". When a server is set to "offline", all images will be retrieved directly from the jukebox. In many cases, sites have chosen to purchase "clustered" Microsoft Windows™ fileservers. This adds an extra layer of redundancy that allows the image shares to be accessible even if a server is down.

Access to image shares is restricted. Only the **V*IST*A** Imaging application has access to the share directories that contain patients' images. This is controlled by having the **V*IST*A** Imaging application supply its own privileged username and password to access the share when it stores or retrieves images.

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 **V*IST*A** 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 **V*IST*A**. Some DICOM image capture capability is available even under conditions where **V*IST*A**, 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

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

Product	Connection type	Used in (Medical Center) Service/Section	Restriction
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 captured on VCR	Video output (may need a frame grabber unit)	GI 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 cholangiopancreato-graphy (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

Product	Connection type	Used in (Medical Center) Service/Section	Restriction
Arthroscope	Video output	Orthopedics	Imaging procedure keys
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 floppy disk or serial port or TWAIN interface	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 **V*IST*A** Imaging System must first be tested by the **V*IST*A** Imaging development team.

2.6 Electronic signature

The **V*IST*A** Imaging System requires an electronic signature when an image is copied or printed from an 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.

2.7 Menus

There are several options that are of particular interest to information security officers. On the Background Processor, there is a system manager menu that allows the user to indicate a device is offline in case of device failure. On the Background Processor, there is also an option that allows the system manager to purge images from the magnetic servers. On the workstations, there is an 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 **V*IST*A** Imaging application. The following table summarizes security keys and their function.

Security Keys	Description
Note: If the 'CAPTURE KEYS' site parameter has been initialized, the following keys will need to be assigned appropriately.	
MAG CAPTURE	Allow Image capture of Images not relating to any Specialty. (i.e. 'NONE' on the Imaging Capture configuration window). Other keys are needed by the user to capture images to the Image File when they relate to a specialty (**V*IST*A** Medicine, Surgery, Radiology, Laboratory, or TIU document).
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

Security Keys	Description
	workstation.
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 CP	Allows an imaging user to capture Clinical Procedure images from the Imaging Capture workstation.
MAGCAP ADMIN	User can capture images of 'Admin Document' specialty from the Imaging Capture workstation.
MAGDISP ADMIN	User can display images captured under the Admin Document specialty. This key should be assigned to one or two designated users.
MAGDISP CLIN	Allows Imaging User to View Clinical Images/Documents.
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 SEE BAD IMAGES	User can view images in VistARad that are associated with an exam that has failed the "Patient Safety" database checks. *This key should be assigned to one or two designated users, to aid in researching integrity problems.*
Note: Please be cautious when assigning the following keys; the keys are intended for Imaging Support personnel. Review the descriptions before assigning these keys.	
MAG PREFETCH	This key allows a user to 'PreFetch' or Queue all images for a patient. The means that all images for a patient that are on the JukeBox will be copied from the jukebox to the magnetic server cache.
MAG DELETE	This key allows the holder to delete images from File 2005. Pointers in parent packages such as Medicine, Surgery, Lab, Radiology, and TIU will also be deleted.
MAG SYSTEM	Given to person(s) managing **V***IST***A** Imaging Systems. Required to modify site parameters via the Background Processor or to modify workstation parameters via the MAGSYS application.
MAG RAD	This key allows user to edit the CT Presets in the Clinical

Security Keys	Description
SETTINGS	Imaging Display Radiology Viewer window.

2.9 File Security

The following table lists all files associated with the **V*IST*A** Imaging application and the default VA FileMan security for each.

File Security							
File Number	**File Name**	**DD Access**	**RD Access**	**WR Access**	**DEL Access**	**LAYGO Access**	**Audit Access**
2005	IMAGE	@	@	@	@	@	
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	@	@	@	@	@	
2005.81	MAG DESCRIPTIVE CATEGORIES	@	@	@	@	@	
2005.82	IMAGE INDEX FOR CLASS	@	@	@	@	@	@
2005.83	IMAGE INDEX FOR TYPES	@	@	@	@	@	@
2005.84	IMAGE INDEX FOR SPECIALTY/SUBSPECIALTY	@	@	@	@	@	@

File Security							
File Number	**File Name**	**DD Access**	**RD Access**	**WR Access**	**DEL Access**	**LAYGO Access**	**Audit Access**
2005.85	IMAGE INDEX FOR PROCEDURE/EVENT	@	@	@	@	@	@
2005.86	IMAGE ACTIONS	@	@	@	@	@	@
2005.87	IMAGE LIST FILTERS	@	@	@	@	@	@
2005.872	DICOM INDEX MAPPING	@	@	@	@	@	@
2006.03	IMAGE BACKGROUND QUEUE	@	@	@	@	@	
2006.031	IMAGE BACKGROUND QUEUE POINTER	@	@	@	@	@	
2006.032	JUKEBOX	@	@	@	@	@	
2006.033	OFFLINE IMAGES	@	@	@	@	@	
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	@	@	@	@	@	
2006.17	MUSE VERSIONS	@	@	@	@	@	@
2006.18	IMAGING USER PREFERENCE	@	@	@	@	@	
2006.19	IMAGING USERS	@	@	@	@	@	

File Security							
File Number	**File Name**	**DD Access**	**RD Access**	**WR Access**	**DEL Access**	**LAYGO Access**	**Audit Access**
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	@	@	@	@	@	@
2006.54	PDU TYPE	@	@	@	@	@	@
2006.55	DICOM WORKLIST PATIENT	@	@	@	@	@	@
2006.56	DICOM WORKLIST STUDY	@	@	@	@	@	@
2006.563	DICOM GATEWAY PARAMETER	@	@	@	@	@	@
2006.564	DICOM QUEUE	@	@	@	@	@	@
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	@	@	@	@	@	@

File Security							
File Number	**File Name**	**DD Access**	**RD Access**	**WR Access**	**DEL Access**	**LAYGO Access**	**Audit Access**
2006.5719	DICOM ERROR LOG	@	@	@	@	@	@
2006.572	EXAMINATION COMPLETE	@	@	@	@	@	@
2006.573	GE PACS QUERY/RETRIEVE	@	@	@	@	@	@
2006.574	DICOM IMAGE OUTPUT	@	@	@	@	@	@
2006.575	DICOM FAILED IMAGES	@	@	@	@	@	@
2006.5761	DICOM MESSAGE STATISTISTICS	@	@	@	@	@	@
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	@	@	@	@	@	@
2006.583	MODALITY WORKLIST DICTIONARY	@	@	@	@	@	@
2006.5831	DICOM HEALTHCARE PROVIDER SERVICE	@	@	@	@	@	@

File Security							
File Number	**File Name**	**DD Access**	**RD Access**	**WR Access**	**DEL Access**	**LAYGO Access**	**Audit Access**
2006.5839	DICOM GMRC TEMP LIST	@	@	@	@	@	@
2006.584	TCP/IP PROVIDER PORT LIST	@	@	@	@	@	@
2006.585	USER APPLICATION	@	@	@	@	@	@
2006.586	PROVIDER APPLICATION	@	@	@	@	@	@
2006.587	DICOM TRANSMIT DESTINATION	@	@	@	@	@	@
2006.589	IMAGING SERVICE DICTIONARY	@	@	@	@	@	@
2006.59	ROUTING RULE	@	@	@	@	@	@
2006.5906	ROUTE LOAD BALANCE	@	@	@	@	@	@
2006.592	DICOM UNDEFINED MODALITIES	@	@	@	@	@	@
2006.593	DICOM INCOMPLETE IMAGE	@	@	@	@	@	@
2006.596	ACTION QUEUE STATUS	@	@	@	@	@	@
2006.598	DICOM ERROR MESSAGE QUEUE	@	@	@	@	@	@
2006.599	DICOM Error Log	@	@	@	@	@	@
2006.61	MAG RAD EXAM STATUS CATEGORIES						
2006.63	MAG RAD LIST DATA ELEMENTS	@	@	@	@	@	@

File Security							
File Number	**File Name**	**DD Access**	**RD Access**	**WR Access**	**DEL Access**	**LAYGO Access**	**Audit Access**
2006.631	MAG RAD LISTS DEFINITION	@	@	@	@		@
2006.634	MAGJ ZLIST SEARCH	@	@	@	@	@	@
2006.65	MAG RAD PRIOR EXAMS LOGIC	@	@	@	@	@	@
2006.69	MAG VISTARAD SITE PARAMETERS	@	@	@	@	@	@
2006.79	DICOM ROUTINE COPY	@	@	@	@	@	@
2006.8	BP WORKSTATIONS	@	@	@	@	@	
2006.81	IMAGING WINDOWS WORKSTATIONS	@	@	@	@	@	@
2006.82	IMAGING WINDOWS SESSIONS	@	@	@	@	@	
2006.83	DICOM WORKSTATION	@	@	@	@	@	@
2006.95	IMAGE ACCESS LOG	@	@	@	@	@	@
2006.96	IMAGE INDEX CONVERSION	@	@	@	@	@	@

2.10 Windows™ Security

Windows™ provides security through the use of user profiles, policies/rights, directory/share permissions and domain configuration. **V***IST***A** Imaging file servers should be configured as a member server of the site resource domain. The **V***IST***A** Imaging Installation manual 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 Guideline and/or policies.

Restricting access to the **V*IST*A** 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. The VA recommends McAfee VirusScan by Network Associates for virus detection software on workstations and Network Associates NetShield virus protection software for Microsoft Windows servers. Additional information can be obtained on the VA HISS website located at https://vaww.ocis.va.gov. Commercial products are available for controlling access to system setup and files. Policies and profiles can be used to restrict access in an Microsoft Windows workstation environment. The BIOS of all **V*IST*A** Imaging workstations should be password protected.

2.11.1 SMS Software and 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 easiest way to make this work is to enable the feature called "Automatic Updates" in the Windows Control Panel, and to set this option to "Download the updates automatically and notify me when they are ready to be installed".

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 such as Microsoft's Systems Management Server™ (SMS) can be used to install inappropriate or unapproved software

without an administrator's knowledge, VistARad workstations cannot be SMS clients. This section explains how to exclude VistARad workstations from the definitions used by an SMS server, and how to remove SMS client software if it is inadvertently installed.

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).

2.11.2.1 SMS(tm) Exclusion

This section explains how to exclude VistARad workstations from the definitions used by Microsoft's Systems Management Server(tm) (SMS) SMS server, and explains how to remove SMS client software if it is inadvertently installed.

Note: Performing the steps below will not only exclude VistARad workstations from SMS "pushes", but will also exclude the workstations from automated inventorying.

2.11.2.1.1 Excluding Workstations from SMS

On the local SMS server, make the following changes to the Windows NT Registry:

1. Run regedit and navigate to the… HKEY_LOCAL_MACHINE\Software\Microsoft\SMS\Components key.
2. Open the SMS_Discovery_Data_Manager subkey.
3. Enter each computer name to be excluded as a separate line for ExcludeServers.

2.11.2.1.2 Removing SMS Client Software

If SMS client software has been installed on a VistARad workstation, perform the following steps:

1. Confirm that the workstation has been added to the ExcludeServers list as described above.
2. On the VistARad workstation, navigate to C:\Winnt\MS\SMS\Core\Bin.
3. Run the cliunins.exe application to remove the SMS client software.

2.12 Audit Trails

The **V***IST***A** Imaging software has several files that can be used to audit usage of **V***IST***A** Imaging workstations and access to Image files. The **V***IST***A** Imaging Windows Workstation File (2006.81) can be used to review the date and time the display or capture 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.

2.13 V*IST*A DICOM Gateway

A **V***IST***A** DICOM Gateway connects to a **V***IST***A** system using the RPC broker (MUMPS-to-MUMPS flavor). Access to the physical equipment of the DICOM Gateway itself is protected using the features of the WindowsTM 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 **V***IST***A** Hospital Information System for details that the DICOM Gateway does not store locally. Since "modalities" are lab-equipment that connect to a DICOM Gateway directly through TCP/IP, using the standard DICOM protocol, a DICOM Gateway has no concept of a "**V***IST***A** user context" for these Modality Worklist queries. In the exception that a DICOM Gateway needs to query its **V***IST***A** 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 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. Some time 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.

2.14 References

The following references for the **V***IST***A** Imaging System are available through the **V***IST***A** Imaging website (http://vaww.va.gov/imaging).

- Installation manuals, technical manual, user manuals, release notes, planning document, and DICOM compliance statements.

- References for Windows NT can be obtained from the Microsoft Corporation.

Glossary

Annotation	The ability to attach notes to images.
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.
Background processing	Simultaneous running of a "job" on a computer while working on another job. Examples would be printing one document while working on another, or the software may do automatic saves while you are working on something else. Background processing can also take place on a separate system connected to the network.
Brightness	The balance of light and dark shades in an image.
Composite video	TV signal that sends color, vertical and horizontal signals together.
Contrast	Range between the lightest and darkest tones in an image.
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.
Digital camera	A camera that transforms a picture into a system of numbers. The picture can then be manipulated pixel (dot) by pixel, and stored and transmitted as a file.
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.
Gray scale	The range of shades of black in an image. The more shades recognized by the device, the clearer and sharper the image will be.

High resolution	An image or a display that has more pixels per inch than a conventional display.
Hot spot	The single pixel that is activated by selection using a mouse, light pen, or other means.
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.
Imaging system	Collection of units that work together to capture and recreate images.
JCAHO	Joint Commission of Accreditation of Health Organizations
Jitter	The flickering of a displayed image.
Jukebox	A device that holds multiple optical discs and can swap them in and out of the drive as needed.
Level	The average pixel value (brightness) of a greyscale image that is displayed.
Login (Logon)	Procedure for gaining access to the system or program.
Mouse	Hand driven input and pointing device.
Multimedia	Combining more than one media for the dissemination of information (i.e., text, graphics, full video motion, audio).
MUMPS	Massachusetts General Hospital Utility Multi-Programming System
Off-line	Something that is not available for access on the system.
On-line	Something that is available for access on the system.

Optical disc	A direct access storage device that is written to and read by laser light. Optical discs can store more data per unit of surface area than can magnetic media. Many optical discs are Write Once Read Many (WORM).
Pan	To view different parts of the image that extend beyond the borders of the screen by moving the image.
Pixel	The individual dots that define a picture.
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
Scaling	Uniformly changing the size of an image.
Scanner	A device that converts a hardcopy image into machine-readable code.
Server	A computer that is dedicated to a task (generally data storage).
Storage media	The physical device onto which data is recorded.
TWAIN	An interface standard for scanners, cameras and other input devices.
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.
Video camera	Camera which records or senses full-motion video.
Video digitizer	A device that changes a video picture into a digital computer language.
V*IST*A	Veterans Health Information System Technology Architecture. **V*IST*A** replaces DHCP.

Window	A rectangular area on a screen (sometimes within another window) that contains controls, such as drop-down boxes, icons, scroll-bars and/or buttons. "Window" is also used to describe the range of pixel values that are displayed for a greyscale image. Adjusting the window is similar to adjusting contrast.
Workstation	A high-powered machine for a single user, typically used for computer-aided design or complex analysis.
WORM	Write Once Read Many. Once written to the disc, data is only available for reading and cannot be altered.
Zoom	To enlarge an image or a portion of an image.