VistA Imaging eXchange (VIX) VIX Enhancements

MAG*3.0*358

VIX Administrator's Guide

November 2024

Version 20.0

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

VistA Imaging eXchange (VIX) Administrator's Guide
November 2024

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 Internet:
http://www.va.gov/imaging

VA intranet: REDACTED

Revision History

NOTE: The revision history cycle begins once changes or enhancements are requested after the document has been baselined.

Date	Revision	Description	Author
11/04/2024	20.0	Initial draft for MAG*3.0*358.	VA IT VistA Imaging Technical team.

Date	Revision	Description	Author
01/02/2024	19.3	Updates for MAG*3.0*348 release date.	VA IT VistA Imaging Technical team.
12/01/2023	19.2	Updates for MAG*3.0*348 release date.	VA IT VistA Imaging Technical team.

Date	Revision	Description	Author
11/01/2023	19.1	Updates for MAG*3.0*358 release date.	VA IT VistA Imaging Technical team.
10/01/2023	19.0	Initial draft for MAG*3.0*348.	VA IT VistA Imaging Technical team.
05/01/2023	18.2	Updates for MAG*3.0*329 release date.	VA IT VistA Imaging Technical team.

Date	Revision	Description	Author
02/17/2023	18.1	Updates for Configure MUSE Functionality for MAG*3.0*329.	VA IT VistA Imaging Technical team.
02/03/2023	18.0	Initial draft for MAG*3.0*329.	VA IT VistA Imaging Technical team.
11/03/2022	17.1	Updates for MAG*3.0*303 to include the current supported SOP classes for the VIX Image Viewer.	VA IT VistA Imaging Technical team.
09/06/2022	17.0	Initial draft for MAG*3.0*303.	VA IT VistA Imaging Technical team.
06/01/2022	16.9	Updates for MAG*3.0*269 release date.	VA IT VistA Imaging Technical team.
05/24/2022	16.8	Additional updates for MAG*3.0*269 T5 to include updated VIX Tools appendix.	VA IT VistA Imaging Technical team.
05/09/2022	16.7	Additional updates for MAG*3.0*269 T5.	VA IT VistA Imaging Technical team.
04/20/2022	16.6	Additional updates for MAG*3.0*269 T4.	VA IT VistA Imaging Technical team.
03/07/2022	16.5	Additional updates for MAG*3.0*269 T3.	VA IT VistA Imaging Technical team.
02/19/2022	16.4	Additional updates for MAG*3.0*269 T3.	VA IT VistA Imaging Technical team.
02/10/2022	16.3	Updates for MAG*3.0*269 T3.	VA IT VistA Imaging Technical team.
12/20/2021	16.2	Updates for MAG*3.0*269 T2.	VA IT VistA Imaging Technical team.
11/30/2021	16.1	Updates for MAG*3.0*269.	VA IT VistA Imaging Technical team.
05/11/2021	16.0	Initial draft for MAG*3.0*269.	VA IT VistA Imaging Technical team.
04/06/2021	15.1	Updates for MAG*3.0*254 to include MUSE configuration section.	VA IT VistA Imaging Technical team.

Date	Revision	Description	Author
01/28/2021	15.0	Updates for MAG*3.0*254.	VA IT VistA Imaging Technical team.
10/11/2018	14.0	Additional updates for MAG*3.0*221.	REDACTED
09/09/2018	13.0	Additional updates for MAG*3.0*201.	REDACTED
04/04/2018	12.0	Updated for MAG*3.0*201.	REDACTED
03/03/2018	11.0	Updated for MAG*3.0*197.	REDACTED
02/02/2018	10.0	Additional updates for MAG*3.0*185.	REDACTED
11/14/2017	9.0	Updated for MAG*3.0*185 and incorporated comments from reviewers.	REDACTED
10/05/2017	8.0	Updated for P170 and 177, including VIX image viewer.	REDACTED
09/09/2013	7.0	Added section ROI VIX Operation and Configuration and Statistics.	REDACTED
08/01/2013	6.0	Renamed for joint rollup of MAG*3.0*34/116/118, MAG*3.0*119, MAG*3.0*127, and MAG*3.0*129.	REDACTED
07/15/2013	5.0	Updated for Imaging patch MAG*3.0*119. Updated sections on Related Information; The VIX Transaction Log; Caching of Metadata and Images.	REDACTED
09/14/2012	4.0	Updated for Imaging patch MAG*3.0*118. Minor grammar and wording corrections, added DICOM Importer Application Services, updated VIX Transaction log location, added new VIX Interfaces, and added new RPCs related to VIX/Importer II.	REDACTED
10/14/2011	3.0	Updated for Imaging patch MAG*3.0*104 to reflect expanded image sharing and involvement of CVIX. Reorganized to support future revisions.	REDACTED
01/20/2011	2.0	Updated for Imaging patch MAG*3.0*115. Clarified "site number" references to properly indicate station #. Added new VistARad-related information in descriptions of the 100 nodes in file #2006.95. Minor wording corrections.	REDACTED

Date	Revision	Description	Author
04/22/2010	1.0	Document created for Imaging patch MAG*3.0*83.	REDACTED

Table of Contents

1. Introduction 14
   1.1. Intended Audience 14
   1.2. Terms of Use 14
   1.3. Document Conventions 14
   1.4. Section Summary 15
   1.5. Related Information 15
   1.6. VIX Support 16
2. VIX Overview 17
   2.1. The VIX and Image Sharing 17
      2.1.1. VA-VA Image Sharing 18
      2.1.2. DoD-to-VA Image Sharing 20
      2.1.3. VA-to-DoD Image Sharing 21
      2.1.4. What is the CVIX? 22
         2.1.4.1. VIXes and Image Sharing at Multidivisional Sites 22
         2.1.4.2. Optional Direct Connection to a DoD Integrator 23
   2.2. DICOM Importer III Application Services 23
   2.3. Image Viewer 23
      2.3.1. Troubleshooting 24
      2.3.2. Windows Services 25
      2.3.3. Windows Processes 25
      2.3.4. Service Logging 25
      2.3.5. Viewer Image Caching 26
      2.3.6. Currently Supported Service-Object Pair (SOP) Classes 28
   2.4. VIX Implementation and Configuration 28
   2.5. VIX Dependencies 29
   2.6. VIX Operational Priority 29
      2.6.1. Standalone Server 29
   2.7. Security, Data Integrity, and Data Sensitivity Considerations 30
3. VIX General Operations 32
   3.1. VIX General Operations Overview 32
   3.2. The VIX and the VistA Site Service 32
   3.3. Using the VIX Transaction Log 33
      3.3.1. VIX Transaction Log Fields 34
      3.3.2. VIX Transaction Log Fields (Export Only) 39
      3.3.3. Log Collector Service 40
   3.4. VIX Data Retention and Purges 40
   3.5. VIX Startup and Shutdown 40
   3.6. Monitoring/Maintaining the VIX 41
      3.6.1. Checking the VIX Service 41

3.7. Monitoring/Maintaining the Image Viewer 42
3.7.1. Troubleshooting the Image Viewer 42
3.7.1.1. Analyzing Image Viewer Logs 43
3.8. The VIX and Backups 43
4. VIX Image Sharing 44
4.1. Remote Metadata Retrieval 44
4.1.1. Metadata Requests from Clinical Display 45
4.1.2. Metadata Requests from VistARad 45
4.2. Metadata Requests from the Zero-Footprint Image Viewer 46
4.3. Remote Image Retrieval 47
4.3.1. Image Quality and VIX Compression 48
4.3.2. Image Types vs. Image Formats 49
4.4. Caching of Metadata and Images 51
4.4.1. Cache Retention Periods 51
4.4.2. Cache Location 51
4.5. Image Sharing-related Logging 51
4.5.1. Logging on VistA 52
4.5.1.1. VIX-related Access Type Values 52
4.5.1.2. VIX-Related Additional Data Values 53
4.5.1.3. Example – RVVAVA Access Type 53
4.5.1.4. Example – RVVADOD Access Type 53
4.5.1.5. Example – RVDODVA Access Type 53
4.5.1.6. Example – VR-RVVAVA Access Type 53
4.5.2. Additional Client Logging 54
4.5.2.1. Clinical Display Message History Log 54
4.5.2.2. VistARad Logging of VIX Operations 54
4.6. Image Sharing and VIX Timeouts 55
4.7. Troubleshooting 56
5. ROI VIX Operation, Configuration and Statistics 59
5.1. How the VIX Processes ROI Requests 59
5.1.1. Processing ROI Disclosure Requests Immediately 59
5.1.2. Periodic Processing of ROI Disclosure Requests 59
5.1.3. Purging Completed Disclosures 60
5.1.4. Processing Disclosure Wait Time 60
5.1.5. ROI Periodic Processing Credentials 60
5.1.6. Alerts About Problems in the ROI Configuration 60
5.2. Getting Information About ROI Processing 61
5.2.1. Information the ROI Processing Status Page Provides 62
5.3. Modifying the ROI Processing and DICOM Query/Retrieve Parameters of the VIX 64
5.4. Changing User List for Get Invalid ROI Credentials Email Notifications 65

6. VIX Reference/Software Description 67
6.1. VIX Java Components 67
6.1.1. VIX Servlet Container 67
6.1.2. VIX Security Realms 67
6.1.3. VIX Interfaces 67
6.1.4. VIX Core 68
6.1.5. VIX Data Sources 68
6.1.6. Java Installation Locations 68
6.1.6.1. VIX folders on the System Drive 68
6.1.6.2. VIX Folders on the System Drive or a Shared Drive 69
6.1.7. Java Logs 69
6.2. VistA/M Information 70
6.2.1. Remote Procedure Calls (RPCs) Used by the VIX 70
6.2.2. Non-MAG RPCs used by the VIX 74
6.2.3. Database Information 75
6.2.4. Exported Menu Options 75
6.2.5. Security Keys 75
6.2.6. User Accounts 75
6.3. Other VIX Components 75
6.3.1. VIX Security Certificate 76
6.3.2. .NET 76
6.3.3. Apache Tomcat 76
6.3.4. Java Runtime Environment (JRE) 76
6.3.5. Laurel Bridge DCF Toolkit 76
6.3.6. Aware JPEG2000 Toolkit License 76
6.3.7. LibreOffice 77
7. Configure MUSE Functionality 78
8. Configure DICOM Service Class Provider (SCP) Functionality 83
8.1. Application Entity (AE) Titles Configuration 83
8.1.1. Laurel Bridge AE Titles Configuration on VIX 83
8.1.2. AE Titles Configuration on DICOM Service Class User (SCU) 85
8.2. Tomcat DICOM SCP Configuration 85
8.3. Laurel Bridge DICOM SCP Configuration 95
9. Configure ID Conversion 96
10. Appendix A: Image Sharing and DICOM Images 97
10.1. VA DICOM Images Provided to DoD 97
11. Appendix B: VIX Tools 99
12. Appendix C: VIX Utility Scripts 101
12.1. Run PowerShell as an Administrator 101

12.2. PowerShell Configuration 102
12.3. Restart Script 102
12.4. Tomcat Permissions Script 103
12.5. Purge Render Database (Cache Curator) Script 104
12.6. Java Management Extensions (JMX) Script 104
12.7. Delete VixCache Script 105
13. Appendix D: McAfee/Trellix Exclusions 106
14. Definitions, Acronyms, and Abbreviations 107

Table of Figures

Figure 1: Remote VA Images Flow Through a VIX 18
Figure 2: Commercial PACS VA Image Flow 19
Figure 3: DoD-to-VA Image Sharing 20
Figure 4: VA-to-DoD Image Sharing 21
Figure 5: Image Viewer Data and Control Flow Using eHMP (Example Application) 24
Figure 6: Windows Services Running 25
Figure 7: Execute Windows PowerShell 27
Figure 8: Check Apache Tomcat Service 42
Figure 9: VIX Viewer and Render Services 42
Figure 10: Release of Information (ROI) Status Page 61
Figure 11: Authentication Required 65
Figure 12: Configure Invalid Credentials Email 66
Figure 13: Sample MuseDataSource-1.0.Config File for One Server (MUSE ENABLED FOR JLV VIX Image Viewer) 79
Figure 14: BP Queue Processor 80
Figure 15: EKG Tab in Network Location Manager in BP Queue Processor 81
Figure 16: Network Location Properties in BP Queue Processor 82
Figure 17: AE Titles Configuration File (Template) 84
Figure 18: AE Titles Configuration File (Example) 84
Figure 19: AE Titles Configuration File w/ Multiple DICOM SCP clients (Example) 85
Figure 20: DICOM SCP Configuration File (Template) 87
Figure 21: ScpConfiguration Configuration File (Example) 88
Figure 22: DICOM SCP Configuration File (Example) 93
Figure 23: DICOM SCP Configuration File with Multiple DICOM SCU Calling AE Titles (Example) 94
Figure 24: DicomScpConfig Configuration File (Template) 95
Figure 25: IdConversionConfiguration.config file (Template) 96
Figure 26: Login Page 100
Figure 27: VIX Tools Page 100
Figure 28: Execute Windows PowerShell 101
Figure 29: PowerShell Script Error 102
Figure 30: Windows PowerShell Restart Script 103

Table of Tables

Table 1: Typographic Conventions 15
Table 2: Image/Artifact Category Notes for DoD-to-VA Image Sharing 20
Table 3: Supported SOP Classes 28
Table 4: Systems for VIX Operation 29
Table 5: VIX Transaction Log Fields 35
Table 6: VIX Transaction Log Fields (Export Only) 39
Table 7: VIX Daily Purge Process 40
Table 8: VIX Service Response to Restart or Interruption 41
Table 9: Remote Metadata Retrieval for Different Remote Site Types 44
Table 10: Clinical Display Metadata Requests Summary 45
Table 11: VistARad Metadata Requests Summary 46
Table 12: Zero-Footprint Image Viewer Metadata Requests Summary 46
Table 13: Remote Image Retrieval for Different Remote Site Types 47
Table 14: VIX Compression Logic for Request Type 48
Table 15: Image Formats VIX can Return Based on Image Type 50
Table 16: Retention Periods by Data Type 51
Table 17: Access Type Values 52
Table 18: Additional Data Fields for Access Type 53
Table 19: VIX Connection Timeout based on Remote System Type 55
Table 20: Troubleshooting VIX-related Image Sharing Problems by Symptoms 56
Table 21: ROI Processing Information 62
Table 22: VIX Interfaces Description 67
Table 23: VIX Data Sources Description 68
Table 24: MAG RPCs used by the VIX 70
Table 25: Non-MAG RPCs used by the VIX 74
Table 26: DICOM Modality Types Provided to DoD 97
Table 27: List of URLs 99
Table 28: Definitions, Acronyms, and Abbreviations 107

1. Introduction

This document explains how to maintain and administer the VistA Imaging eXchange (VIX) service.

The VIX is used to facilitate data sharing and exchange across organizational and functional boundaries. Currently, the VIX's primary purpose is to support image sharing between VA (Department of Veterans Affairs) medical facilities and between VA and the Department of Defense (DoD) medical facilities. It is anticipated that the VIX's role will expand to support data sharing and exchange within a facility and between facilities.

The VIX hosts a zero-footprint viewer providing services to consuming application, chiefly eHMP and Joint Legacy Viewer / Joint Longitudinal Viewer (JLV). With these changes, the VIX is a critical component as it provides access not only to remote but local images as well. Maintenance of this component is critical to the clinical operation at the site level. The operation of a site VIX also affects access to the portion of the patient record stored at the site.

This document assumes that the VIX is installed and configured. For information about VIX system requirements, installation, and configuration, see the VIX Installation Guide.

1.1. Intended Audience

This document is intended for VA staff responsible for managing a local VIX.

One part of this document, *Image Sharing Related Logging*, may also be of interest to VA Imaging Coordinators at non-VIX sites. This section describes how remote VIXes log access to locally stored images.

This document presumes a working knowledge of the VistA environment, VistA Imaging components and workflow, Windows server administration, and Windows cluster administration.

1.2. Terms of Use

The VIX is a component of VistA Imaging and is regulated as a medical device by the Food and Drug Administration (FDA). Use of the VIX is subject to the following provisions:

- Federal law restricts this device to use by or on the order of either a licensed practitioner or persons lawfully engaged in the manufacture or distribution of the product.
- The FDA classifies VistA Imaging and the VIX (as a component of VistA Imaging) as a medical device. Unauthorized modifications to VistA Imaging, including the VIX, such as installing unapproved software, will adulterate the medical device. The use of an adulterated medical device violates US federal law (21CFR820).
- 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 such a system.

1.3. Document Conventions

This document uses the following typographic conventions (Table 1).

Table 1: Typographic Conventions

Symbol/Typeface	Meaning/Use	Example
Bold	User input, selection, or menu item (such as a button or field element) on the Graphical User Interface (GUI).	Click **Finish**. Choose **Open** from the **File** menu. Type the user account name in the **Name** field.
Monospaced font (typically in a box) (Bold indicates user input or selection).	Command-line sample or output (such as character-based screen captures and computer source code), menus, file names.	Navigate to the \Docs\Imaging_Docs_Latest folder.
Italics	Emphasis, reference to section in the document or another document, or a variable.	For more information, see the Vista Imaging DICOM Gateway Installation Guide.
Square brackets, monospace or italics.	Variable, placeholder, VistA menu, XML element.	Access the Kernel Installation and Distribution System Menu [XPD MAIN]. ;3.0;IMAGING;**[Patch List]**;Mar 19, 2002;Build 1989;Feb 21, 2011 Set the access code for the account with VistA credentials (inside <accessCode>).

1.4. Section Summary

- **VIX Overview** – A high-level overview of VIX capabilities and key concepts.
- **VIX General Operations** – A description of day-to-day activities that relate to all VIX capabilities.
- **VIX Image Sharing** – A description of VIX operations specific to image sharing.
- **ROI VIX Operation, Configuration and Statistics** – A description of how the VIX processes Release of Information (ROI) requests.
- **VIX Reference/Software Description** – VIX technical information.
- **Appendices** – Supplemental and supporting material.

1.5. Related Information

Additional documents containing information about the VIX can be found on the VistA Imaging SharePoint site here: https://www.va.gov/vdl/application.asp?appid=105

1.6. VIX Support

If you encounter any problems with the VIX, use the information in the *Troubleshooting* section to try to determine the possible cause of the problem. If problems persist, log a Remedy ticket or call the National Service Desk at REDACTED.

2. VIX Overview

This chapter provides a high-level summary of what the VIX does and how it does it. This chapter covers:

- *The VIX and Image Sharing*
- *DICOM Importer III Application Services*
- *Image Viewer*
- *VIX Implementation and Configuration*
- *VIX Dependencies*
- *Standalone Server*
- *Security, Data Integrity, and Data Sensitivity Considerations*

2.1. The VIX and Image Sharing

The VIX implements image sharing between the Department of Veterans Affairs (VA) and the participating Department of Defense (DoD) medical facilities. The VIX also supports and extends VA-to-VA remote image sharing for Clinical Display and VistARad.

The VIX delivers these capabilities in such a way that:

- Clinicians can locate and review images from all VA and participating DoD facilities without manually logging into the remote site.
- Wide Area Network (WAN) traffic is minimized whenever possible using the VIX's compression and caching strategies.
- The VIX handles the burden of connection management and data retrieval rather than client applications such as Clinical Display and VistARad.

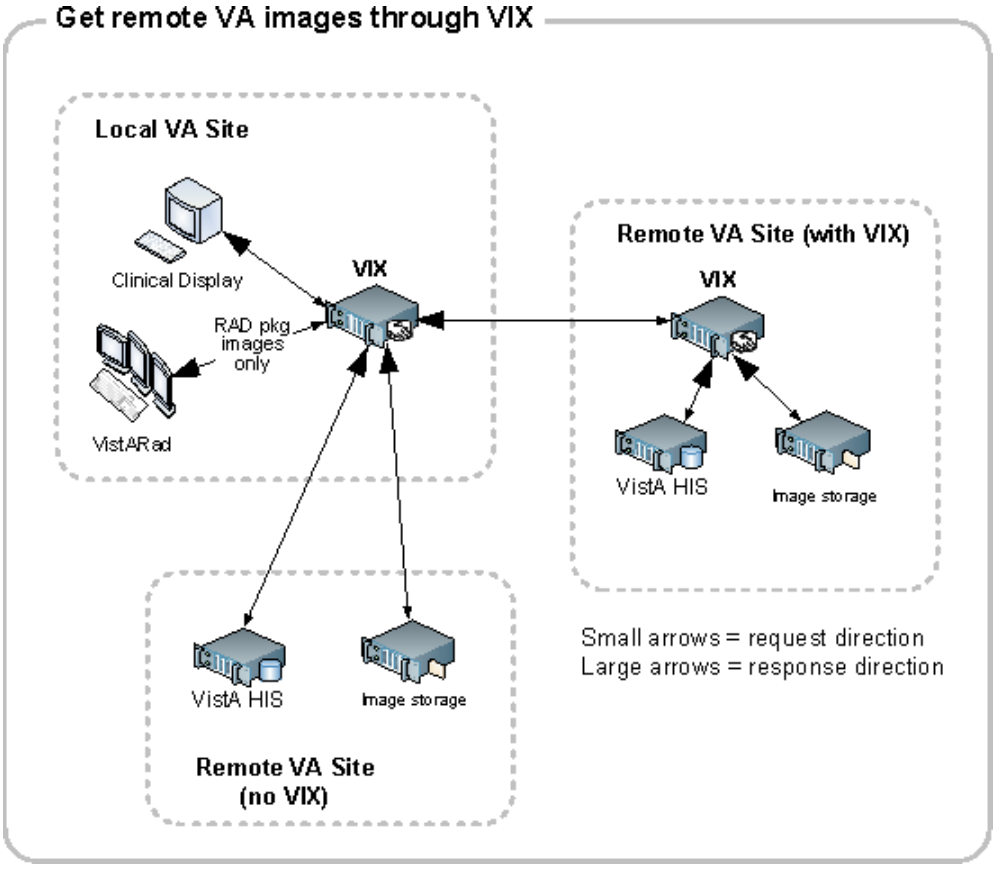
At sites where a VIX is implemented, the VIX's involvement in data retrieval begins when a clinician selects a patient who has been seen at the local hospital as well as at one or more remote hospitals. The clinician's client software (Clinical Display or VistARad) pulls information about locally stored images from the local VistA system, while information about remote images is pulled from remote sites via VIX. The clinician uses this information to decide what images to display. Local images are retrieved directly from the local hospital, while remote images are retrieved via the VIX. From the clinician's perspective, accessing an image works the same way, regardless if the image is from local storage, a remote VA site, or from the DoD.

The following sections outline how a VIX fits in when accessing remote images.

2.1.1. VA-VA Image Sharing

Figure 1 shows how remote VA images and related metadata flow through a VIX.

Figure 1: Remote VA Images Flow Through a VIX

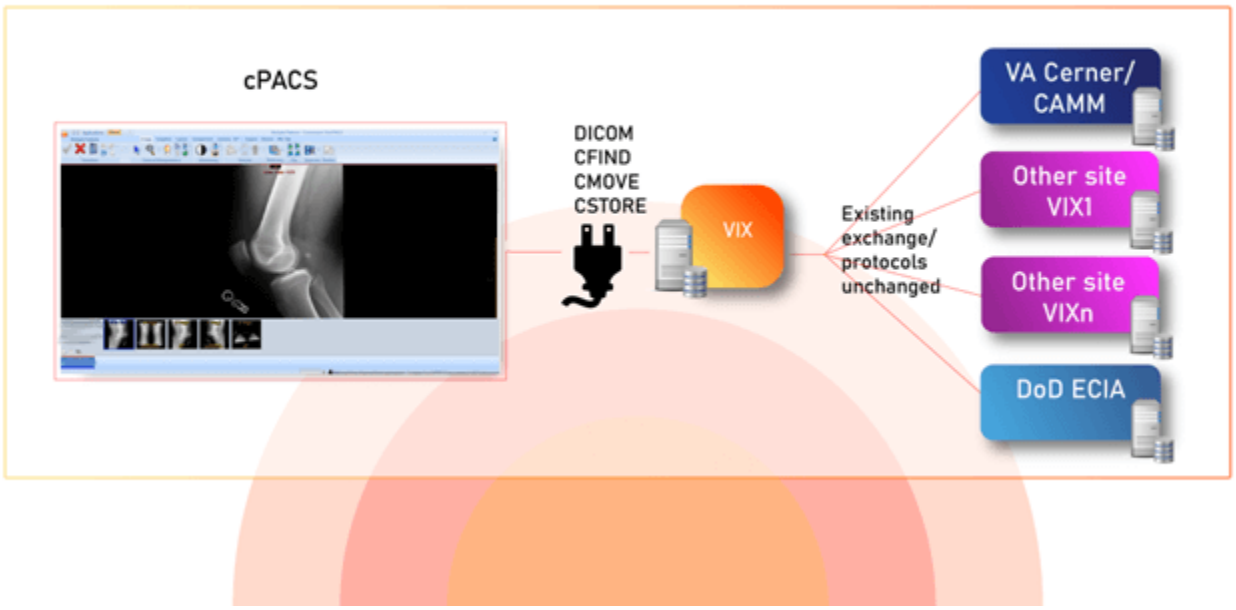


When the VIX is used for VA-to-VA image sharing, the VIX can handle anything stored in VistA Imaging. This includes radiology images, clinical images of all types, scanned documents, video, and audio.

NOTE: If a local VIX is not implemented, VA-VA image sharing is still available (at a reduced performance) to local Clinical Display and zero-footprint Image Viewer users, but not to VistARad users.

Commercial picture archiving and communication system (PACS) (Figure 2) equipment or other query retrieve devices communicate with the local VIX. The local VIX then communicates with the other VistA site VIX systems, just as the VIX system currently does for Clinical Display, VistARad, and the VIX Viewer. In this way, Commercial PAC equipment can import before local and remote images into the viewer.

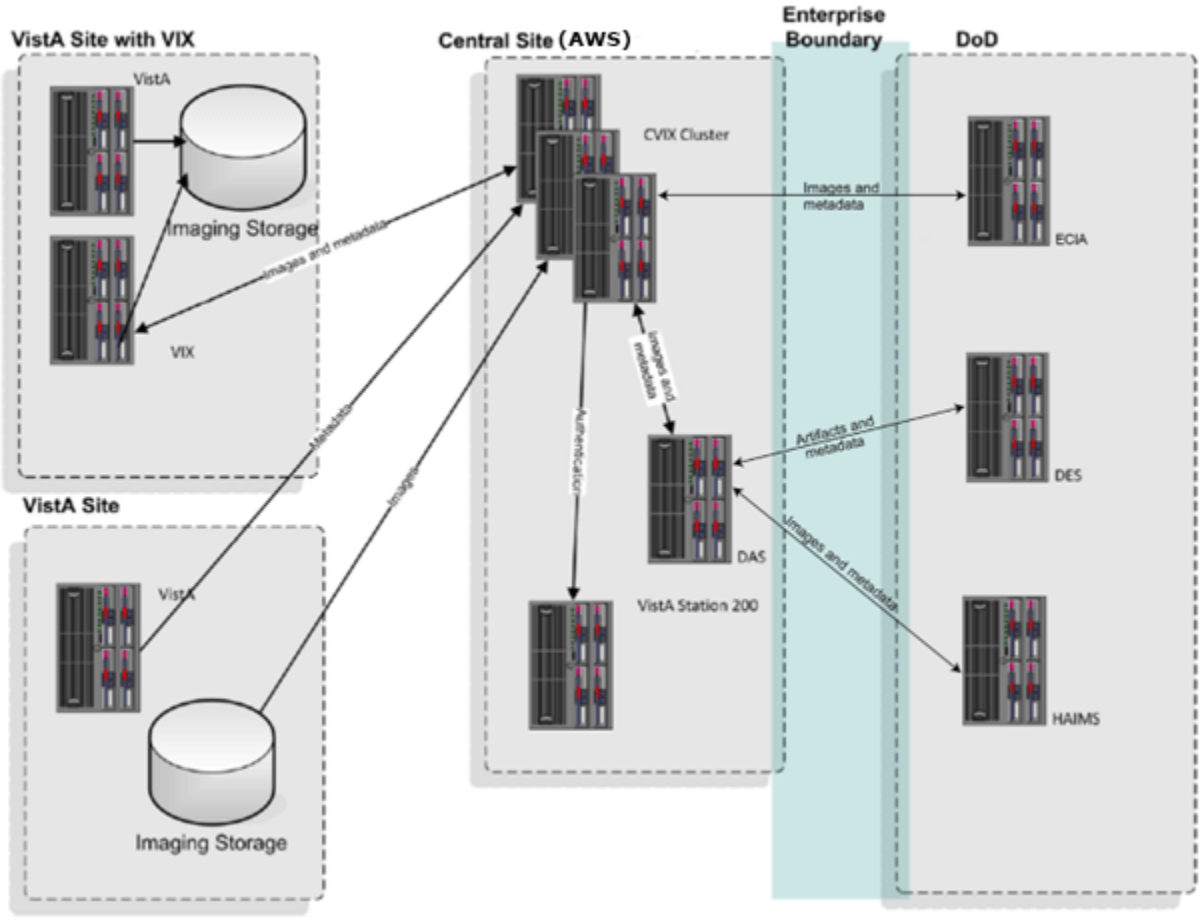
Figure 2: Commercial PACS VA Image Flow



2.1.2. DoD-to-VA Image Sharing

When a local VIX is used to retrieve DoD images for shared VA/DoD patients, the local VIX sends clinicians' requests to the Centralized VistA Image Exchange (CVIX). The CVIX, in turn, handles the communication with the various sources of DoD images (Figure 3).

Figure 3: DoD-to-VA Image Sharing



VA clinicians can access the types of DoD images in Table 2 for shared patients if a local VIX is implemented and if the appropriate DoD image sources are online.

NOTE: There is an ability to switch between HAIMS (Health Artifact and Image Management Solution) and ECIA (Enterprise Clinical Imaging Archive) for DoD images.

Table 2: Image/Artifact Category Notes for DoD-to-VA Image Sharing

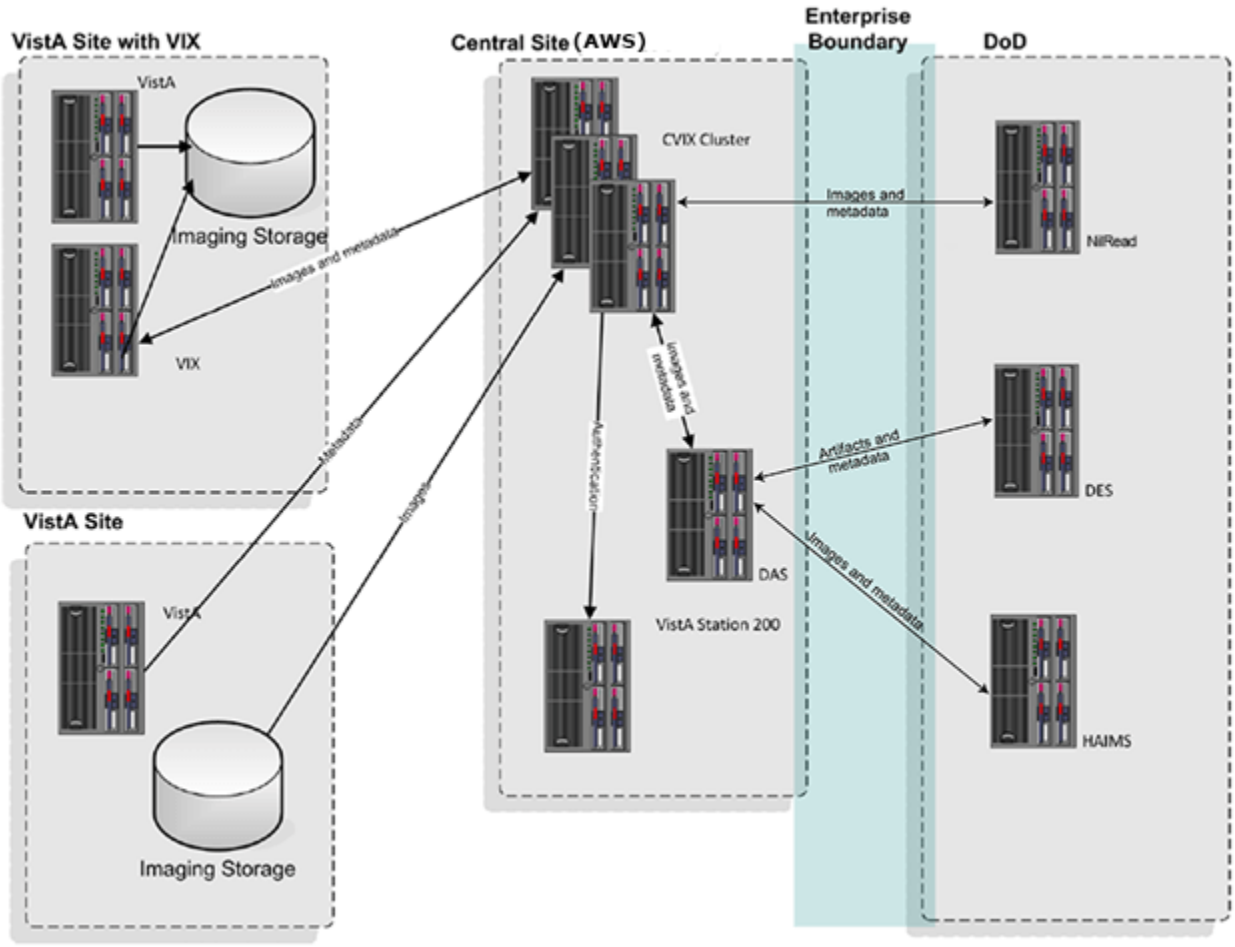
Image/Artifact Category	Notes
DoD DICOM images	Available from participating DoD facilities via the ECIA, which is through the CVIX. **NOTE:** There are a limited number of non-image DICOM objects that are not provided. For more information, see *DoD DICOM Object Filtering.*

Image/Artifact Category	Notes
DoD artifacts (non-radiology medical images, scanned documents, etc.)	Available if Data Exchange Service (DES) servers are online, accessible through DAS (Data Access Service), and if DAS servers are capable of communicating with the CVIX.

2.1.3. VA-to-DoD Image Sharing

When a VA site implements a VIX, that VIX also allows DoD clinicians to access locally stored Digital Imaging and Communications in Medicine (DICOM) images for VA/DoD shared patients (Figure 4). For additional details about the types of images involved, see *VA DICOM Images Provided to DoD.*

Figure 4: VA-to-DoD Image Sharing



NOTE: DoD clinician image access requests are logged in the local VistA system.

NOTE: DoD clinicians can access locally stored non-DICOM medical images and scanned documents using the CVIX alone as long as the patient in question is a shared VA/DoD patient. A local VIX is not required.

NOTE: There is an ability to switch between HAIMS and NilRead™ or other query retrieve devices for DoD images.

2.1.4. What is the CVIX?

The CVIX service functions as a VIX for the entire DoD. It:

- Provides a single point for VA access to DoD images. Among other things, this means that local site VIXes do not have to be modified if there is a change in how DoD image sources request or provide data; only the CVIX is impacted.
- Provides the portal used by all DoD clinicians to request all VA images. In this role, the CVIX uses the VistA system at Station 200 to provide VA treating facility information for shared patients and temporary VA credentials for DoD clinicians.

The CVIX server also:

- Hosts the VistA Site Service
- Hosts the VIX Log Collector

2.1.4.1. VIXes and Image Sharing at Multidivisional Sites

VIX implementation at a multidivisional site can be handled in two ways:

- A multidivisional site can implement a single VIX at a primary division to serve all divisions.
- A multidivisional site can implement a VIX at the primary division and one or more subdivisions.

When a local clinician at a VIX-equipped multidivisional site requests remote metadata and images, the closest VIX is used. For example:

- If the division where the clinician is logged into has a VIX, that VIX is used in preference to any other VIXes that may be present.
- If the division where the clinician logged into does not have a VIX, the VIX at the primary division is used.

When clinicians outside of the multidivisional site, request local metadata and images from a VIX-equipped multidivisional site:

- Metadata requests are always handled by the VIX at the primary division because that VIX is local to the applicable VistA database.
- If a subdivision has local image storage and a VIX, the VIX at that subdivision provides the image to the remote requestor.

If a subdivision has local image storage but does not have a VIX, the VIX at the primary division provides the image to the remote requestor.

Performance considerations aside, these distinctions free clinicians from having to determine which VIX to use.

NOTE: Images from different subdivisions within a multidivisional site are considered local images by client software (such as Clinical Display and VistARad). Because of this, the clients request these images directly and not via the VIX.

2.1.4.2. Optional Direct Connection to a DoD Integrator

If a participating DoD facility shares a direct network connection with a VA site that has a VIX, the DoD facility's integrator and the VA's VIX can be configured to communicate directly for DICOM image transfers. This allows the images to be accessed at LAN speeds rather than WAN speeds.

NOTE: This capability is used for DICOM images only.

For more information about this option, contact the VistA Imaging development group at REDACTED .

2.2. DICOM Importer III Application Services

The Importer III is a distributed application for allowing users to import outside studies from CD, DVD, or network sources and process and reconcile studies that have entered the DICOM correct workflow. It is composed of a client application that uses the VIX as an application server, and a server component running on the site's HDIGs that picks up reconciled studies and work items for asynchronous processing.

In its role as the Importer III's application server, the VIX provides the following broad categories of functionality:

- User services including login, user key retrieval, and related functions.
- Patient services including search, patient sensitivity logging, and related functions.
- Storage services including retrieving the current read and write locations for the image shares.
- DICOM Importer application services, including
    - Validation of application version compatibility
    - Importer work item creation, updating, retrieval, and deletion.
    - Decoding of DICOMDIR files
    - Inspecting images from studies to determine whether or not they already exist in VistA.
    - Order retrieval for a specified patient
    - Metadata retrieval for Ordering Providers, Ordering Locations, Procedures, and Procedure Modifiers
    - Searching for and generating reports

2.3. Image Viewer

MAG*3.0*177 introduced new VIX services to support a zero-footprint web-based image viewer. The "Viewer" web application which is also known as the:

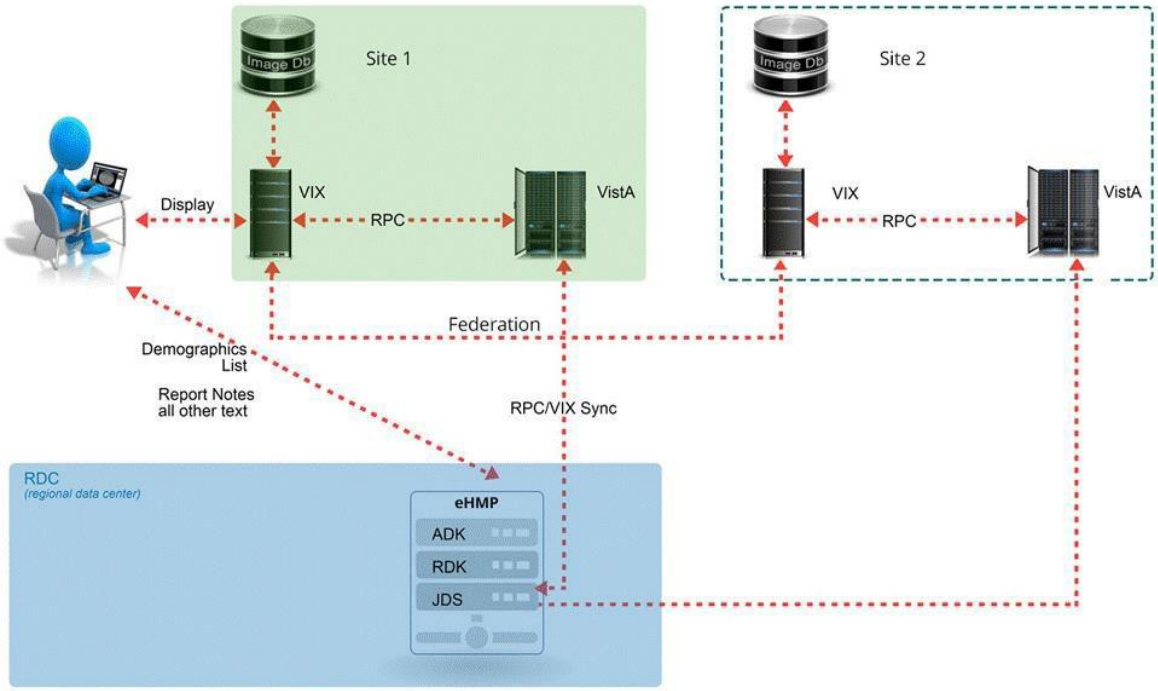
- CVIX Viewer
- VIX Viewer

- Enhanced Image Viewer
- Image Viewer
- VistA Imaging Viewer

The zero-footprint image viewer is not a standalone application. It is a service for external applications to integrate with their apps for viewing images stored in VistA Imaging or images in other enterprises accessible through VistA Imaging (i.e. DoD).

The viewing of images to the zero-footprint viewer redirects to the server from the user's local VIX. This arrangement (Figure 5) keeps image traffic local to the facility as much as possible (for better performance). All image access using the zero-footprint image viewer, whether local or remote, goes through the VIX and utilizes these services.

Figure 5: Image Viewer Data and Control Flow Using eHMP (Example Application)



2.3.1. Troubleshooting

It is important to ensure the viewer and render Windows services are up and running as they are critical for viewing images while using the zero-footprint image viewer.

All VIX services prior to patch MAG*3.0*170 run under the Apache Tomcat Windows service. After that patch, the services run under their own separate Windows services. See details below to verify all VIX Windows services and processes are operational.

It is also important to verify that the VIX is sized appropriately and the usage of resources such as disk drive, Central Processing Unit (CPU), and memory are not exceeded.

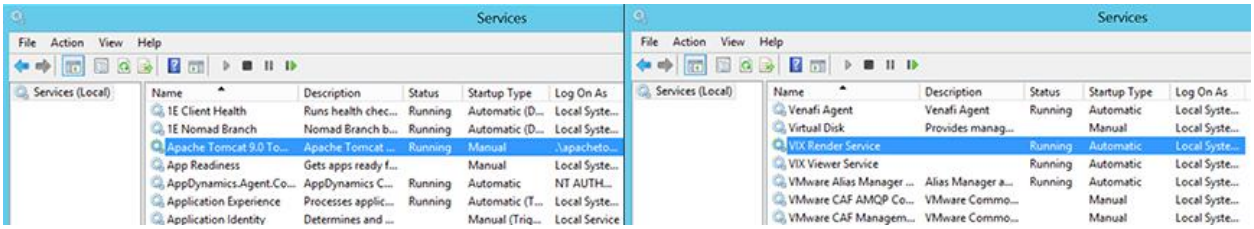
2.3.2. Windows Services

Ensure that Apache Tomcat, VIX Render Service, and VIX Viewer Service are running and operational (Figure 6).

1. **VIX Viewer Service**: The viewer service is the only public interface used by consuming applications such as eHMP and JLV. It is used to fetch image related metadata to view images in a web browser. The zero-footprint image viewer is hosted and served out by the Viewer service.
2. **VIX Render Service**: The Render service is not a public interface; it is an internal service to pre-process images so they can be displayed efficiently in a web image viewing application. The Render service is used by the Viewer service. The Render cache is a cache of pre-processed images which allows subsequent image accesses through the viewer to be much quicker because there is no need to pre-process these images.

NOTE: The Apache Tomcat version may vary depending on which patch level is installed.

Figure 6: Windows Services Running



2.3.3. Windows Processes

Verify that the VIX Viewer and Render processes are running in the Windows Task Manager.

1. Launch the Windows Task Manager
2. Look for the following processes:
    a. VIX.Viewer.Service
    b. VIX.Render.Service
    c. Hydra.IX.Processer (x10) – the number of worker processes configurable on the VIX; the actual amount may be more or less.
    d. Hydra.VistA.Worker (x5) - the number of worker processes configurable on the VIX; the actual amount may be more or less.
3. If any of these processes are not running, restart the Viewer and Render services.

NOTE: It can take up to a minute for all Hydra.IX.Processor processes to start.

2.3.4. Service Logging

If all related VIX Windows services and processes are running, the service logs can be checked for errors and other information. By default, the logging level for the services is set to "Warn".

This means that warnings and errors can appear in the log files. If a more granular level of logging is needed for troubleshooting, you can change the *LogLevel* from "Warn" to either "Debug" or "Trace" in each of the config files listed below:

- **VIX Viewer Service:** C:\Program Files\VistA\Imaging\VIX.Config\VIX.Viewer.config
- **VIX Render Service:** C:\Program Files\VistA\Imaging\VIX.Config\VIX.Render.config

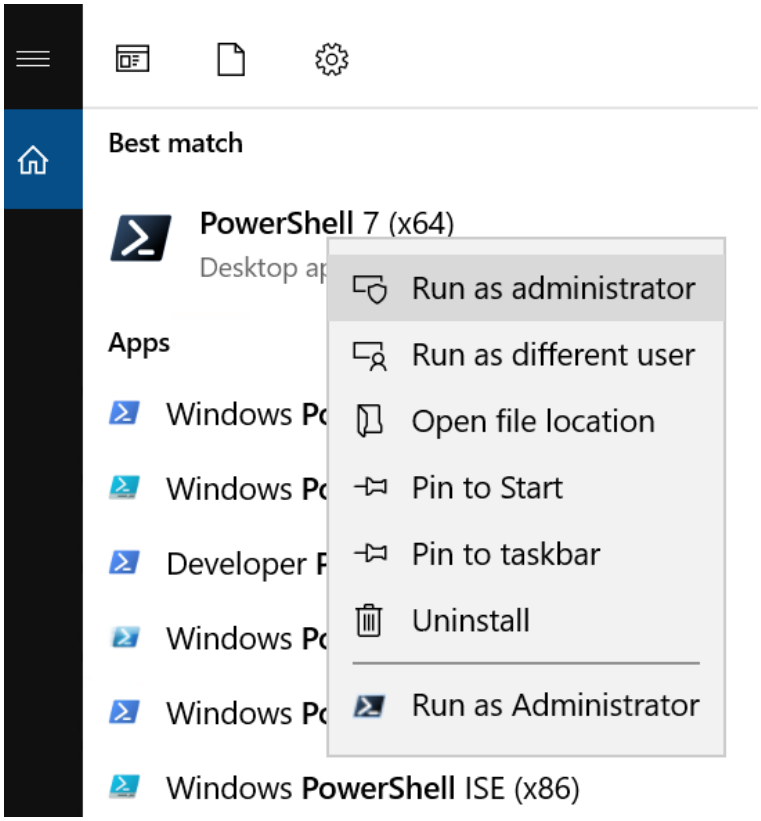
NOTE: Once you are done troubleshooting, be sure to set the logging level back to "Warn," or the log files might become very large and potentially fill up the hard drive.

2.3.5. Viewer Image Caching

The zero-footprint image viewer uses pre-processed images and metadata stored in the VIX Render cache. The VIX render cache is a temporary cache of files built automatically when images are requested for viewing. When images are requested for viewing, the Viewer service fetches the images from the local VIX cache and calls the Render service to create optimized versions of those images for rendering in a web browser. The following describes how to manually re-initialize the Render cache on any given VIX server if needed:

1. Run PowerShell as an administrator (Figure 7).
    a. Right-click **Start**.
    b. Left-click **Search**.
    c. Type **powershell**.
    d. Right-click **PowerShell 7 (x64)**
    e. Left-click Run as administrator.

Figure 7: Execute Windows PowerShell



2. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes**.
3. Once PowerShell launches, **type** the command:
   `cd "C:\Program Files\VistA\Imaging\Scripts"`
   Then press **[ENTER]** to change the working directory to the Scripts folder.
4. Then **type** the command:
   `.\CacheCurator.ps1`
   And press **[ENTER]** to execute the script. Wait for the script to complete.
5. Wait for the script to complete and then close PowerShell.
6. Verify Viewer operations by opening a few studies by launching via zero-footprint Image Viewer in JLV.

2.3.6. Currently Supported Service-Object Pair (SOP) Classes

Table 3 contains a list of currently supported Service-Object Pair (SOP) classes.

Table 3: Supported SOP Classes

SOP Class Name	SOP Class UID
Computed Radiography Image Storage	1.2.840.10008.5.1.4.1.1.1
Digital X-Ray Image Storage - For Presentation	1.2.840.10008.5.1.4.1.1.1.1
Digital Mammography X-Ray Image Storage - For Presentation	1.2.840.10008.5.1.4.1.1.1.2
Digital Intra-Oral X-Ray Image Storage - For Presentation	1.2.840.10008.5.1.4.1.1.1.3
CT Image Storage	1.2.840.10008.5.1.4.1.1.2
Enhanced Computerized Tomography (CT) Image Storage	1.2.840.10008.5.1.4.1.1.2.1
Ultrasound Multi-frame Image Storage	1.2.840.10008.5.1.4.1.1.3.1
MR Image Storage	1.2.840.10008.5.1.4.1.1.4
Enhanced MR Image Storage	1.2.840.10008.5.1.4.1.1.4.1
Ultrasound Image Storage	1.2.840.10008.5.1.4.1.1.6.1
Secondary Capture Image Storage	1.2.840.10008.5.1.4.1.1.7
12-lead ECG Waveform Storage	1.2.840.10008.5.1.4.1.1.9.1.1
Hemodynamic Waveform Storage	1.2.840.10008.5.1.4.1.1.9.2.1
X-Ray Angiographic Image Storage	1.2.840.10008.5.1.4.1.1.12.1
X-Ray Radiofluoroscopic Image Storage	1.2.840.10008.5.1.4.1.1.12.2
Enhanced XRF Image Storage	1.2.840.10008.5.1.4.1.1.12.2.1
X-Ray 3D Angiographic Image Storage	1.2.840.10008.5.1.4.1.1.13.1.1
Nuclear Medicine Image Storage	1.2.840.10008.5.1.4.1.1.20
VL Endoscopic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.1
VL Photographic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.4
Basic Text SR	1.2.840.10008.5.1.4.1.1.88.11
Enhanced SR	1.2.840.10008.5.1.4.1.1.88.22
X-Ray Radiation Dose SR	1.2.840.10008.5.1.4.1.1.88.67
Encapsulated PDF Storage	1.2.840.10008.5.1.4.1.1.104.1
Positron Emission Tomography Image Storage	1.2.840.10008.5.1.4.1.1.128

2.4. VIX Implementation and Configuration

The VIX is hosted on a dedicated virtual machine (VM). Careful considerations should be given when sizing the VIX. With the introduction of the Image Viewer, the VIX uses a lot more

resources as it has to process the images for rendering, and it also can cache a large number of images.

VIX configuration is largely automated and is handled as part of the VIX installation process.

Installation details, including licensing, supported operating systems, and hardware requirements, are covered in the VIX Installation Guide.

2.5. VIX Dependencies

The systems in Table 4 must be present for proper VIX operation.

Except for the local VistA database, the VIX can function for some time at reduced efficiency if any of these systems are temporarily unavailable.

Table 4: Systems for VIX Operation

Name/Location	Function	Interface Method
Local VistA	Provides metadata and image locations to requesting VIXes, controls access to local VIX transaction log; VistA logging of VIX-mediated image accesses.	LAN/RPC
VIX cache	Provides cached images for improved speed.	LAN
Remote VistA	Source of remotely stored VA images for local clinician access. (The VIX continues to operate if a specific remote VistA system is unavailable; it just cannot provide images from that remote system.)	WAN/http
CVIX (at VA data center)	Source of remotely stored DoD images for local clinician access. (The VIX continues to operate if CVIX is unavailable; it just cannot provide DoD images.) Also hosts the VistA site service, which provides connection data to the VIX. A VIX uses locally cached connection data if the VistA Site Service is unavailable.	WAN/http

2.6. VIX Operational Priority

The operational priority of the VIX depends on the nature of the server where the VIX is installed and what the VIX is being used for at a given site.

2.6.1. Standalone Server

When the VIX is installed on a standalone server, the VIX's operational priority depends on the role of clinicians using the VIX for remote image access. If the standalone VIX server is shut down:

- Clinicians using Clinical Display can still retrieve remote VA images (at a reduced performance) using Remote Image Views; however, this may be temporarily inaccessible. Clinical Display attempts to revert to pre-VIX

remove image views and Clinical Display may need to be restarted. In this scenario, the operational priority of a VIX on a standalone server is low.

- Radiologists performing remote reading using the VistARad VIX-assisted operations cannot view local and remote images together unless the images are routed to VistARad using the DICOM Gateway's routing function. Because of the variations involved, each site must make its operational priority assessment in this case.
- DICOM Importer client users cannot login and import images.
- Clinicians viewing images or artifacts (local or remote) in JLV cannot access them during the duration of the VIX shutdown.
- iMedConsent users Signed Informed Consent ability to store new consent forms will be unavailable.
- Any new Ingest consuming application will be unavailable to store new contents.
- Integrated Visualization System (IVS) mobile application users cannot access local images.
- Enterprise DICOM Query/Retrieve (Q/R) functionality will not be available.
- Access to DoD images or artifacts will not be available.
- Access to VA Cerner images or artifacts will not be available.
- Any other external application calling a local VIX service directly will be impacted during the duration of the VIX shutdown.

For detailed information about how the VIX responds if the hosting server is rebooted, see *VIX Startup and Shutdown.*

2.7. Security, Data Integrity, and Data Sensitivity Considerations

The VIX uses the following security, data integrity, and sensitive data handling methods.

- The VIX only responds to requests from authenticated applications. Application-level authentication is invisible to the user who initiated the request.
- Requests for VA data include user credentials that are authenticated and logged by the VistA system where the data resides. The VIX supports both Broker Security Exchange (BSE) and pre-BSE-style remote logins.
- Requests for VA data include user credentials that are authenticated and logged by the VistA system where the data resides. The VIX supports BSE, Identity and Access Management (IAM) STS (Secure Token Service), and pre-BSE-style remote logins.

- Access to the VIX transaction log requires authentication with the local VistA system (relative to the VIX in question). It is limited to VistA users that hold the MAG VIX ADMIN security key.
- VIX installation and VIX-to-VIX communications cannot proceed without a security certificate.
- The VIX delegates the sensitivity (data integrity checking implemented by the application requesting data from the VIX. [When Clinical Display requests data, Clinical Display specific logic is used. When VistARad requests data, VistARad specific logic is used.]).

3. VIX General Operations

This chapter covers:

- *VIX General Operations Overview*
- *The VIX and the VistA Service*
- *Using the VIX Transaction Log*
- *VIX Data Retention and Purges*
- *VIX Startup and Shutdown*
- *Monitoring/Maintaining the VIX*
- *Monitoring/Maintaining the VIX Viewer*
- *The VIX and Backups*

3.1. VIX General Operations Overview

VIX operations fall into two categories.

- General operations, which are described in this chapter.
- Function-specific operations (such as image sharing), which are covered later in this manual.

General operations are the activities that always occur as long as the VIX is running. These include retrieving data from the VistA Site Service, general logging, purging old data, and VIX startup/shutdown.

While most VIX operations are automated, the VIX does require some basic monitoring. For more information, see *Monitoring/Maintaining the VIX*.

3.2. The VIX and the VistA Site Service

The VistA Site Service is a CVIX-hosted central repository of connection information. A VIX (along with other VistA Imaging components) uses the VistA Site Service to get connection information for other VistA sites, other VIXes, and the CVIX itself.

The VIX automatically downloads and caches connection information from the site service each day at 11:00 PM, and any time the VIX is restarted. The VIX uses this cached information rather than access the site service for every transaction.

If your local connection information for VistA or the VIX changes, you must do the following:

1. Contact the REDACTED mail group to update your site's information in the VistA Site Service.
2. After step 1 is complete, re-run the VIX installation wizard to update your VIX configuration information. For details, see the VIX Installation Guide.

3.3. Using the VIX Transaction Log

The VIX transaction log records information about every image and metadata transfer handled by the VIX. Entries in the log are retained for 30 days and then purged. A permanent backup copy of the VIX transaction log is also stored remotely.

The VIX transaction log can be accessed using Chrome or Edge. The main transaction log Web page can display, filter, and export log entries of interest.

To access the transaction log, you need the following:

- A VistA account with the MAG VIX ADMIN security key assigned to it (while the log is a Web page, the VIX uses a VistA account to secure the log).
- Access to https://***FQDN***:REDACTED/Vix/secure/VixLog.jsp

  (where ***FQDN*** is the server the VIX is installed on.)

NOTE: For security reasons, completely close out of your browser at the end of your session.

You can only access the VIX transaction log while the VIX is running.

To view the VIX transaction log, complete the following steps.

1. Navigate to https://***FQDN***:REDACTED/Vix/secure/VixLog.jsp.
2. Enter your VistA access and verify codes in the User Name and Password boxes and click **OK**.

   NOTE: Transaction log credentials are authenticated against the local **VistA** system. Attempting to use Windows credentials do not work.
3. The VIX Transaction Log page displays.
   - By default, the page displays the 100 most recent transactions for the current day.
   - The transactions are ordered from newest to oldest.
4. For detailed information about each field in the log, see *VIX Transaction Log Fields*.
5. To view different parts of the log, use the paging buttons near the top and at the bottom of the log as follows:
   - Click Next to show the next page of (older) entries.
   - Click Last to show the last page of (oldest) entries.
   - Click Prev to show the previous page of (newer) entries.
   - Click First to show the first page (newest) entries in the log.

To change the date range and page size in the VIX transaction log, complete the following steps.

1. To change the date range used to filter log entries, change the values in the **From Date/Time** and **To Date/Time** boxes, and then click **Show in Browser**.

To export part of the transaction log, complete the following steps**.**

7. On the Transaction Log page, use the date/time range boxes near the top of the page to specify the desired date and time range of entries to export.
    - Dates are formatted as YYYY-MM-DD HH-MM.
    - The most recent log entries are shown first.
8. To change the number of entries displayed on each page, select a different value from the Transactions per Page box, and then click Show in Browser.
    - 1,000 exported log entries result in an approximately 0.5 megabyte file.
    - The **Transactions per Page** setting does not apply when log entries are supported.
9. Click **Save as CSV** for comma-separated values or **Save as TSV** for tab-separated values.
10. Use the browser Save dialog box to specify where to store the file.
11. Use a spreadsheet program or a text editor to open the resulting file.

3.3.1. VIX Transaction Log Fields

When the transaction log is displayed in a Web browser, the fields in Table 5 are shown. These fields are also included when the transaction log is exported as a tab-separated values (TSV) or comma-separated values (CSV) file.

Fields that only appear when the transaction log is exported are listed in the next section.

Table 5: VIX Transaction Log Fields

Name	Description
Date and Time	When the VIX processed the transaction. Formatted as MM-DD-YYYY, HH:MM:SS, AM/PM.
Time on VIX	The length of the transaction in milliseconds, begins when the VIX receives a message and ends when the VIX begins to respond.

Name	Description
ICN	The Integration Control Number used to uniquely identify the patient across the VA and DoD systems. (**NOTE** that the Integration Control Number (ICN) is not equivalent to the VA patient ID, and is not considered Protected Health Information.)
Query Type	A multi-part field that indicates [*handler method receiving site* <- *sending site*]. *handler* identifies the VIX Web application that handled the request. For details see *VIX Interfaces*. *method* identifies the specific operation performed: image transfer – Used to transfer an image. getStudyList – Provides the DoD with study metadata from a VA VistA system via the CVIX. Other methods relate to metadata and are described in *Remote Metadata*. *receiving site* <- *sending site* indicates: The station number and home community ID (where applicable) of the sending and receiving sites.
Query Filter	Applies to study metadata only. Indicates whether a list of all available studies for a patient was transferred or if a subset based on date was transferred.
Asynchronous	Indicates whether the transaction was performed asynchronously (true) or synchronously (false).
Items Returned	The number of items returned to the requester. For study metadata, indicates the number of studies or images in the list being transmitted. For an image, this field has a value of 1 if the requested image was transmitted or 0 if the requested image was not found. For other operations, this column is not populated.

Name	Description
Items Received	The number of items retrieved from the remote site. For study metadata, indicates the number of studies or images in the list being received. For an image, this field has a value of 1 if the requested image was received or 0 if the requested image was not received. If the VIX is operating asynchronously, the values in this field may not match the values in the Items Returned field. In the exported log, this field is labeled *Data Source Items Received.*
Bytes Returned	If populated, the amount of data returned in the request. In the exported log, this field is labeled *Façade Bytes Returned.*
Bytes Received	If populated, the amount of data received in the request. In the exported log, this field is labeled *Data Source Bytes Received.*
Throughput	The image transfer rate. Both the rate and the units of measurement (KB/sec, MB/sec are indicated). They are not populated for metadata. This value is calculated at runtime and is not present in the exported log.
Quality	Populated for images only. Can be one of the following: • THUMBNAIL • REFERENCE • DIAGNOSTIC • DIAGNOSTIC UNCOMPRESSED For more information about these parameters, see *Image Quality and VIX Compression*.
Command Class Name	Internal VIX command used for debugging and support.
Originating IP Address	The IP address of the workstation that initiated the image or metadata request.
User	The name of the clinician that initiated the request.
Item in Cache?	TRUE indicates the image is served from the cache. FALSE indicates the image had to be retrieved from its original storage location. It is not populated for other types of transactions.
Error Message	If a request fails, this field contains an error message describing the failure.
Modality	If applicable, indicates the modality associated with an image request (standard DICOM modality type codes are used).
Purpose of Use	Included for HIPAA (Health Insurance Portability and Accountability Act) tracking purposes.

Name	Description
Data Source Protocol	The source of the data being handled: vistaimaging – Data from a VistA system: vftp – Data from another VIX
Response Code	The response code for a request; generally equivalent to HTTP response codes but, in some cases, they are used for statuses specific to the VIX. Typical values include: 200 – OK (success) 401 – Unauthorized 404 – Not found 409 – Image exists but is not yet available on DoD integrator and/or Imaging jukebox 412 – BSE token expired 415 – Image conversion exception 500 – Internal server error
Realm Site Number	The STATION NUMBER (field (#99)) of the INSTITUTION file (#4) of the site that the requester's credentials are authenticated against.
URN	Only populated for image transactions. Universal Resource Name (URN); the unique name of the image being requested.
Transaction Number	The Globally Unique Identifier (GUID) for an image or metadata transaction. For transactions that originate from Clinical Display or the DoD, the same identifier appears in the Image Access log at the site where the images are stored.
VIX Software Version	The software version used by the local VIX.
VistA Login Method	The method used to access a VistA system. This is only populated when connecting to VistA and only for the transaction that initiates the connection. Possible values are BSE, CAPRI, or LOCAL.
Client Version	The version number of the Clinical Display software. This field is populated only for Clinical Display requests.
Data Source Method	Identifies the specific operation performed by the data source.
Data Source Version	The version number of the data source.
DataSourceResponse Server	The name of the server that responded to the metadata or image request. Only populated for requests directed to a VIX or CVIX. **NOTE:** This field cannot be populated if the requesting or responding server is a MAG*3.0*83 VIX.
VIX Site Number	The site number of the local VIX (as defined in the local VIX's VixConfig.xml file). The site number should match the station number (field #99) defined in the INSTITUTION file (#4).

Name	Description
Requesting VIX Site Number	The site number of the requesting VIX (as defined in the remote VIX's VixConfig.xml file), Only populated for Federation (VIX-to-VIX) requests. The site number should match the station number (field #99) defined in the INSTITUTION file (#4).

3.3.2. VIX Transaction Log Fields (Export Only)

When the transaction log is exported as a tab- or comma-separated file, the exported file includes all of the fields available in the browser view of the log (see previous section). The exported file also includes additional fields that are described in Table 6.

Table 6: VIX Transaction Log Fields (Export Only)

Name	Description
Façade Bytes Retrieved	The number of bytes returned to the requestor, where the requestor could be Clinical Display, VistARad, another VIX, or the CVIX.
Data Source Bytes Returned	The number of bytes returned from the data source, where the data source could be a remote VistA system, a VIX, the CVIX, or a DoD data source such as DAS or DES or ECIA.
Machine Name	Name of the VIX server that performed the transaction.
Requesting Site	The ID of the site that originated the request; this value is also shown in the Query Type column.
Exception Class Name	Internal data used for debugging and support.
Time to First Byte	Number of milliseconds elapsed from the point where the VIX opens a connection to a remote site until the remote site begins responding to the request.
Responding Site	The ID of the site that filled the request; this value is also shown in the Query Type column.
Command ID	Internal ID used for debugging and support.
Parent Command ID	Internal ID used for debugging and support.
Façade Image Format Sent	The format of the image VIX returns to the requester.
Façade Image Quality Sent	The quality of the image VIX returns to the requester; in some cases, this quality is better than the quality requested (as indicated in the "Quality" column).
Data Source Image Format Received	The format of the image VIX receives from its source.
Data Source Image Quality Received	The quality of the image VIX receives from its source.
Debug Information	Internal messaging used for debugging and support.
Thread ID	The name of the thread that processed the transaction.

3.3.3. Log Collector Service

The VIX Log Collector service automatically backs up VIX transaction logs and stores the backup copies on a centralized data center server. This allows the information in VIX transaction logs to be retained after the logs are purged locally (the local retention period is 30 days). The Log Collector service is hosted on the same data center servers where the CVIX resides.

Once a day, the log collector service copies each VIX's local transaction logs to a data server storage area for permanent storage. The time that the backup is performed is configured centrally and is set to be during low-usage hours.

When the Log Collector performs its daily backup, it collects only one full day's worth of VIX transaction log entries to limit network impact. For example: on Monday, the Log Collector service collects all VIX log entries from the previous Saturday.

If the Log Collector cannot reach a VIX on a given day, it queues its backup attempt and attempts to copy any backlogged items during the next backup period. Multiple failed attempts to back up a specific transaction log generates an email warning to data center administrators (email address entered during the VIX installation), who then would contact the local VIX administrator if local corrective action were needed.

The VIX Log Collector service does not require any site-level or local VIX configuration.

3.4. VIX Data Retention and Purges

The VIX writes only a limited amount of data to VistA; this is described in *Database Information*. The VIX transaction log is stored on the server where the VIX is installed (see Section 3.3 for details); images and associated metadata are stored in the VIX cache.

The VIX runs a daily purge process for locally stored data, as described in Table 7:

Table 7: VIX Daily Purge Process

Operation	When Performed
Purge Java logs	1 A.M. daily for Java log entries more than 5 days old.
Purge transaction log entries	2 A.M. daily for transaction log entries more than 5 days old.
Purge VIX cache	3 A.M. daily for images more than 30 days old. Once per minute for old VA metadata, once per hour for old DoD metadata.

3.5. VIX Startup and Shutdown

The VIX service is designed to be running at all times except during daily automatic scheduled restarts. The daily restarts occur at 4:00 AM by default, but this time can be modified as desired. When the VIX is implemented on the same cluster used for Imaging resources, the VIX is a part of the same resource group used to manage image storage and is not intended to be shut down or restarted independently from the rest of the resource group.

In general, the only time the VIX service needs to be shut down independently from the hosting server is when the VIX software is being updated. For details, including user impact, refer to the VIX Installation Guide.

Table 8 summarizes how the VIX service responds if there is a restart of the server on which the VIX is installed or an interruption of the VIX's connection to the local VistA System.

Table 8: VIX Service Response to Restart or Interruption

Scenario	VIX Service Behavior
Unplanned server shutdown (or failover)	If the VIX is installed on a standalone server, the VIX service restarts itself after the server is restarted.
Planned server shutdown (maintenance, Microsoft software updates, etc.)	The VIX service does not need to be stopped; the VIX service restarts automatically once the server is restarted.
VIX service fatal error (server unaffected)	On a standalone server, the VIX service restarts itself automatically after 60 seconds and continues restarting itself if it encounters additional errors.
Local VistA system restart and/or restore	In the event of a local VistA system restart, the VIX automatically refreshes any previously cached connections within 30 seconds to one minute. VIX operations are unaffected in a VistA system database restore; the VIX stores no configuration information on VistA.

3.6. Monitoring/Maintaining the VIX

In typical usage scenarios, the VIX service needs only minimal monitoring and maintenance.

- Once a day, access the transaction log to verify that the VIX is running and that the VIX communication ports REDACTED are not blocked. If necessary, you can also verify the state of the VIX service directly as described below.
- Once a week, check available space on the drive used for the VIX cache. In a newly implemented VIX, the VIX cache size increases rapidly for the first 30 days, and then should level off as the VIX begins to purge older images.
- Optionally, you can get a sense of the VIX processing load by using the Windows Task Manager to determine the CPU cycles being consumed by the Apache Tomcat task.

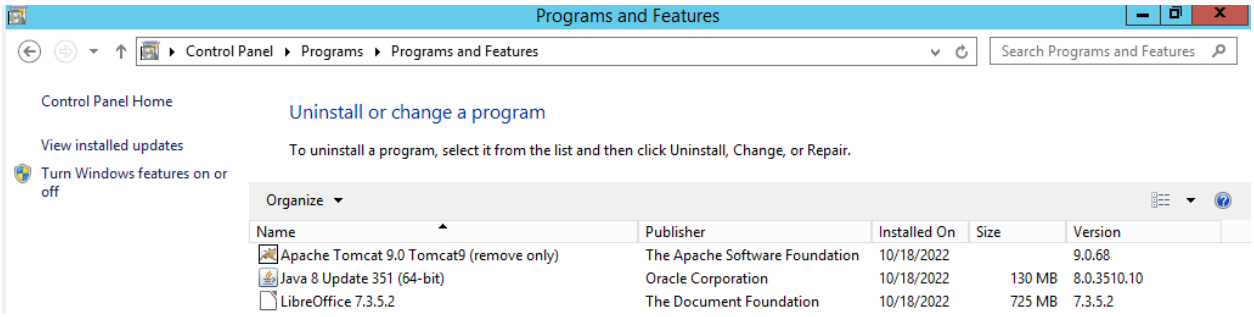
As described in the previous section, the VIX service restarts automatically if the hosting server is restarted.

3.6.1. Checking the VIX Service

1. On the server where the VIX is installed, log in as a local administrator.
2. Open the Services window (click **Start | All Programs | Administrative Tools | Services**) shown below.

3. On the right side of the window, locate the Apache Tomcat service and verify that its status is **Running** (Figure 8).

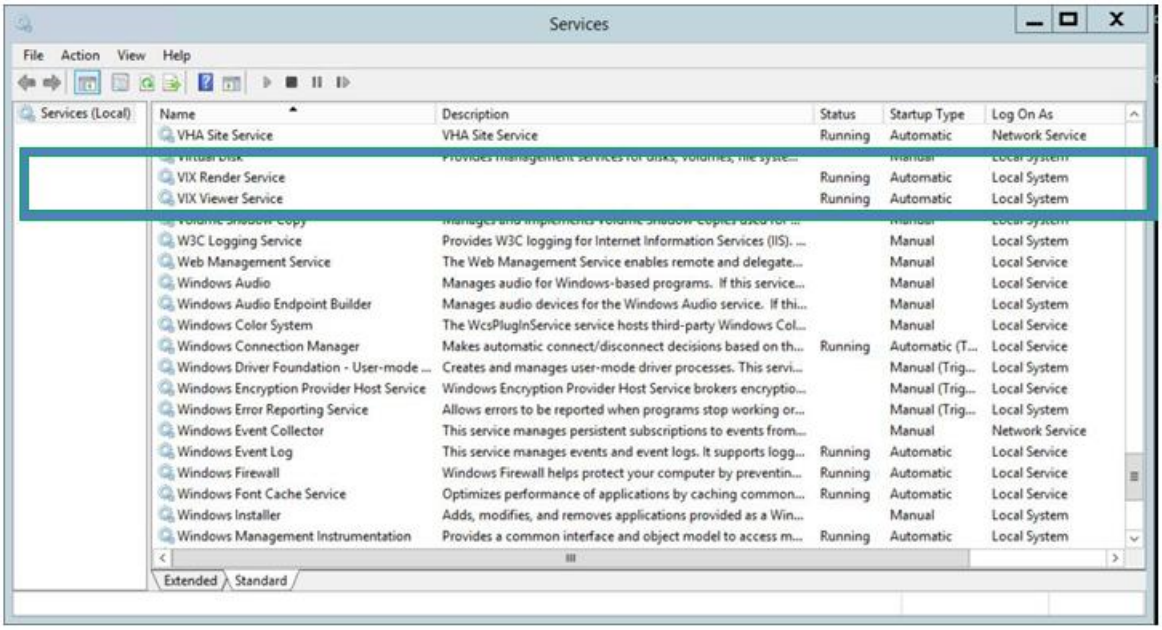
Figure 8: Check Apache Tomcat Service



3.7. Monitoring/Maintaining the Image Viewer

The Image Viewer hosts two independent services. These services show up as the VIX Viewer Service and the VIX Render Service (Figure 9).

Figure 9: VIX Viewer and Render Services



The Viewer and Render services must be operational for the site VIX to be able to provide viewing. To verify operation, one has to log into the consuming applications, select a patient with images, and display the images. If the operation fails, proceed to the *Troubleshooting* section.

3.7.1. Troubleshooting the Image Viewer

The operation of the Image Viewer depends on the presence and correct operation of a number of resources.

- The Apache Tomcat service must be operational, and the VIX services must be operational.

- There should be sufficient disk space available for the VIX and Render caches.
- The VIX Viewer and Render Services must be running and operational.

To verify that the VIX is operational, proceed to the normal troubleshooting of VIX services.

Review the Render Service logs to look for any errors related to access to the SQLite located in:

System Drive*Program Files\VistA\Imaging\VIX.Render.Service\log*

In case the SQLite is failing, follow the steps outlined in *Viewer Image Caching* to clear the cache.

3.7.1.1. Analyzing Image Viewer Logs

The VIX Viewer keeps logs in ***System Drive***:\Program Files\VistA\Imaging\VIX.Viewer.Service\log and ***System Drive***:\Program Files\VistA\Imaging\VIX.Render.Service\log.

Review the logs for errors and other information you seek.

Modify the log level according to the instructions in the *Service Logging* section.

3.8. The VIX and Backups

The VIX itself does not need to be explicitly backed up.

- The VIX transaction logs are automatically backed up offsite.
- The VIX cache is transitory and does not need to be backed up.
- VIX-specific configuration settings can be recovered by reinstalling the VIX software.

NOTE: The Laurel Bridge DICOM Connectivity Framework (DCF) toolkit that the VIX uses has a unique product serial number that should be stored in a safe place in case the VIX needs to be reinstalled. For details about where and how this serial number is used, see the VIX Installation Guide. If you need to recover this serial number and there is no local record, you can contact the REDACTED mail group.

4. VIX Image Sharing

This chapter describes the VIX operations that are specific to image sharing. Specifically, this chapter covers:

- *Remote Metadata Retrieval*
- *Remote Image Retrieval*
- *Caching of Metadata and Images*
- *Image Sharing-related Logging*
- *Image Sharing and VIX Timeouts*
- *Troubleshooting*

4.1. Remote Metadata Retrieval

When a VIX is used to retrieve remote images, the image retrieval is always preceded by retrieving applicable metadata. (In the context of the VIX, metadata is anything that describes an image or image-like object. Metadata includes patient names, IDs of various types, procedure names, index field values, number of images in an exam, radiology reports, and so on.) Also, in some cases, such as retrieving an exam report, metadata retrieval is the only action needed to fulfill a clinician's data request.

Many Clinical Display or VistARad operations silently trigger requests to the VIX to retrieve metadata from remote sites. In general, the VIX handles metadata retrievals as follows:

1. The application (Clinical Display or VistARad) issues a request for metadata based on a clinician's activities.
2. The local VIX determines whether caching is allowed for the specific request. For details about which requests are cached, see the tables in the next two sections.
3. If caching is not allowed, the VIX skips all cache checks, retrieves the metadata directly from the remote site, and proceeds to step 5.
4. If caching is allowed, the VIX first attempts to retrieve the desired metadata from its local cache. If the metadata cannot be found locally, it is retrieved from the remote site (Table 9).

Table 9: Remote Metadata Retrieval for Different Remote Site Types

Remote site type	How remote metadata is retrieved
VA site with VIX	The remote VIX retrieves the metadata, either from the remote VIX's cache or the remote site's VistA system.
VA site; no VIX	The local VIX retrieves the metadata directly from the remote VistA Imaging system.
DoD (via CVIX)	The CVIX retrieves the metadata either from its own cache or from the applicable DoD system.

5. The local VIX passes the data back to the requesting application.

4.1.1. Metadata Requests from Clinical Display

Table 10 summarizes the metadata requests that Clinical Display can issue to a VIX. The request names used in the table are reflected in the Query Type field of the VIX transaction log.

Table 10: Clinical Display Metadata Requests Summary

Clinical Display Metadata Request	Data Returned	VIX caching allowed?
getImageDev Fields	Populates data in the Image Information Advanced window when **Field Values** is used to look up IMAGE file (#2005) values for a remote image.	No
getImage Information	Populates data in the Image Information window.	No
getImageSystem GlobalNode	Populates data in the Image Information Advanced window when **^MAG(2005** is used to display the global for a remote image.	No
getPatientShallow StudyList	Provides the study metadata used in remote site buttons, the Image List, and Abstracts windows. **NOTE:** For this request, the local VIX always gets new data from remote VistA system and always locally caches the data it retrieves. This is done, so the data is readily available for getStudyImageList requests that use the same data.	Yes, see note
getStudyImageList	Provides the study metadata needed to populate the Group Abstracts window.	Yes
getStudyReport	Retrieves a report for a remote exam.	Yes
pingServerEvent	Indicates whether a remote site is available.	n/a
postImageAccess Event	Sends a message to a VA site IMAGE ACCESS LOG file (#2006.95) when a VA image is viewed, copied, or printed.	n/a

4.1.2. Metadata Requests from VistARad

Table 11 summarizes the metadata requests that VistARad can issue to a VIX. The request names used in the table are reflected in the Query Type field of the VIX transaction log.

Table 11: VistARad Metadata Requests Summary

VistARad Metadata Request	Data Returned	VIX caching allowed?
getActiveWorklist	Populates remote worklists accessed using the VistARad Monitored Sites exam list tab.	No
getExamDetails	Retrieves additional exam metadata when a local VistARad user opens a remote exam. **NOTE:** In some cases, this request can be partially filled using data previously cached to fill a recent getSiteExamList request. If this is the case, the VIX uses whatever cached data is available and pulls the rest of the data from the remote site.	Yes, see note
getExamSiteMetadataCachedStatus	Checks to see if a list of exams for a remote patient is already on the local VIX cache.	n/a
getReport	Retrieves a report for a remote exam.	Yes
getRequisition	Retrieves a requisition for a remote exam.	Yes
getSiteExamList	Retrieves a list of exams for a specific patient from a remote site. **NOTE:** Whenever this request is made, the VIX automatically issues an asynchronous getExamDetails request.	Yes, see note
pingServer	Indicates if a remote site is available.	n/a
postImageAccess	Sends a message to a VA site IMAGE ACCESS LOG file (#2006.95) when a VA image is viewed, copied, or printed.	n/a

4.2. Metadata Requests from the Zero-Footprint Image Viewer

Table 12 summarizes the metadata requests that the Zero-Footprint Image Viewer can issue to a VIX.

Table 12: Zero-Footprint Image Viewer Metadata Requests Summary

New Image Viewer Metadata Request	Data Returned	VIX caching allowed?
/vix/viewer/studyquery	The basic metadata of the studies.	Yes
detailsUrl	Detailed metadata about the study.	Yes
thumbnailUrl	Thumbnail image that could be used to represent the study.	Yes

New Image Viewer Metadata Request	Data Returned	VIX caching allowed?
manageUrl	A web page that displays image thumbnails, imaging data etc. You can delete images or manage controlled images using this web page.	Yes
viewerUrl	A web page containing the image viewer.	Yes
/vix/viewer/ping	Check if the service is running.	Yes

4.3. Remote Image Retrieval

When a clinician selects a remote VA or DoD image for display, the VIX uses complex processing to deliver the most desirable image in the shortest amount of time.

The following steps summarize this process.

1. The clinician initiates the display of a remote VA or DoD image.
2. The application (Clinical Display or VistARad) issues a request for the image to the local VIX. The contents of this request (which was provided by the VIX in an earlier metadata retrieval) includes the following:
   - The image identifier
   - The desired image quality (see *Image Quality and VIX Compression*)
   - A list of acceptable image formats (see *Image Types vs. Image Formats*)
3. The local VIX first checks its local cache for the image. If the VIX finds the image in its cache and if the image of the desired quality and is in any of the acceptable formats, the local VIX stops the search and proceeds to step 6.
4. If the image is not stored on the local VIX's cache, the VIX queries the remote site for the image (Table 13).

Table 13: Remote Image Retrieval for Different Remote Site Types

Remote Site Type	How Remote Image is Retrieved
VA site with VIX	The remote VIX retrieves the image, either from the remote VIX's cache or from the remote site's VistA system. The remote VIX may convert or compress the image (based on the quality specified in the request) to increase the speed of WAN transfers.
VA site; no VIX	The local VIX retrieves the image directly from the remote VistA Imaging system.
DoD (via CVIX)	The CVIX retrieves the image, either from its own cache or from the applicable DoD system. The CVIX may convert or compress the image (based on the quality specified in the request) to reduce retrieval times.

5. If needed, the local VIX decompresses or converts the image into one of the acceptable image formats.
6. The local VIX passes the image to the requesting application.

4.3.1. Image Quality and VIX Compression

The combination of the requested image quality and whether there is a remote VIX involved can affect how a VIX fills a request for a remote image.

Table 14 summarizes these processing differences. For simplicity's sake, this table presumes that the request originates locally, that the requester is a VA clinician, and that an image of the requested quality is *not* already in either the local or remote VIX cache (in which case some or all of the processing would be skipped).

Table 14: VIX Compression Logic for Request Type

Parameter	Requested by	VIX Compression Logic*
DIAGNOSTIC	Clinical Display Radiology Viewer and VistARad, Image Viewer	If a remote VIX is present, the remote VIX locates the highest-resolution image available and automatically converts the image into a lossless compressed format before sending the image across the WAN to the local VIX. For radiology images, lossless DICOM encapsulated JPEG 2000 is the most frequently used format with a compression ratio of about 2.5:1. If there is no remote VIX, the local VIX locates the highest- resolution image available at the remote site and pulls the image across the WAN in the image's native (uncompressed) format.
DIAGNOSTIC UNCOMPRESSED	Clinical Display Full Resolution Viewer, Image Viewer	If a remote VIX is present, it automatically packages the images as a ZIP file before transferring them across the WAN. If there is no remote VIX, the local VIX locates the highest- resolution image available at the remote site and pulls the image across the WAN in the image's native (uncompressed) format.

Parameter	Requested by	VIX Compression Logic*
REFERENCE	Clinical Display Radiology Viewer only, Image Viewer	If a remote VIX is present, it generates a new reference-quality copy of the image using the highest resolution source image available. Then the remote VIX sends the reference quality image across the WAN to the local VIX. • The new image is as good as, if not better than, any pre-existing reference quality image (s) stored on the remote VistA system. • The compression ratio achieved averages about 24:1 for CR images and 10:1 for CT and MR images. If there is no remote VIX, the local VIX checks the remote VistA system for a downsampled image. • If a downsampled image is present (as is usually the case for CR or DR images), that image is retrieved across the WAN. • If a downsampled image is not present (as may be the case for CT and MR images), the local VIX pulls the full resolution image from the remote site across the WAN. The local VIX then converts the image to one of the formats specified in the image request.
THUMBNAIL	Clinical Display, Image Viewer	The presence or absence of a remote VIX does not impact how thumbnail images are handled.

* If the requested image originates from the DoD, the CVIX performs the same operations that a remote VIX would perform.

4.3.2. Image Types vs. Image Formats

When a local VA clinician requests a remote image from the VIX, an earlier metadata retrieval has already established the formats that the desired image can be delivered in.

Table 15 lists possible formats that the VIX can return based on image type. When multiple formats are listed, the VIX checks each potential storage location (VIX local cache, VIX remote cache [if present], remote VistA system) for an instance of the image in any of the possible formats before proceeding to the next more remote storage location. If the image has to ultimately be retrieved from the remote site, and if it is not in one of the possible formats, the Image Viewer converts the image to one of the possible formats below before returning it to the requesting application.

Table 15: Image Formats VIX can Return Based on Image Type

Image Type (from #2005.021)	Image Description (from #2005.021)	Possible formats returned by VIX
1	JPEG	JPEG, TIFF, bitmap
3*	XRAY (TGA) (intended for Clinical Display Radiology Viewer)	DICOMJ2K, J2K, DICOM, TGA
3**	XRAY (TGA) (intended for VistARad)	DICOM, TGA
9	Black and White image	JPEG, TIFF, bitmap
17	Color Scan	JPEG, TIFF, bitmap
18	Patient Photo	JPEG, TIFF, bitmap
19	XRAY_JPEG	JPEG, TIFF, bitmap
15	TIFF	JPEG, TIFF, bitmap
21	Motion Video (AVI, MPG)	AVI
100*	DICOM (intended for Clinical Display Radiology Viewer)	DICOMJ2K, J2K, DICOM, TGA
100**	DICOM (intended for VistARad)	DICOM, TGA
101	HTML	HTML
102	Word	DOC
103	ASCII Text	TEXT_PLAIN
104	PDF	PDF
105	RTF	RTF
103	Audio (WAV, MP3)	WAV, MP3

* The local VIX always attempts to convert the requested image to DICOM J2K if the header data is available.

** The local VIX always attempts to convert the requested image to DICOM if the header data is available.

4.4. Caching of Metadata and Images

The VIX automatically stores all images, and most of the metadata it handles as a part of image sharing in its own local cache. The VIX cache is self-managing and is independent of other Imaging storage areas and caches.

The VIX cache improves the VIX performance by storing data (especially images) retrieved from remote sites and/or processed by the VIX. If the image is requested again, it can be pulled from the local cache of the VIX without having to retrieve it from the remote site or reprocess it.

At multidivisional sites where there can be more than one VIX, the VIX that handles the data is the only VIX that caches the data (if applicable).

NOTE: Metadata and images cached by the VIX are considered transitory copies and are not a part of the patient record. The site from which the data originates is the official custodian of the data, not the VIX.

4.4.1. Cache Retention Periods

The VIX purges data from its cache when the retention period for the data is reached. The images are considered static data, allowing relatively long cache retention while retaining data consistency. Metadata, which is less static, is retained for shorter periods.

Table 16 lists retention periods based on the source and type of data.

Table 16: Retention Periods by Data Type

Data type	Retained for	Scan to delete old items is run
VA and DoD images	30 days	Once per day at 3 AM
VA metadata	1 hour	Once per minute
DoD metadata	1 day	Once per hour
DICOM SCP images and metadata	30 days	Once per minute

4.4.2. Cache Location

The cache is located in the /VixCache folder on a local drive (when the VIX is installed on a dedicated standalone server).

NOTE: Never manually change the contents of the Vix Cache folder and subfolders using Windows Explorer while the VIX is running.

NOTE: If you need to change the location of the VIX cache, you must re-run the VIX installation wizard to update your VIX's configuration information. For details, see the VIX Installation Guide.

4.5. Image Sharing-related Logging

In addition to the VIX transaction log, VIX-supported image sharing is logged on VistA and temporarily logged by Clinical Display.

4.5.1. Logging on VistA

The IMAGE ACCESS LOG file (#2006.95) uses specific values in the ACCESS TYPE field (#1) and the ADDITIONAL DATA field (#100) to indicate when a VIX was involved in an image access.

4.5.1.1. VIX-related Access Type Values

If the ACCESS TYPE field (#1) in an IMAGE ACCESS LOG file (#2006.95) entry contains one of the values in Table 17, the VIX accessed the image on behalf of a remote requester.

NOTE that only the values unique to the VIX are described. For information about other entries in the IMAGE ACCESS LOG file (#2006.95), refer to the file's data dictionary (Table 17).

Table 17: Access Type Values

Access Type Value	Description
RVVAVA	A locally stored image that a remote VA Clinical Display user accesses via a VIX. **NOTE:** This value can be present even if there is no local VIX (i.e., the image was accessed via a remote VIX).
VR-RVVAVA	A locally stored image that a remote VA VistARad user accesses via a VIX. **NOTE:** This value can be present even if there is no local VIX (i.e., the image was accessed via a remote VIX). **NOTE:** A similar value, VR-RVVAVA/REM, indicates a remote VistARad access *without* a VIX.
RVVADOD	A locally stored image that a DoD clinician requests via the VIX (or CVIX if a local VIX is not present). **NOTE:** In this scenario, the VIX (or CVIX) reports all *requests*. Because the requested image is ultimately passed to DoD systems, the VIX (or CVIX) cannot report if the requested image was accessed or not.
RVDODVA	A remotely stored DoD image that a local VA Clinical Display user accesses via the VIX. **NOTE:** The VIX logs this activity at the requesting site rather than at the site where the image is stored because the DoD storage site is unknown to the VIX. **NOTE:** Access to remotely stored DoD images is not logged in #2006.95 if the access is made using VistARad. However, these accesses are recorded in the VIX transaction log.

4.5.1.2. VIX-Related Additional Data Values

The VIX also populates the Additional Data field (#100) based on data provided by the requesting application (Table 18). Because the VIX adds a lot of information to this single free-text field, the VIX uses the vertical bar "|" character to organize the Additional Data field into four parts. Note that these parts exist for organizational purposes only and are not considered discrete pieces in the FileMan sense.

Table 18: Additional Data Fields for Access Type

If Access Type is...	Part 1	Part 2	Part 3	Part 4
RVVAVA	empty	VIX transaction ID	Requesting VA site ID	empty
RVVADOD	empty	VIX transaction ID	Requesting VA site ID	Username of the requesting DoD clinician
RVDODVA	DoD image ID	VIX transaction ID	local VA site ID	empty
VR-RVVAVA	VIX transaction ID	VIX transaction ID	VIX transaction ID	VIX transaction ID

4.5.1.3. Example – RVVAVA Access Type

```
^MAG(2006.95,16401,0)=16401^RVVAVA^126^51^DOD^ROU^3090216.081305^1023^1^4892
^688
^MAG(2006.95,16401,100)=|246a2052-70b1-4ed7-af55-bea35b1|688|
```

4.5.1.4. Example – RVVADOD Access Type

```
^MAG(2006.95,610535,0)=610535^RVVADOD^1376^8820^DOD^XXX^3100302.0
94747^ 1023^1^6557^660
^MAG(2006.95,610535,100)=|5aafabc4-2361-4a34-b843-
5aad4163620c XX.XXX.MIL/HP0000-PZ01|DoDUsername
```

4.5.1.5. Example – RVDODVA Access Type

```
^MAG(2006.95,610566,0)=610566^RVDODVA^126^^Wrks^ROU^3100302.134155^1023^1
^6561^ 660
^MAG(2006.95,610566,100)=urn:bhieimage:rp02_0108_rp01-e403e3c3-bdc2-
4494-b816- 3757b435ec0b|{EEEF890A-4C66-4F8C-8121-2CD1FE8F9B80}|660|
```

4.5.1.6. Example – VR-RVVAVA Access Type

```
^MAG(2006.95,720029,0)=720029^VR-
RVVAVA^126^506^VRAD:3.0.90.6^ROU^
3100405.161144^1011^1^8478^660
^MAG(2006.95,720029,100)={71247e80-f250-42c3-b8ea-9156b6d03a28}
```

4.5.2. Additional Client Logging

4.5.2.1. Clinical Display Message History Log

The Message History log on a Clinical Display workstation can also be used to check/troubleshoot VIX activities.

- To access this log, click located in the lower-left corner of the main Clinical Display window.
- The "transid" in the Message History log can be traced to specific transactions in the VIX transaction log. See *VIX Transaction Log Fields* for details.
- Specific details (such as Internal Entry Numbers (IENs) and image paths) are shown only if the active user holds the MAG SYSTEM key.
- The Message History Log is session-specific and is cleared when Clinical Display is exited.

4.5.2.2. VistARad Logging of VIX Operations

Refer to VistARad documentation for details.

4.6. Image Sharing and VIX Timeouts

When a local VIX retrieves metadata and images from remote sites, the system load at the remote site and WAN network traffic impacts the time needed to complete the retrieval. If a request for data cannot be completed in a timely manner, the local VIX cancels its request. This prevents excessive delays in client applications (Clinical Display and VistARad) that use the VIX.

Table 19 summarizes VIX connection timeout parameters based on the type of remote system and data involved.

Table 19: VIX Connection Timeout based on Remote System Type

Remote System Type	Local VIX Timeout if No Response
VA data via a remote VIX	For metadata, 600 seconds for data transfer to begin (this is to handle very large datasets; usually, data transfer begins in a few seconds). For images, wait up to 30 seconds for initial connection and up to 120 seconds for data transfer to begin.
VA data from a remote non-VIX VA site	For metadata, no timeout. For images, N/A because the local VIX only starts the operation if it can connect to the remote site and can verify that the remote image is present.
DoD data via the CVIX	For metadata, the CVIX waits up to 45 seconds to retrieve DoD metadata before sending a timeout message to the local VIX. For images, the CVIX waits up to 30 seconds for the initial connection with the DoD image source, and up to 120 seconds for the image transfer to begin. If the CVIX is able to retrieve data from some DoD sources but not all of them, the CVIX passes a partial response message to the local VIX. **NOTE:** For some patients, especially polytrauma cases, the source of DoD DICOM data needs more than 45 seconds to process the request. If this happens at the CVIX, the local VIX sends a "Try Again" message to the local requesting application (such as Clinical Display or VistARad). In most cases, the requested data is available within a minute or so, and a subsequent request is successful. **NOTE:** Because the CVIX can retrieve DoD data from multiple sources, there may be cases where one DoD data source responds, but another does not. If this happens at the CVIX, the local VIX sends a partial message to the local requesting application.

4.7. Troubleshooting

Table 20 may help diagnose potential VIX-related image sharing problems.

Table 20: Troubleshooting VIX-related Image Sharing Problems by Symptoms

Symptom	Check
VIX transaction log not accessible	On the server where the VIX is installed, make sure that the VIX is running and that ports REDACTED are not blocked by antivirus firewalls or by an ACL (access control list) update. Also, make sure the VIX service is running as described in *Monitoring/Maintaining the* VIX.
Clinical Display cannot connect to any remote sites	Make sure the local VIX is running and that required ports are open as described above (if you can access the VIX transaction log, the VIX is running). Determine if the issue is specific to one Clinical Display workstation or if it affects all workstations. On an affected Clinical Display workstation, disconnect from and reconnect to all remote sites. If that does not work, restart the Clinical Display software. (If the VIX is the source of the issue, restarting Clinical Display makes Clinical Display use pre-VIX remote image views that are independent of a VIX. However, pre-VIX remote image views cannot be used to access DoD images, and in some cases, they have poorer performance than VIX-supported remote image views.)
VistARad cannot connect to any remote sites	Make sure the local VIX is running and that required ports are open as described above (if you can access the VIX transaction log, the VIX is running). Determine if the issue is specific to one VistARad workstation or if it affects all workstations. On an affected VistARad workstation, go to **View | Settings | VIX Configuration** and verify that the settings on the tab are correct. See the VistARad documentation for details.

Symptom	Check
Retrieval times increase significantly relative to previous retrievals	If the problem is specific to one remote site, there may be an issue with the remote site's VIX. Image retrievals continue at reduced performance until the remote VIX is up and running. If the problem is specific to Clinical Display, check to see if Clinical Display is using pre-VIX remote image views. If this is the case, restart Clinical Display to verify that it uses the VIX for subsequent image retrievals. If the problem is specific to VistARad, refer to VistARad documentation for details. In rare cases, the local VIX cache may become full. (If the VIX cache is full, the VIX continues to retrieve images but bypasses its cache. If the VIX cache is full, contact customer support. If the problem affects all remote sites and the potential issues above have been eliminated, WAN congestion may be the issue.
A specific VA remote site is disconnected (but other remote sites are available)	Determine if the problem affects multiple patients or if it occurs only for a specific patient. If the problem is specific to a single patient, the most likely cause is a problem with the metadata being retrieved from the remote site. If the problem affects all patients, the issue is most likely connectivity with the remote site. In both cases, contact the remote site (if possible) or customer support.
Some, but not all remote images from VA sites are inaccessible	Try to determine if the problem is specific to certain sites, patients, or image types; then contact customer support. If the problem is specific to remote radiology images, try to view those images using both VistARad and the Clinical Display Radiology Viewer; then report the results to customer support.
ID mismatch icon or Questionable Integrity warning for remote images	If the metadata of a remote image does not correlate with local identifiers, the VIX still retrieves the image and stores it in the VIX cache, but Clinical Display or VistARad might block the display of an image. If possible, contact the remote site's Imaging Coordinator, or contact customer support.
DoD remote site button in Clinical Display shows "Try Again" label	This can occur if the source of DoD DICOM images cannot respond to a metadata request via the CVIX within 30 seconds. This is especially likely to happen if the patient in question is a polytrauma patient with a large number of studies. In most cases, the originating system can finish processing the request in a minute or so. Clicking the DoD button again renews the request, and the VIX retrieves the data if it is available.

Symptom	Check
DoD remote site button in Clinical Display shows "Partial" label	This can occur if one or more DoD data sources cannot respond to a request for metadata in a timely manner. If this occurs, the CVIX sends all available metadata back to the local VIX and uses the "partial" flag to indicate that the data is potentially incomplete. If this issue persists, especially for multiple patients, contact customer support.
DoD remote site is unavailable (no "Try Again" label in button)	If the DoD is available on VistARad workstations but not on Clinical Display workstations, verify that the Clinical Display workstations are using the VIX to retrieve images. To do this, check the Image ID of the remote image in the Clinical Display Image List. If the Image ID is prefixed with the string "urn", the VIX is being used. If a standard ID is shown, the VIX is not being used, and you should restart the workstations in question and then try to reconnect to the DoD. If this occurs for Patch 93 Clinical Display only, verify that the MAG VIEW DOD IMAGES security key is assigned to the user. (This key is not checked for Patch 94 or later.) If the connection remains unavailable for more than an hour, contact customer support.
DoD connection is available, but images are inaccessible	If an "Image not Available" icon shows in Clinical Display, there was a delay in processing the images. Wait 30 seconds, and try to display the image again. If an "Image not Found" icon is shown in Clinical Display, the issue cannot be resolved on the VA side. If the image is deemed necessary for medical care, contact customer support.
One or more images appear to be corrupted	Display the image on a different Clinical Display or VistARad workstation to verify that the problem is with the actual image (rather than a transitory display error). If the problem persists, contact customer support immediately.

5. ROI VIX Operation, Configuration and Statistics

This chapter explains how the VIX processes ROI (Release of Information) requests, describes the ROI-related statistics and configuration parameters, and explains how to configure the other ROI-related parameters of the VIX.

5.1. How the VIX Processes ROI Requests

There are two ways in which the VIX can process ROI disclosure requests:

- Immediately when it gets the disclosure request and/or
- Periodically, in the background

How the VIX processes ROI disclosures is determined by two parameters in its configuration. By default, both parameters are enabled, and the VIX uses both ways to process ROI disclosure requests simultaneously.

Users with the MAG VIX ADMIN security key can modify these parameters.

NOTE: At least one of the two ROI processing parameters must be enabled for the VIX to process ROI requests. If both parameters are disabled, the VIX does not process ROI requests. It displays a message alerting VIX administrators to the fact that ROI requests cannot be processed until at least one of the parameters is enabled.

NOTE: Reinstalling the VIX service resets these parameters to their default enabled values. If these values have been changed manually, the change needs to be reapplied after the VIX service is installed.

5.1.1. Processing ROI Disclosure Requests Immediately

When the parameter **Process Disclosure Requests Immediately** is enabled, the VIX processes ROI disclosure requests when it receives them. This option does not require ROI processing credentials. The VIX uses the credentials of the user who submits the ROI request to process the disclosure. By default, this option is enabled. However, if the VIX gets too busy, users with the MAG VIX ADMIN security key can disable this option and configure the VIX to only process ROI disclosures periodically.

NOTE: If the VIX is interrupted while processing an ROI request because of a network disconnection or a VIX restart, the ROI disclosure completes only if periodic processing is enabled. If periodic processing is not enabled, the request does not complete.

5.1.2. Periodic Processing of ROI Disclosure Requests

When periodic processing is enabled, the VIX processes ROI disclosure requests periodically, in the background. Enabling periodic processing is useful because it allows an ROI disclosure to be completed even if the VIX operation is interrupted because the VIX was restarted or because it ran into an issue.

Periodic processing requires a valid VistA account with ROI processing credentials. If the credentials provided to the VIX are invalid, periodic processing does not work.

For information about setting ROI Processing credentials, see *ROI Periodic Processing Credentials*.

5.1.3. Purging Completed Disclosures

When the parameter **Completed Disclosures Purge Processing** is enabled, the VIX purges old ROI disclosures after the number of days specified in the parameter **Completed Disclosures Purge Days**.

The purge removes the metadata associated with an ROI disclosure from the VistA database. The actual ROI disclosure result is removed when the VIX cache purges data, typically after 30 days.

Completed disclosures purge processing requires a valid VistA account with ROI periodic processing credentials. If the credentials provided to the VIX are invalid, completed disclosures purge processing does not work.

5.1.4. Processing Disclosure Wait Time

The parameter **Processing Disclosure Wait Time** indicates the number of minutes the VIX waits for an ROI disclosure to be in a processing state before resetting the disclosure request. ROI disclosures are processed in several either active or waiting states. If a request stays in an active state beyond the number of minutes specified in this parameter, it is reset to a waiting state to be processed. By default, the wait time to process a work item is 120 minutes. The value should be set to a period that is long enough for a work item to complete but not too long to orphan the ROI disclosure request.

For information about setting ROI Processing credentials, see *ROI Periodic Processing Credentials*.

5.1.5. ROI Periodic Processing Credentials

The ROI periodic processing credentials are the credentials the VIX uses to do periodic processing for ROI. These credentials must be valid VistA credentials with the MAG DICOM and OR CPRS GUI CHART secondary menu (options for the Computerized Patient Record System (CPRS)). The credentials can be the credentials of the same service account that the DICOM Gateway and the HDIG (Hybrid DICOM Gateway) use.

For more information about setting the access and verify codes of the account, see the VIX Installation Guide.

Users with the MAG VIX ADMIN security key can reset the access and verify code of the account through the ROI Processing Status page. For more information about the procedure, see Modifying the ROI Processing Parameters of the VIX.

5.1.6. Alerts About Problems in the ROI Configuration

If the VIX encounters a problem with the ROI processing configuration, for example, if both periodic processing and **Process Disclosure Requests Immediately** are disabled, it displays an alert at the top of the ROI Processing Status page and ROI Configuration page. When there is a message, this means that there is a problem with the current configuration, and you should take action to resolve the issue or issues. For information about the procedure for modifying the ROI processing parameters of the VIX, see *Modifying the ROI Processing Parameters of the VIX*.

5.2. Getting Information About ROI Processing

You can see the status of an ROI request and get information about ROI statistics on the ROI Processing Status page.

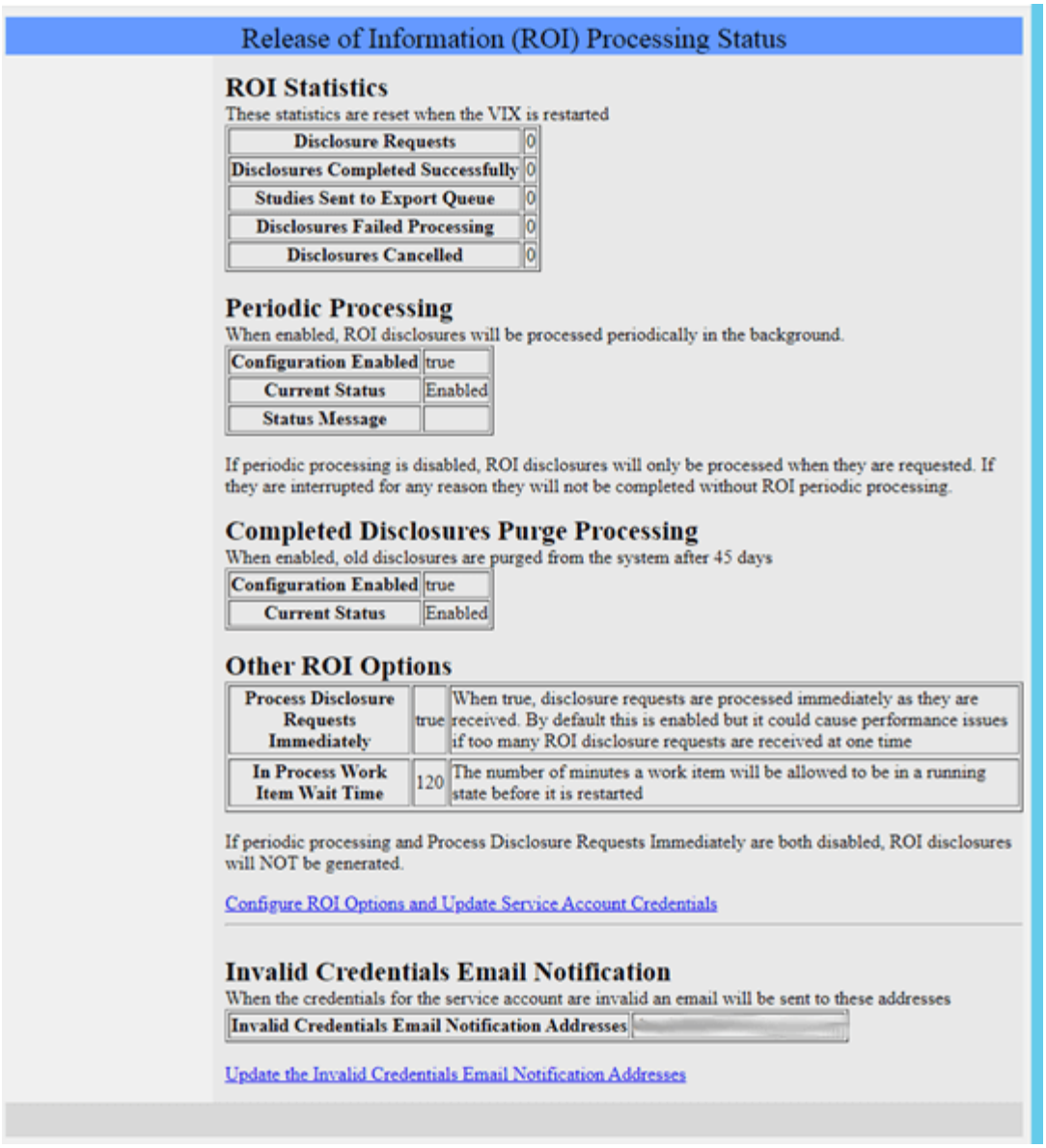
To display the ROI Processing Status page:

In your browser, open the URL for the ROI Processing Status page:
https://*FQDN*:REDACTED/ROIWebApp

where ***FQDN*** is the name of the fully qualified domain name (*FQDN*) of the server on which the VIX is installed.

Figure 10 shows the ROI Processing Status page.

Figure 10: Release of Information (ROI) Status Page



5.2.1. Information the ROI Processing Status Page Provides

The ROI Processing Status page provides statistics about the ROI processing jobs since the last VIX restart. The counters for each field are reset every time the VIX is restarted.

Table 21 explains the information that the VIX provides for ROI processing.

Table 21: ROI Processing Information

Group	Field	Description
ROI Statistics	Disclosure Requests	The number of requests made to the VIX for ROI disclosures.
ROI Statistics	Disclosures Completed Successfully	The number of successfully completed ROI disclosures.
ROI Statistics	Studies Sent to Export Queue	The number of studies sent to the export queue to be processed. A disclosure may contain several studies that are sent to the export queue (among others that may be processed by the VIX).
ROI Statistics	Disclosures Failed Processing	The number of ROI disclosures that did not complete successfully.
ROI Statistics	Disclosures Cancelled	The number of ROI disclosures that were canceled before completion.
Periodic Processing	N/A	When periodic processing is enabled, the VIX processes ROI disclosures in the periodically in the background. Periodic processing requires an account with ROI processing credentials, which is configured when the VIX is installed. For more information about periodic processing, see Periodic Processing of ROI Disclosure Requests.
Periodic Processing	Configuration Enabled	When this parameter is set to true, periodic processing is enabled, and the VIX processes ROI requests periodically in the background.
Periodic Processing	Current Status	Indicates the current status of periodic processing. The values are: Disabled – Indicates that periodic processing is disabled. Enabled – Indicates that periodic processing is enabled and that there is an account with valid ROI processing credentials.

Group	Field	Description
Completed Disclosures Purge Processing	N/A	When completed disclosures purge processing is enabled, the VIX purges old ROI disclosures after the number of days specified in its configuration. Completed disclosures purge processing requires an account with ROI processing credentials. For more information, see Purging Completed Disclosures.
Completed Disclosures Purge Processing	Configuration Enabled	Indicates if completed disclosures purge processing is enabled. When this parameter is set to true, completed disclosures purge processing is enabled.
Completed Disclosures Purge Processing	Current Status	Indicates the current status of completed disclosures purge processing. The values are: Disabled – Indicates that completed disclosures purge processing is disabled. Enabled – Indicates that completed disclosures purge processing is enabled and that there is an account with valid ROI processing credentials.
Other ROI Options	Process Disclosure Requests Immediately	When enabled, the VIX processes ROI disclosures immediately when requested. This option does not require ROI processing credentials. The VIX uses the credentials of the user who submits the ROI request to process the disclosure. For more information, see Processing ROI Disclosure Requests Immediately.
Other ROI Options	In Process Work Item Wait Time	Indicates the number of minutes the VIX waits for an ROI disclosure to be in a processing state before resetting the disclosure request. ROI disclosures are processed in several either active or waiting states. For more information, see Processing Disclosure Wait Time.
Configure ROI Options and Update Service Account Credentials	N/A	To change any of the VIX ROI configuration settings, click on the Configure ROI Options and Update Service Account Credentials link. Accessing this configuration page requires VistA credentials for a user with the MAG VIX ADMIN security key. This page also allows resetting the access and verify codes for the service account of the site's VIX on its local VistA.

Group	Field	Description
Invalid Credentials Email Notification	N/A	To change any of these settings, click on the Configure ROI Options link. This configuration page requires VistA credentials for a user with the MAG VIX ADMIN security key. When the VIX is configured to do periodic processing for ROI or completed disclosures purge processing, it authenticates the ROI processing credentials. If the account credentials are invalid or expired, the VIX sends an email notification of the invalid credentials.
Invalid Credentials Email Notification	Invalid Credentials Email Notification Addresses	The email address or addresses to which the VIX sends an email notification about invalid ROI processing credentials. The value can include multiple email addresses (separated by a comma) and/or an email group. The email comes from the REDACTED email account. The values are specified when the VIX is installed. Users with the MAG VIX ADMIN key can modify these values.
Update the Invalid Credentials Email Notification Addresses	N/A	To change the email addresses to send notifications to click on the Update the Invalid Credentials Email Notification Addresses link. Accessing this page requires VistA credentials for a user with the MAG VIX ADMIN security key.
Alert Messages	N/A	If there is a problem with the VIX ROI processing configuration, the VIX displays a message at the top of the page, indicating that you need to change the configuration to resolve the issue. For more information about the alerts, see Alerts.

5.3. Modifying the ROI Processing and DICOM Query/Retrieve Parameters of the VIX

Users with the MAG VIX ADMIN security key can change the ROI configuration parameters of the VIX and re-set the access and verify codes of the service account of the site's VIX on its local VistA with the ROI periodic processing credentials and DICOM (Q/R) credentials.

To change the ROI processing parameters of the VIX:

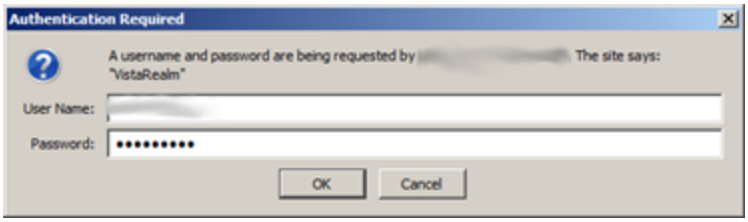
1. In your browser, open the URL for the ROI Statistics page:
   https://*FQDN*:REDACTED/ROIWebApp

   where ***FQDN*** is the name of the ***FQDN*** of the computer on which the VIX is installed.

2. In the ROI Processing Status page, click the link **Configure ROI Options and Update Service Account Credentials**.

3. In the dialog box that displays (Figure 11), enter the access, and verify code of the user with the MAG VIX ADMIN security key. Then, click, **OK**.

Figure 11: Authentication Required



4. In the Configure ROI page, modify the configuration parameters as desired. For information about the parameters, see *Information the ROI Processing Status Page Provides*.
5. Click the **Save Configuration** button to save the changes. The page refreshes with a status message indicating if the changes were saved or if there was an error.
6. To return to the ROI Processing Status page, click on the **ROI Status** link on the left side of the page.

5.4. Changing User List for Get Invalid ROI Credentials Email Notifications

When the VIX encounters a problem with the service account credentials (invalid credentials or expired verify code), it sends an email notification to the address or addresses specified in its configuration. The parameter **Invalid Credentials Email Notification Addresses** specifies the email address or addresses to which the VIX sends an email notification about invalid ROI processing credentials. The value can include multiple email addresses (separated by a comma) and/or an email group.

The email notification for invalid credentials comes from the REDACTED email account. The values of the **Invalid Credentials Email Notification Addresses** are specified when the VIX is installed. Users with the MAG VIX ADMIN key can modify these values.

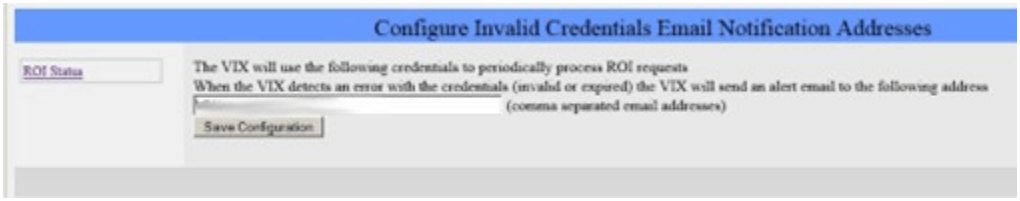
To change the list of email addresses to which the VIX sends notifications about invalid ROI processing credentials:

1. In your browser, open the URL for the ROI Statistics page:
   https://*FQDN*:REDACTED/ROIWebApp

   where ***FQDN*** is the name of the ***FQDN*** of the computer on which the VIX is installed
2. In the ROI Processing Status page, click the link **Update the Invalid Credentials Email Notification Addresses**.
3. In the dialog box that displays (Figure 11), enter the access, and verify code of the user with the MAG VIX ADMIN security key. Then, click **OK**.

4. In the Configure Invalid Credentials Email Notification Addresses page, modify the list of addresses as desired (Figure 12). The list can contain multiple addresses separated by commas and/or an email group.

Figure 12: Configure Invalid Credentials Email



5. Click the **Save Configuration** button to save the changes. The page refreshes with a status message indicating if the changes were saved or if there was an error.
6. To return to the ROI Processing Status page, click on the **ROI Status** link on the left side of the page.

6. VIX Reference/Software Description

6.1. VIX Java Components

The following sections summarize the primary Java components of the VIX.

6.1.1. VIX Servlet Container

The VIX uses an Apache Tomcat-based servlet container to provide the environment used to execute the Java code on the VIX. This servlet container is installed automatically as part of the VIX installation process.

6.1.2. VIX Security Realms

The VIX implements security realms to verify that only properly authenticated applications (Clinical Display, VistARad, and other VIXes) can use the interfaces provided by the VIX Web applications. Authentication is handled silently by the application and the VIX and does not require an explicit login by clinicians requesting images.

6.1.3. VIX Interfaces

The VIX uses a dedicated interface for each outside application that requests and receives data from the VIX.

VIX interfaces are used for both metadata and image retrieval. In general, each VIX interface implements a Web service that handles metadata requests and an image servlet that handles image requests. Table 22 summarizes each VIX interface.

Table 22: VIX Interfaces Description

Interface Name	Description
VistARad interface	Handles metadata and image requests from local VistARad workstations.
Clinical Display interface	Handles metadata and image requests from local Clinical Display workstations.
Federation interface	Handles metadata and image requests from other remote VIXes or the CVIX.
User services interface	Handles user-related functionality such as authentication and security key retrieval.
Patient services interface	Handles patient-related functionality, including patient search and sensitive patient access logging.
Storage services interface	Handles requests related to read and write locations and metadata.
DICOM Importer services interface	Handles application-specific requests for the importer, including study and order metadata, performing create, read, update, and delete (CRUD) operations on work items, dealing with Importer reports, and other related features.

When an interface receives a request, it issues the appropriate command to the VIX core for proper disposition. When the VIX core ultimately provides a response (the requested data), the same interface responds to the requesting application.

6.1.4. VIX Core

The VIX core provides the central switching intelligence for the VIX. It performs the following:

- Examines commands received from all the VIX interfaces.
- Determines which VIX data source is the best one to retrieve the data requested and packages the request appropriately before passing the request to the data source.
- Implements and manages the VIX cache.

6.1.5. VIX Data Sources

The VIX has a dedicated data source for each outside entity from which it retrieves data. Data sources receive requests from and return responses to the VIX core. Table 23 summarizes each VIX data source. These data sources are identified in the Data Source Protocol field in the VIX transaction log.

Table 23: VIX Data Sources Description

Data Source Name	Description
vistaimaging	Retrieves data from a VistA System using RPCs.
vftp	Retrieves data from other VIXes (or the CVIX) using their Federation interfaces.

6.1.6. Java Installation Locations

On the server where the VIX is installed, VIX-related files are stored in the locations described below.

For installation procedures, see the VIX Installation Guide.

6.1.6.1. VIX folders on the System Drive

The following VIX-related folders are on the system drive (usually C:\). Note that because the VIX is a collection of services hosted in a servlet container, most VIX related-files cannot be stored under \Program Files\VistA.

\DCF_Runtime

Laurel Bridge DCF toolkit files

\Program Files\Apache Software Foundation\Tomcat 9.0

Primary application area for the VIX servlet engine and VIX program files. Includes:

\bin – servlet engine executables and Aware JPEG2000 toolkit files

\conf – servlet engine configuration files

\lib – shared servlet engine files, VIX core and data source files, and Aware JPEG2000 toolkit files

\logs – Java and debugging logs

\temp – temporary files

\webapps – VIX Web applications and associated parameter files

\work – servlet engine system files

\Program Files\Java\jre-1.8-431

The runtime environment files and resources for the VIX servlet engine and for VIX Java components.

\Program Files\Vista\Imaging\VixInstaller

VIX installation files and resources.

\VixCertStore

Stores VIX security certificates. For details about security certificates, see the *VIX Security Certificate* section.

6.1.6.2. VIX Folders on the System Drive or a Shared Drive

When the VIX is installed on a standalone server, the following folders can be on either the system drive or on a shared drive at the site's discretion.

\VixCache

This is the primary storage area for images and metadata that the VIX caches. For details about the VIX cache, see *Caching of Metadata and Images*.

\VixConfig

Configuration files used by the VIX Java components and the VIX transaction log.

NOTE: Files in the VixConfig folder are generated as part of the VIX installation process and are regenerated when the VIX is updated.

6.1.7. Java Logs

The active Java logs reside in \Program Files\Apache Software Foundation\Tomcat 9.0\logs on each CVIX server. For active logs, a new instance is generated each day. For older logs, they are retained in the log archive folder named ImagingArchivedLogs with the corresponding drive letter specified during installation.

NOTE: A symbolic link with name ImagingArchivedLogsLink also resides in \Program Files\Apache Software Foundation\Tomcat 9.0\logs. This symbolic link points to the log archive folder named ImagingArchivedLogs with the corresponding drive letter specified during installation.

Older logs are retained with the date appended to their filenames in a zip format and stored in their respective archive folders. Further, older logs exceeding a pre-defined size (default 250 MB) for each day are rolled over and a new file is generated with a number appended to their filenames after the date.

catalina.log: Tomcat (VIX servlet container) output.

host-manager.log: Java host manager application output.

ImagingCache.log: VIX cache output.

ImagingExchangeWebApp.log: VIX interface/web application output.

jakarta_service.log: Windows jakarta service output.

localhost.log: generated but not populated.

manager.log: generated but not populated.

stderr.log: Tomcat service errors.

VistaRealm.log: VIX security realm output.

6.2. VistA/M Information

The following sections describe how a VIX interacts with local and remote VistA systems.

6.2.1. Remote Procedure Calls (RPCs) Used by the VIX

The VIX uses numerous Remote Procedure Calls (RPCs). Most of these RPCs are part of the VistA Imaging (MAG) package and are listed in Table 24. RPCs from other packages are listed in the next section.

Table 24: MAG RPCs used by the VIX

RPC Name	Description
MAG BROKER SECURITY Routine: BSE^MAGS2BSE	Returns a BSE token from BSE XUS SET VISITOR.
MAG DICOM GET HOSP LOCATION Routine: GETLOC^MAGDRPCB	Returns a list of matching hospital locations.
MAG DICOM RADIOLOGY MODIFIERS Routine: MOD^MAGDRPCA	Returns a list of entries from the PROCEDURES MODIFIER file (#71.2) sorted by Radiology Imaging Type.
MAG DICOM RADIOLOGY PROCEDURES Routine: PROC^MAGDRPCA	This RPC returns a list of Radiology Procedures for "no-credit" Imaging locations within a given division. If the division does not have any "no-credit" Imaging locations defined, the results return an error message indicating the problem. Modified by MAG*3.0*118 to – optionally – filter out procedure types Broad and Parent.
MAG DOD GET STUDIES IEN Routine: STUDY2^MAGDQR21	Returns study information based on the IMAGE file (#2005) Internal Entry Number (IEN) of the image group that is provided as a parameter.
MAG DOD GET STUDIES UID Routine: STUDY1^MAGDQR21	Returns study information based on the Study Unique Identifier (UID) that is provided as a parameter.
MAG EVENT AUDIT Routine: EVENT^MAGUAUD	The RPC is used to populate the data dictionaries (tables) introduced in this patch.
MAG GET NETLOC Routine: SHARE^MAGGTU6	Returns a list of all entries in the NETWORK LOCATION file (#2005.2).
MAG IMAGE CURRENT INFO Routine: INFO^MAGDQR04	Returns current values for the various DICOM tags that are to be included in the header of an image.
MAG NEW SOP INSTANCE UID Routine: NEWUID^MAGDRPC9	Generates a new SOP Instance UID for an image and stores the value in the IMAGE file (#2005) if a SOP instance UID is not already present.

RPC Name	Description
MAG3 CPRS TIU NOTE Routine: IMAGES^MAGGNTI	Returns a list of all images for a Text Integration Utility (TIU) document.
MAG4 GET IMAGE INFO Routine: GETINFO^MAGGTU3	Returns specific fields of an image entry for display in the Clinical Display Image Information window.
MAG4 INDEX GET ORIGIN Routine: IGO^MAGSIXGT	This call returns an array of INDEX ORIGIN.
MAG4 PAT GET IMAGES Routine: PGI^MAGSIXG1	Returns a list of image groups from the IMAGE file (#2005) based on filters provided.
MAGG CPRS RAD EXAM Routine: IMAGEC^MAGGTRAI	Returns a list of images for the radiology exam.
MAGG DEV FIELD VALUES Routine: GETS^MAGGTSYS	Returns a list of field values for an IEN in the IMAGE file (#2005).
MAGG GROUP IMAGES Routine: GROUP^MAGGTIG	Returns array of images for a group entry in the IMAGE file (#2005). Included for backward compatibility only.
MAGG INSTALL Routine: GPACHX^MAGQBUT4	Returns a list of all Imaging package installs on the host system.
MAGG LOGOFF Routine: LOGOFF^MAGGTAU	Tracks the time of the Imaging session.
MAGG OFFLINE IMAGE ACCESSED Routine: MAIL^MAGGTU3	Sends a message when there is an attempt to access an image from an offline jukebox platter.
MAGG PAT FIND Routine: FIND^MAGGTPT1	Used for patient lookups.
MAGG PAT INFO Routine: INFO^MAGGTPT1	Returns a string of '^' delimited pieces of patient information.
MAGG PAT PHOTOS Routine: PHOTOS^MAGGTIG	Returns a list of patient photo IDs.
MAGG SYS GLOBAL NODE Routine: MAG^MAGGTSY2	Returns the global node of an IMAGE file (#2005) entry.
MAGG WRKS UPDATES Routine: UPD^MAGGTAU	Starts a new session for image access logging.
MAGGACTION LOG Routine: LOGACT^MAGGTU6	Call to log an action performed on the image. Actions are logged the IMAGE ACCESS LOG file (#2006.95).
MAGGRPT Routine: BRK^MAGGTRPT	Returns associated report for Image IEN.
MAGGUSER2 Routine: USERINF2^MAGGTU3	Returns information about a Clinical Display user.

RPC Name	Description
MAGJ CACHELOCATION Routine: CACHEQ^MAGJUTL3	Obtains the locations for images that have been routed to remote sites/workstations.
MAGJ CPTMATCH Routine: CPTGRP^MAGJUTL4	Finds related radiology procedures based on the matching tables in the MAG RAD CPT MATCHING file (#2006.67).
MAGJ EXAM REPORT Routine: RADRPT^MAGJRPT	Retrieves a radiology report.
MAGJ PT ALL EXAMS Routine: PTLSTALL^MAGJLST1	Retrieves a list of all radiology exams for a selected patient.
MAGJ RADACTIVEEXAMS Routine: ACTIVE^MAGJLS2	Retrieves lists of "unread," "recent," or "all active" radiology exams for VistARad.
MAGJ RADCASEIMAGES Routine: OPENCASE^MAGJEX1	Fetches IMAGE file (#2005) information for all the images for a selected case. If the case's images are on the archive (jukebox), then this RPC initiates a fetch of the image files from the archive.
MAGJ RADORDERDISP Routine: ORD^MAGJRPT	Returns the Detailed Request Display (order) for the radiology exam.
MAGJ STUDY DATA Routine RPCIN^MAGJEX3	Obtains various study and/or image data stored in XML format.
MAGJ USER2 Routine: USERINF2^MAGJUTL3	Returns information about a VistARad user.
MAGJ VIX LOG REMOTE IMG ACCESS Routine: LOGRIA^MAGJVAPI	Logs remote image accesses.
MAGN CPRS IMAGE LIST Routine: IMAGEL^MAGNTRAI	Lists images for Rad Exams or TIU Notes by CPRS context.
MAGV ADD WORK ITEM TAGS Routine: ADDTAG^MAGVIM01	Allows tags to be added to work items in the WORK ITEM (#2006.941) file. Tags consist of a tag name and a tag value. Tags and values can be used to look up entries in the WORK ITEM (#2006.941) file.
MAGV CONFIRM RAD ORDER Routine: CONFIRM^MAGVIM06	Returns a RAD/NUC MED ORDERS file (#75.1) IEN for a set of DICOM Unique Identifiers.
MAGV CREATE WORK ITEM Routine:CRTITEM^MAGVIM01	Creates work item entries in the WORK ITEM file (#2006.94) and the WORK ITEM HISTORY file (#2006.941).
MAGV DELETE WORK ITEM Routine:DELWITEM^MAGVIM01	Deletes a single entry in the WORK ITEM file (#2006.941).
MAGV FIND WORK ITEM Routine:	Returns an array of work items with values that match the parameters provided.

RPC Name	Description
MAGV GET NEXT WORK ITEM Routine:FIND^MAGVIM01	Returns the work item with the oldest LAST UPDATED date/time with the specified expected status and work item type.
MAGV GET PAT ORDERS Routine:GETORD^MAGVIM02	Returns an array of consult or radiology orders for and input patient enterprise identifier.
MAGV GET WORK ITEM Routine: GETITEM^MAGVIM01	Returns all of the data elements for a single entry in the WORK ITEM file (#2006.941).
MAGV GET WORKLISTS Routine: GETLIST^MAGVIM01	Returns a list of all worklist entries in the WORKLIST file (#2006.942). The worklists name and active status are returned in an array.
MAGV IMPORT MEDIA LOG STORE Routine: IMPMEDIA^MAGVIM03	Files data from an Importer III media import event to the MAGV IMPORT MEDIA LOG file (#2006.9422).
MAGV IMPORT STATUS Routine: IMSTATUS^MAGVIM01	Given a set of UIDS, a patient identifier, and an accession number, this remote procedure returns the import status of a matching item.
MAGV IMPORT STUDY LOG REPORT Routine: IMPLOGEX^MAGVIM03	Exports data from the MAGV IMPORT STUDY LOG file (#2006.9421) as formatted reports.
MAGV IMPORT STUDY LOG STORE Routine: IMPLOGIN^MAGVIM03	Collects study-level data for objects imported by the DICOM Importer III.
MAGV RAD EXAM ORDER Routine: XMORDER^MAGVIM05	Wraps a call to the RAMAG EXAM ORDER remote procedure, and re-formats the output for the DICOM Importer III application. Returns the IEN of the new order in the RAD/NUC MED ORDERS file (#75.1), or an array of error messages.
MAGV RAD EXAM REGISTER Routine: XMREGSTR^MAGVIM05	Wraps a call to the RAMAG EXAM REGISTER remote procedure, and re-formats the output for the DICOM Importer III application. Returns the IEN of the new case in the RAD/NUC MED PATIENT file (#70), or an array of error messages.
MAGV RAD STAT COMPLETE Routine: XMCOMPLT^MAGVIM05	Wraps call to code underlying the remote procedure RAMAG EXAM COMPLETE.
MAGV RAD STAT EXAMINED Routine: XMEXAMIN^MAGVIM05	Wraps calls to the remote procedure RAMAG EXAMINED and re-formats the output.
MAGV UPDATE WORK ITEM Routine: UPDITEM^MAGVIM01	Updates a work item in the WORK ITEM file (#2006.94). It also creates an entry in the WORK ITEM HISTORY file (#2006.941).

6.2.2. Non-MAG RPCs used by the VIX

Table 25 lists RPCs from non-MAG packages (i.e., packages other than VistA Imaging) used by the VIX. The use of these RPCs is governed by Integration Control Registrations (ICRs) stored in FORUM. For information about viewing specific ICRs, see Chapter 12 in the VistA Imaging Technical Manual.

Table 25: Non-MAG RPCs used by the VIX

RPC Name	Description
DDR FILER Routine: FILEC^DDR3	Generic call to file edits into a FileMan file.
DG SENSITIVE RECORD ACCESS Routine: PTSEC^DGSEC4	Verifies that a user is not accessing his/her own Patient file record if the RESTRICT PATIENT RECORD ACCESS field (#1201) in the MAS PARAMETERS file (#43) is set to yes and the user does not hold the DG RECORD ACCESS security key. If the parameter is set to yes and the user is not a key holder, a social security number must be defined in the NEW PERSON file (#200) for the user to access any Patient file (#2) record.
DG SENSITIVE RECORD BULLETIN Routine: NOTICE^DGSEC4	Adds an entry to the DG Security Log file (#38.1) and generates the sensitive record access bulletin depending on the value in the ACTION input parameter.
PSB GETPROVIDER Routine: PROVLST^PSBRPCMO	Used to get a list of active providers.
VAFCTFU CONVERT ICN TO DFN Routine: GETDFN^VAFCTFU1	Given a patient ICN, this returns the patient's Internal Entry Number (IEN) from the PATIENT file (#2).
VAFCTFU GET TREATING LIST Routine: TFL^VAFCTFU1	Given a patient Data File Number (DFN), this returns a list of treating facilities.
XUS AV CODE Routine: VALIDAV^XUSRB	Checks to see whether an ACCESS/VERIFY code pair is valid.
XUS DIVISION GET Routine: DIVGET^XUSRB2	Returns a list of divisions of a user.
XUS DIVISION SET Routine: DIVSET^XUSRB2	Sets the user's selected division in Designated User (DUZ)(2) during sign-on.
XUS ESSO VALIDATE Routine: ESSO^XUESSO4	Verifies that a provided Identity and Access Management (IAM) Secure Token Service (STS) authentication token is valid.
XUS SIGNON SETUP Routine: SETUP^XUSRB	Establishes the environment necessary for DHCP sign-on.
XWB CREATE CONTEXT Routine: CRCONTXT^XWBSEC	Establishes context on the server that the Broker checks before executing any other remote procedure.
XWB GET VARIABLE VALUE Routine: VARVAL^XWBLIB	Accepts the name of a variable to return its value to the caller.

6.2.3. Database Information

The VIX retrieves data from both local and remote VistA databases using the RPCs described in the previous sections.

The VIX writes data to VistA if it needs to update the following:

- IMAGE ACCESS LOG file (#2006.95). See *Logging on VistA.*
- IMAGE file (#2005) with SOP instance UIDs for images that do not have SOP instance UIDs already. The VIX uses the MAG NEW SOP INSTANCE UID RPC used by other Imaging components for the same purpose.

There are no general VIX parameters stored on VistA. Any site-specific VIX parameters are set during installation and are stored in the local configuration files of the VIX.

6.2.4. Exported Menu Options

There are no exported VistA menu options associated with the VIX.

6.2.5. Security Keys

The VIX uses the MAG VIX ADMIN security key to determine who can access the VIX transaction log. See *Using the VIX Transaction* Log for more information.

When a Clinical Display, Image Viewer, or VistARad user uses the VIX to access remote VA images, their locally assigned security keys are honored on the remote VistA system. VistARad and Clinical Display security keys are described in the VistA Imaging Technical Manual.

6.2.6. User Accounts

When a VA clinician retrieves metadata or images from a remote VA site via a VIX, their VistA account information is used to automatically log into the remote VA site. Users do not need to explicitly enter access or verify codes.

When a DoD clinician retrieves metadata or images from a VA site, the credentialing is handled by the Station 200 VistA system co-located with the CVIX. If a local service account was established for the initial VIX implementation (MAG*3.0*83), that account is no longer needed after updating to the most recent VIX.

A DoD clinician's requests for local images are logged at the site where the images reside. See *Image Sharing-related Logging* for details.

6.3. Other VIX Components

The VIX incorporates the following additional components.

- *Security certificate*
- *.NET*
- *Apache Tomcat*
- *Sun JRE*
- *Laurel Bridge DCF toolkit*

- *Aware JPEG2000 toolkit*
- *LibreOffice*

Each component is described in the following sections. All of these components are integral to VIX operations and cannot be modified without impacting VIX operations.

6.3.1. VIX Security Certificate

When a VIX communicates with another VIX, they exchange security certificates for authentication purposes. This long-term security certificate is stored in the \VixCertStore directory on the server where the VIX is installed.

The VIX security certificate is provided as a part of the VIX installation process and must be available to complete a VIX installation.

6.3.2. .NET

The .NET 4.8.X framework is needed to install, update, and run the VIX software.

Patches for .NET 4.8.X, if any, should be installed as soon as reasonably possible after they are released in accordance with local site maintenance policies and the Windows update guidelines documented in the VistA Imaging Technical Manual.

Other versions of .NET have no impact on the VIX installer or update processes and can be installed or not in accordance with local policy.

6.3.3. Apache Tomcat

The VIX's servlet container and the VIX itself require Apache Tomcat. The VIX Installation automatically installs Tomcat.

Do not install later versions of Tomcat. The VIX installation software bundles the correct version for the VIX.

6.3.4. Java Runtime Environment (JRE)

The VIX's servlet container and the VIX itself require the Oracle Java Runtime Environment (JRE). The JRE is installed automatically as a part of the VIX installation process.

Do not install later versions of the JRE. The correct JRE for the VIX is bundled with the VIX installation software.

6.3.5. Laurel Bridge DCF Toolkit

The Laurel Bridge DCF toolkit, version 3.3.68c, is a third-party toolkit that VIX uses to convert images to and from DICOM format.

The license for this toolkit is tied to the server where the VIX is installed. Shifting to a new server requires an updated license from Laurel Bridge. If a new or updated license is needed, contact the REDACTED mail group.

Version 3.3.68c of this toolkit is bundled with the VIX installer and is installed automatically as part of the VIX setup process. Do not install this toolkit manually.

6.3.6. Aware JPEG2000 Toolkit License

For information regarding the Aware Toolkit License, see the VIX Installation Guide.

6.3.7. LibreOffice

The VIX requires the install of LibreOffice 24.2.5, a third-party open-source office productivity software suite, to support Rich Text Format (RTF) files. The VIX Installation automatically installs LibreOffice.

7. Configure MUSE Functionality

Configuring the MUSE functionality is performed as part of the VIX Installation, see the VIX Installation Guide. This section provides details in the event the MUSE functionality needs to be further enabled or configured. Configuration of the MUSE interface will require the value of the MUSE host, the value of the MUSE username, the password for the MUSE, the MUSE port, and the MUSE protocol for the site's online MUSE server. If the MUSE username and password are not documented in existing site VistA Imaging documentation, please contact the local BioMed team or MUSE administrator for the information.

Has the MUSE functionality already been configured to be enabled?

- To determine if MUSE functionality is already configured to be enabled, open the MuseDataSource-1.0.Config file located in C:\VixConfig. Run, Notepad, Notepad++, or WordPad as an administrator and then open the file.
    - **No, it is not enabled**. If the MuseDataSource-1.0.Config file located in C:\VixConfig is similar to the template displayed in Figure 13, continue with this section to perform the steps to enable MUSE functionality.
    - **Yes, it is enabled.** If the MuseDataSource-1.0.Config file located in C:\VixConfig is not similar to the template displayed in Figure 13 (i.e. a real MUSE site number, host, username, password, port, and protocol are present), the MUSE functionality is already enabled. There is no reason to perform this section unless reconfiguring or modifying additional configuration options.

NOTE: It is expected that the site administrator is aware of all needed entries in the MUSE configuration, including `museSiteNumber`, `host`, `username`, `password`, `port`, and `protocol`. One method to obtain the values of `museSiteNumber`, `host`, `port` and `username` is ***from the Background Processor (discussed below in this step)*** If the `password` is not documented in existing site VistA Imaging documentation or if *not* available, please contact the local BioMed team or MUSE administrator.

By default, the MuseDataSource-1.0.Config file is located in C:\VixConfig. Open the MuseDataSource-1.0.Config file. Run Notepad, Notepad++, or WordPad as an administrator and then open the MuseDataSource-1.0.Config file (Figure 13):

Figure 13: Sample MuseDataSource-1.0.Config File for One Server (MUSE ENABLED FOR JLV VIX Image Viewer)

```
<gov.va.med.imaging.musedatasource.configuration.MuseConfiguration>
  <servers>
    <gov.va.med.imaging.musedatasource.configuration.MuseServerConfiguration>
      <id>0</id>
      <museSiteNumber>***MUSE SITE NUMBER HERE***</museSiteNumber>
      <host>***MUSE HOST HERE***</host>
      <port>    </port>
      <metadataTimeoutMs>60000</metadataTimeoutMs>
      <username>***MUSE USER HERE***</username>
      <password>***MUSE PASSWORD HERE***</password>
      <protocol>http</protocol>
      <museDisabled>false</museDisabled>
    </gov.va.med.imaging.musedatasource.configuration.MuseServerConfiguration>
  </servers>
  <museAPIKey>***MUSE API KEY HERE***</museAPIKey>
  <museApplicationName>MUSEAPIREST</museApplicationName>
  <musePatientFilterRegularExpression>000(-*)0(-*).*</musePatientFilterRegularExpression>
  <preExpirationMinutes>2</preExpirationMinutes>
  <expirationDateFormat>yyyy-MM-dd&apos;T&apos;HHmmss.nZ</expirationDateFormat>
  <enableSessionCache>true</enableSessionCache>
</gov.va.med.imaging.musedatasource.configuration.MuseConfiguration>
```

The MuseDataSource-1.0.Config file allows for modification of the default values with those for the site:

1. `<museSiteNumber>**MUSE SITE NUMBER HERE**</museSiteNumber>`
   With the <museSiteNumber> tag, enter the MUSE site number of the MUSE server that contains EKGs for your facility.
2. `<host>**MUSE HOST HERE**</host>`
   With the <host> tag, enter the MUSE host.
3. `<port>REDACTED</host>`
   With in the <port> tag, enter the MUSE port.
4. `<username>**MUSE USER HERE**</username>`
   Within the <username> tag, enter the MUSE username.
5. `<password>**MUSE PWD HERE**</password>`
   Within the <password> tag, enter the MUSE password obtained from existing site VistA Imaging documentation (if not available, please contact the local BioMed team or MUSE administrator).
6. `<protocol>http</protocol>`
   Within the <protocol> tag, change the protocol.
7. `<museDisabled>false</museDisabled>`
   Verify with the <museDisabled> tag, false is entered if the MUSE is enabled.

NOTE: The default standard MUSE port is REDACTED and protocol is http. The default MUSE™ NX port is REDACTED and protocol is https.

The MuseDataSource-1.0.Config file allows for modification of additional configuration options:

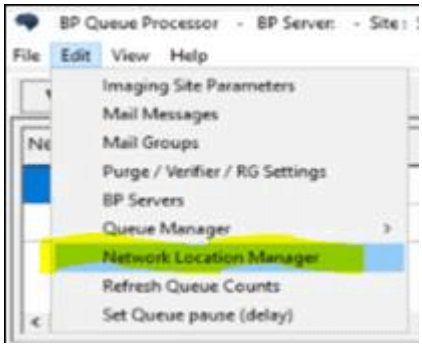
1. `<preExpirationMinutes>2</preExpirationMinutes>`
   Set the value for the time of expiration of the MUSE session in minutes of how long before the MUSE's own session timeouts before the VIX expires cached sessions.
2. `<expirationDateFormat> yyyy-MM-dd'T'HHmmss.nZ< </expirationDateFormat>`
   Specify the date format to support the expiration time of the session.
   NOTE: The default setting of yyyy-MM-dd'T'HHmmss.nZ corresponds to yyyy-MM-dd'T'HHmmss.nZ where the ' renders as ‘ in XML.
3. `<enableSessionCache> true</enableSessionCache>`
   Insert the value true or false, to turn on or off, respectively, MUSE session caching.

Save the MuseDataSource-1.0.Config file if updating entries.

One of the methods identified to obtain the values of `museSiteNumber, host, port,` and `username` is from Background Processor (BP) Queue Processor. For more information on the Background Processor, please see the *VistA Imaging System Background Processor User Manual*. If the site is running the BP Queue processor, use the below steps to obtain the values of `museSiteNumber`, `host`, and `username`.

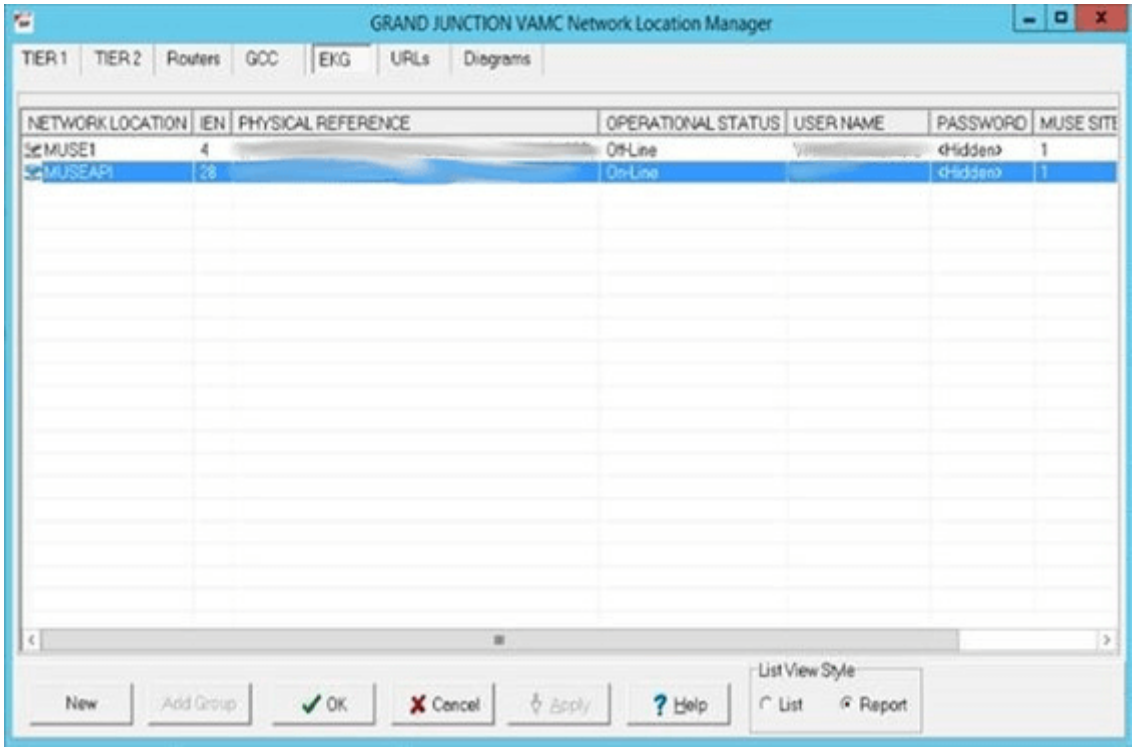
1. From the Background Processor Queue Processor (Figure 14) menu bar, select **Edit** > **Network Location Manager** to open the Network Location Manager window.

Figure 14: BP Queue Processor



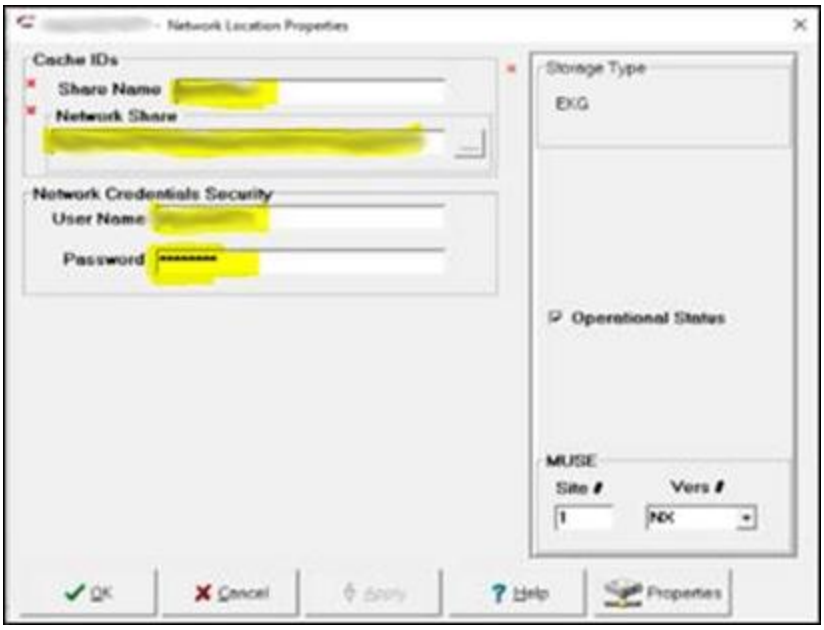
2. Click on the EKG tab in the Network Location Manager window. A listing of the network location of available MUSE servers will appear (Figure 15).
   NOTE: Pay attention to the Operational Status of available MUSE servers. Only add the MUSE server that is **On-Line and contains EKGs of the local site**.

Figure 15: EKG Tab in Network Location Manager in BP Queue Processor



3. To obtain details for a MUSE server, right-click on the server and run **Properties** to launch Network Location Properties. The network share and username for that MUSE server displays (Figure 16).
4. Use the details from the Network Location Properties tab in the BP Queue Processor to obtain the <museSiteNumber>, <host>, <port>, and <username> entries for the MuseDataSource-1.0.Config file.

Figure 16: Network Location Properties in BP Queue Processor



Under the "Storage Type" on the right side (Figure 16), the MUSE site number for the <museSiteNumber> entry is listed under "Site #" under "MUSE". The Fully Qualified Domain Name of the Server for the <host> entry is listed under "Network Share" between \\ and \ The port number (with \ before and after) for the <port> entry is appended to the Fully Qualified Domain Name. The MUSE Site Username for the <username> entry displays under "User Name" under "Network Credentials Security".

Once inside the file, MuseDataSource-1.0.Config, if a manual edit is required, note the entries for the <museSiteNumber>, <host>, <username>, and <port> and update them with the information for the MUSE server that is Operational. The parameter line for <password> with the MUSE site password must be manually added and can be obtained from the existing site VistA Imaging documentation (if not available, obtain the MUSE site password from the local BioMed team or MUSE administrator). After updating the MUSE config file, MuseDataSource-1.0.Config, as described above, save the file and restart the Apache Tomcat service, VIX Viewer service, and VIX Render service. One way to restart the VIX services this can be performed is by executing the restart script (Restart_VIX_Services.ps1) as described in the VIX Installation Guide.

NOTE: If using MUSE™ NX, under the "Storage Type" on the right side the Network Location Properties tab in the BP Queue Processor, "NX" is selected under the "Vers #".

8. Configure DICOM Service Class Provider (SCP) Functionality

This section provides details on the DICOM Service Class Provider (SCP) configuration. The DICOM SCP enables Commercial PACS and various query retrieve devices at VA facilities, and NilRead™ or other query retrieve devices at DoD facilities, to get remote VistA images through the use of DICOM C-FIND and C-MOVE.

Henceforth, this section refers to the Commercial PACS, NilRead™, and query retrieve devices as a DICOM SCP client.

NOTE: Commercial PACS is for VIX, but CVIX also has the capability to provide data to NilRead™ to read, as the protocol used is the same; however, other query retrieve devices can also be used.

Application Entity (AE) Titles Configuration must be performed manually after VIX Installation and a Tomcat restart performed after completed. The VIX install performs some of the configuration for the DICOM SCP automatically with reasonable defaults and predefined entries. Reasonable defaults and predefined entries include the configurations described in *Tomcat DICOM SCP Configuration* and *Laurel Bridge DICOM SCP Configuration*. If specific configuration values are desired instead of the reasonable defaults, then after updating and saving the configuration file, a Tomcat restart must be completed.

NOTE: For additional installations and/or subsequent patch releases, no additional changes to the *Application Entity (AE) Titles Configuration* are necessary unless the settings configured have changed and an update is needed.

NOTE: To update access and verify codes for the account with VistA credentials, plain text versions can be entered directly into the configuration file and are encrypted after restarting the Apache Tomcat service. One way this restart can be performed is by executing the restart script (Restart_VIX_Services.ps1) as described in the VIX Installation Guide. The access and verify codes can also be updated as described in section 5.3 Modifying the ROI Processing and DICOM Query/Retrieve Parameters of the VIX in this VIX Administration Guide or with a reconfigure installation described in the VIX Installation Guide and in the section “Using the VIX Installation Wizard to Reconfigure the VIX,” to perform a reconfigure installation.

8.1. Application Entity (AE) Titles Configuration

This section describes both the calling and called Application Entity (AE) Titles that must both be configured for DICOM SCP to work. It is necessary to configure both the AE Titles on the VIX server with those of the DICOM SCP client and also to configure the AE Titles on the DICOM SCP client with those of the VIX server.

NOTE: The port for the host for DICOM SCP must be configured as a bi-directional open port in any firewall.

8.1.1. Laurel Bridge AE Titles Configuration on VIX

The mapping of external AE Titles to Transmission Control Protocol/Internet Protocol (TCP/IP) addresses and ports is configurable and set at the time of installation by installation/administration personnel on the VIX server. This mapping is necessary for resolving

the IP address and port of C-MOVE Destination AE and must be correctly configured for the Laurel Bridge SCP AE to correctly function as a C-MOVE SCP.

This section describes how to configure the AE Titles configuration file ae_title_mappings located in the folders cfg\dicom within the Laurel Bridge installation directory (C:\DCF_RunTime_x64\cfg\dicom by default).

Open the ae_title_mappings file to perform edits. Run Notepad, Notepad++, or WordPad as an administrator and then open the file.

For each DICOM SCP client, the AE Title name and its host/port attributes must be set. For each DICOM SCP client, update the following entries for the AE Titles configuration file (refer to Figure 17 for line numbers):

1. Set the IP address for the host for the DICOM SCP client (after host = - line 11).
2. Set the port for the DICOM SCP client where the DICOM SCP is used for the C-STORE operation (after port = - line 12).
3. Set the AE Title the DICOM SCP client is using to communicate with the DICOM SCP (calling AE) (inside [ ] - line 10 and after ae_title = - line 13).

Ensure that each of these lines is uncommented (i.e. remove the # at the front of the line if present). Save the ae_title_mappings file after updating the entries.

Figure 17: AE Titles Configuration File (Template)

```
1  #
2  # VistA Imaging map between an Application Entity Title and a full address
3  # i.e. host:port:called-ae-title
4  #
5  # [ **Insert AE Title the Commercial PACS client is using to communicate with the DICOM SCP** ]
6  # host = **Insert IP Address for the host for the Commercial PACS client**
7  # port = **Insert port for the Commercial PACS client where the DICOM SCP is used for the C-STORE operation**
8  # ae_title = **Insert AE Title the Commercial PACS client is using to communicate with the DICOM SCP**
9
10 [ **Insert AE Title the Commercial PACS client is using to communicate with the DICOM SCP** ]
11 host = **Insert IP Address for the host for the Commercial PACS client**
12 port = **Insert port for the Commercial PACS client where the DICOM SCP is used for the C-STORE operation**
13 ae_title = **Insert AE Title the Commercial PACS client is using to communicate with the DICOM SCP**
14
```

An example of the ae_title_mappings file updated for one DICOM SCP client is shown in Figure 18.

NOTE: The example in Figure 18 for configuration of one DICOM SCP client is not how an actual VIX site's ae_title_mappings file is to be configured. This example is for illustrative purposes only.

Figure 18: AE Titles Configuration File (Example)

```
1  #
2  # VistA Imaging map between an Application Entity Title and a full address
3  # i.e. host:port:called-ae-title
4  #
5  # [ **Insert AE Title the Commercial PACS client is using to communicate with the DICOM SCP** ]
6  # host = **Insert IP Address for the host for the Commercial PACS client**
7  # port = **Insert port for the Commercial PACS client where the DICOM SCP is used for the C-STORE operation**
8  # ae_title = **Insert AE Title the Commercial PACS client is using to communicate with the DICOM SCP**
9
10 [
11 host =
12 port =
13 ae_title =
14
```

For each additional DICOM SCP client, similarly, add lines for the host, port, and ae_title with the correct values as new lines below the prior lines for the prior DICOM SCP client (Figure 19). Save the ae_title_mappings file after updating the entries.

Figure 19: AE Titles Configuration File w/ Multiple DICOM SCP clients (Example)

```
#
# VistA Imaging map between an Application Entity Title and a full address
# i.e. host:port:called-ae-title
#
# [ **Insert AE Title the Commercial PACS client is using to communicate with the DICOM SCP** ]
# host = **Insert IP Address for the host for the Commercial PACS client**
# port = **Insert port for the Commercial PACS client where the DICOM SCP is used for the C-STORE operation**
# ae_title = **Insert AE Title the Commercial PACS client is using to communicate with the DICOM SCP**

[ **Insert AE Title the 1st Commercial PACS client is using to communicate with the DICOM SCP** ]
host = **Insert IP Address for the host for the 1st Commercial PACS client**
port = **Insert port for the 1st Commercial PACS client where the DICOM SCP is used for the C-STORE operation**
ae_title = **Insert AE Title the 1st Commercial PACS client is using to communicate with the DICOM SCP**

[ **Insert AE Title the 2nd Commercial PACS client is using to communicate with the DICOM SCP** ]
host = **Insert IP Address for the host for the 2nd Commercial PACS client**
port = **Insert port for the 2nd Commercial PACS client where the DICOM SCP is used for the C-STORE operation**
ae_title = **Insert AE Title the 2nd Commercial PACS client is using to communicate with the DICOM SCP**

```

After updating the ae_title_mappings file, as described above, it is necessary to restart the Apache Tomcat service. One way this can be performed is by executing the restart script (Restart_VIX_Services.ps1) as described in the VIX Installation Guide.

8.1.2. AE Titles Configuration on DICOM Service Class User (SCU)

This section describes the AE Titles configuration on the DICOM Service Class User (SCU). Installation/administration personnel on the VIX server might not be able to perform this configuration and, in which case, must provide the necessary information to the DICOM SCU administration personnel to perform.

The following three pieces of information are needed for the configuration of the DICOM SCU Client: 1) the IP address for the host for the VIX server, 2) the port of DICOM SCP on the VIX server, and 3) the AE Title of DICOM SCP (called AE).

Many different DICOM SCU vendors exist and each of these systems has their own distinct approach for configuration. If additional information regarding specifics of configuring the DICOM SCU is needed, please reach out to its vendor or consult its documentation.

8.2. Tomcat DICOM SCP Configuration

This section provides details on the ScpConfiguration.Config file located in C:\VixConfig. To update access and verify codes for the account with VistA credentials, plain text versions can be entered directly into the configuration file and are encrypted after restarting the Apache Tomcat service. One way this restart can be performed is by executing the restart script (Restart_VIX_Services.ps1) as described in the VIX Installation Guide. The access and verify codes can also be updated as described in section 5.3 Modifying the ROI Processing and DICOM Query/Retrieve Parameters of the VIX in this VIX Administration Guide or with a reconfigure installation described in the VIX Installation Guide and in the section “Using the VIX Installation Wizard to Reconfigure the VIX,” to perform a reconfigure installation.

NOTE: Tomcat hosts the DICOM SCP, and the DICOM SCP uses the Laurel Bridge library. Refer to the *Laurel Bridge AE Titles Configuration on VIX* to configure the ae_title_mappings file which contains the AE Title and port to trust for DICOM SCP.

The VIX install performs some of the configuration for the DICOM SCP automatically with reasonable defaults and predefined entries. Update two entries in the ScpConfiguration.Config file located in C:\VixConfig to configure the DICOM SCP. Run Notepad, Notepad++, or WordPad as an administrator and then open the file.

Update two entries in the ScpConfiguration.Config file located in C:\VixConfig to configure the DICOM SCP. Run Notepad, Notepad++, or WordPad as an administrator and then open the file.

Update the following entries for the DICOM SCP functionality (refer to Figure 20 for line numbers):

1. Set the DICOM SCU calling AE title, inside opening and closing aeTitle tags (inside <aeTitle> </aeTitle> - line 22). Change the value from the default setting of ALL.
2. Set the DICOM SCU IP address inside the opening and closing callingAeIp tags (inside <callingAeIp> </callingAeIp> - line 23). Change the value from the default setting of 0.0.0.0.

Figure 20: DICOM SCP Configuration File (Template)

```
1  <gov.va.med.imaging.facade.configuration.ScpConfiguration>
2    <dirty>false</dirty>
3    <accessCode>[redacted]</accessCode>
4    <verifyCode>[redacted]/verifyCode>
5    <siteFetchTPoolMax>20</siteFetchTPoolMax>
6    <siteFetchTimeLimit>45</siteFetchTimeLimit>
7    <imageFetchTPoolMax>15</imageFetchTPoolMax>
8    <imageFetchTimeLimit>1000000</imageFetchTimeLimit>
9    <useRemoteImageFetch>true</useRemoteImageFetch>
10   <useDirectFetch>true</useDirectFetch>
11   <cacheLifespan>1</cacheLifespan>
12   <preFetchSeries>true</preFetchSeries>
13   <calledAETitle>ANY_0.0.0.0</calledAETitle>
14   <imageQueueSize>10000</imageQueueSize>
15   <cacheMetaHoursToLive>24</cacheMetaHoursToLive>
16   <isFdtEnabled>true</isFdtEnabled>
17   <fdtPort>[redacted]</fdtPort>
18   <isGenRptFromImage>true</isGenRptFromImage>
19   <useP34>true</useP34>
20   <callingAEConfigs>
21     <gov.va.med.imaging.facade.configuration.ScpCallingAE>
22       <aeTitle>ALL/aeTitle>
23       <callingAeIp>0.0.0.0</callingAeIp>
24       <buildReport>SC</buildReport>
25       <returnQueryLevel>false</returnQueryLevel>
26       <studyQueryFilter>radiology</studyQueryFilter>
27       <sendKeepAlive>false</sendKeepAlive>
28       <useMultiAssociations>false<useMultiAssociations>
29       <cstoreTPoolMax>3</cstoreTPoolMax>
30       <remotePatientResolution>true</remotePatientResolution>
31       <modalityBlockList>
32         <gov.va.med.imaging.facade.configuration.ScpModalityList>
33           <dataSource>ALL</dataSource>
34           <addImageLevelFilter>false</addImageLevelFilter>
35           <modalities>
36             <string>none</string>
37           </modalities>
38         </gov.va.med.imaging.facade.configuration.ScpModalityList>
39       </modalityBlockList>
40       <siteCodeBlackList>
41         <string>100</string>
42         <string>200CLMS</string>
43         <string>200CORP</string>
44         <string>741</string>
45       </siteCodeBlackList>
46       <sopClassBlackList>
47         <string>1.2.840.10008.5.1.4.1.1.66</string>
48       <sopClassBlacklist>
49     </gov.va.med.imaging.facade.configuration.ScpCallingAE>
50   </callingAEConfigs>
51 </gov.va.med.imaging.facade.configuration.ScpConfiguration>
```

An example of the ScpConfiguration.Config file updated for one DICOM SCP client is shown in Figure 21.

NOTE: The example in Figure 21 for configuration of the aeTitle and callingAeIp is not how an actual VIX site's ScpConfiguration.Config file is to be configured. This example is for illustrative purposes only.

Figure 21: ScpConfiguration Configuration File (Example)

```
<gov.va.med.imaging.facade.configuration.ScpConfiguration>
  <dirty>false</dirty>
  <accessCode>[redacted]</accessCode>
  <verifyCode>[redacted]</verifyCode>
  <siteFetchTPoolMax>20</siteFetchTPoolMax>
  <siteFetchTimeLimit>45</siteFetchTimeLimit>
  <imageFetchTPoolMax>15</imageFetchTPoolMax>
  <imageFetchTimeLimit>1000000</imageFetchTimeLimit>
  <useRemoteImageFetch>true</useRemoteImageFetch>
  <useDirectFetch>true</useDirectFetch>
  <cacheLifespan>1</cacheLifespan>
  <preFetchSeries>true</preFetchSeries>
  <calledAETitle>ANY_0.0.0.0</calledAETitle>
  <imageQueueSize>10000</imageQueueSize>
  <cacheMetaHoursToLive>24</cacheMetaHoursToLive>
  <isFdtEnabled>true</isFdtEnabled>
  <fdtPort>[redacted]</fdtPort>
  <isGenRptFromImage>true</isGenRptFromImage>
  <useP34>true</useP34>
  <callingAEConfigs>
    <gov.va.med.imaging.facade.configuration.ScpCallingAE>
      <aeTitle>[redacted]aeTitle>
      <callingAeIp>[redacted]</callingAeIp>
      <buildReport>SC</buildReport>
      <returnQueryLevel>false</returnQueryLevel>
      <studyQueryFilter>radiology</studyQueryFilter>
      <sendKeepAlive>false</sendKeepAlive>
      <useMultiAssociations>false<useMultiAssociations>
      <cstoreTPoolMax>3</cstoreTPoolMax>
      <remotePatientResolution>true</remotePatientResolution>
      <modalityBlockList>
        <gov.va.med.imaging.facade.configuration.ScpModalityList>
          <dataSource>ALL</dataSource>
          <addImageLevelFilter>false</addImageLevelFilter>
          <modalities>
            <string>none</string>
          </modalities>
        </gov.va.med.imaging.facade.configuration.ScpModalityList>
      </modalityBlockList>
      <siteCodeBlackList>
        <string>100</string>
        <string>200CLMS</string>
        <string>200CORP</string>
        <string>741</string>
      </siteCodeBlackList>
      <sopClassBlackList>
        <string>1.2.840.10008.5.1.4.1.1.66</string>
      <sopClassBlacklist>
    </gov.va.med.imaging.facade.configuration.ScpCallingAE>
  </callingAEConfigs>
</gov.va.med.imaging.facade.configuration.ScpConfiguration>
```

Update the following entries for desired DICOM SCP functionality desired beyond the reasonable defaults that are pre-populated (refer to Figure 22 for line numbers):

1. Set the access code for the account with VistA credentials (inside <accessCode> </accessCode > - line 3). A plain text version can be entered and will be encrypted after Tomcat restart.
2. Set the verify code for the account with VistA credentials (inside <verifyCode> </verifyCode > - line 4). A plain text version can be entered and will be encrypted after Tomcat restart.
3. Set the entry for the maximum thread pool size for simultaneous VIX site fetching (inside <siteFetchTPoolMax> </siteFetchTPoolMax> - line 5). The default setting is to fetch from at most 20 VIX sites at the same time.
4. Set the entry for the maximum time to wait for fetching from the VIX site. If the thread does not finish within this maximum time the C-FIND will not count the studies from that VIX site in the response (inside <siteFetchTimeLimit> </siteFetchTimeLimit> - line 6). The fetching thread continues if it is not finished within the time limit. If the fetching is finally successful, the user may re-initiate the C-FIND search and the studies from that site will be counted. The default setting is set to 45 seconds. Depending on the DICOM SCU server settings, this setting may be adjusted to a time the DICOM SCU is willing to wait.
5. Set the entry for the maximum thread pool size for simultaneous image fetching through the local ImageWebApp (inside <imageFetchTPoolMax> </imageFetchTPoolMax> - line 7). The default setting is to fetch from at most 15 images at the same time.
6. Set the entry for the maximum time to wait for fetching the images. (inside <imageFetchTimeLimit> </imageFetchTimeLimit> - line 8). The default setting is set to 1,000,000 seconds. Since the default maximum time to wait for fetching the images is longer than one day, there is no effective limit due to the nightly server restart.
7. Set the value to true or false to use the remote image service (true) or the local image service (false) (inside <useRemoteImageFetch> </useRemoteImageFetch> - line 9). The default setting is set to true.
8. Set the value to true or false to use direct image fetch (inside <useDirectFetch> </useDirectFetch > - line 10). The default setting is set to true which retrieves the file paths for the images from the remote VistA and retrieves the images directly from the Server Message Block (SMB) storage. If set to false, direct image fetch is not used.
9. Each time a user makes a query for a patient (C-FIND), the query information (patient ID) and the study metadata is stored in memory cache for future reference by subsequent series queries and image retrieval (C-MOVE). Set the entry for the cache retention period of how long (in hours) this query information and study metadata is stored in memory (inside <cacheLifespan> </cacheLifespan> - line 11). If 0 is entered, the entries are kept indefinitely in memory or until the next Apache Tomcat service restart.
10. Set the value to true or false for if the C-FIND operation, when querying for studies, also caches the list of studies series metadata in the background (<preFetchSeries> </preFetchSeries>) - line 12.
11. If desired to set allowed AE Titles for the C-FIND caller called AE that it is calling, inside the opening and closing calledAETitle tags (line 13), insert the AE Title of

DICOM SCP (called AE) followed by an underscore (_) followed by the IP address for the host for the VIX server.

12. Set the entry for the maximum number of images able to be queued to download at once (inside <imageQueueSize> </imageQueueSize> - line 14). The default setting is to 10,000 images.
13. Set the entry for the number of hours cached metadata is considered valid (metadata older than this time can be overwritten) (inside <cacheMetaHoursToLive> </cacheMetaHoursToLive> - line 15). The default setting is to 24 hours.
14. If desired to enable fast data transfer set isFdtEnabled to true inside the opening and closing isFdtEnabled tags, otherwise set false (inside <isFdtEnabled> </isFdtEnabled> - line 16). The default setting is true.
15. If desired to change the port for fast data transfer set the port inside the opening and closing fdtPort tags (inside <fdtPort> </fdtPort> - line 17). The default port is 2762.

    NOTE: The selected port for fast data transfer must be visible to other VIX across the VA.
16. Set the parameter isGenRptFromImage to reference the first downloaded DICOM image for certain headers (set to true) or the equivalent data in VistA for the report (set to false) (inside <isGenRptFromImage> </isGenRptFromImage> - line 18). The default is true.
17. If desired to return patch 34 SOP class images from studies set useP34 to true inside the opening and closing useP34 tags, otherwise set false (inside <useP34> </useP34> - line 19). The default setting is true.
18. If desired to see the VA reports as Secondary Capture images, set buildReport to SC inside the opening and closing buildReport tagNs (inside <buildReport> </buildReport> - line 24). To see VA reports as Structured Reports, set buildReport to SR inside the opening and closing buildReport tags (inside <buildReport> </buildReport> - line 24). To turn off VA report generation, set buildReport to NONE inside the opening and closing buildReport tags (inside <buildReport> </buildReport> - line 24).
19. If desired to return study query level in C-FIND responses set returnQueryLevel to true inside the opening and closing returnQueryLevel tags, otherwise set false (inside <returnQueryLevel> </returnQueryLevel> - line 25).
20. The default setting for studyQueryFilter is radiology inside the opening and closing studyQueryFilter tags (inside <studyQueryFilter> </studyQueryFilter> - line 26).

    Radiology includes all DICOM exams with some exceptions. The setting for studyQueryFilter can be changed to all or one of the following specializations which are mapped to VA-specific modalities: cl_cardiology, cl_dermatology, cl_dicom, cl_dental, cl_eyecare, cl_other, and cl_radiology. All includes all exams regardless of their contents, though any exam without an associated Study Instance UID will automatically be excluded from the results. The specialization mappings are defined in DicomCategoryFilterConfiguration.config and can be updated if desired. The specialization mappings include: cl_cardiology filters for any cardiology related study modality, cl_dermatology filters for any dermatology related study modality, cl_dicom filters for any DICOM related study modality, cl_dental filters for any dental related study modality, cl_eyecare filters for any eyecare related study modality, cl_other filters

for any other modality not included in other filters available, cl_radiology filters for any radiology related study modality.

21. If desired to not have actively serviced C-MOVE timeouts, set sendKeepAlive to true inside the opening and closing sendKeepAlive tags, otherwise set false (inside <sendKeepAlive> </ sendKeepAlive > - line 27). The default setting is false.
22. If desired to use concurrent C-STORE, set useMultiAssociations to true inside the opening and closing useMultiAssociations tags, otherwise set false (inside <useMultiAssociations> </useMultiAssociations> - line 28). The default setting is false.
23. Set the maximum number of concurrent C-STORE connections inside the opening and closing cstoreTPoolMax tags (inside <cstoreTPoolMax> </cstoreTPoolMax> - line 29). The default setting is 3 maximum concurrent connections.
24. If desired to query patient identifiers unknown to the local VistA set remotePatientResolution to true inside the opening and closing remotePatientResolution tags, otherwise set false (inside <remotePatientResolution> </ remotePatientResolution> - line 30). The default setting is false. When true the VIX will fall back to querying CVIX with any patient identifiers it receives that cannot be resolved locally.
25. If desired to not fetch certain modality images, set the entries inside the opening and closing modalityBlockList tags for different dataSources.
    a. For each dataSource (DoD or VA), set different modality lists, if necessary, by inserting DoD or VA inside the opening and closing dataSource tags (<dataSource> </dataSource> - line 33), by default the value is ALL.
    b. The modalities will be filtered at study and series levels. If needed, set at the image level. To do so, set true at the image level when needed by inserting true inside the opening and closing addImageLevelFilter tags, otherwise set false (<addImageLevelFilter> </addImageLevelFilter> - line 34).
    c. List all the modalities to be blocked for that dataSource separately using string tags inside the opening and closing modalities section (<modalities> </modalities> - lines 35 and 37). Examples of modalities to potentially include inside the string tags include SR and PR.
26. The installer automatically generates a default blacklist consisting of site codes that configured DICOM SCUs do not receive data from. Your local site code and the site codes of your Veterans Integrated Service Network (VISN) appear in the <siteCodeBlackList> section in the file ScpConfiguration.config located in the C:\VixConfig folder. If you want your site's data to be available to the configured DICOM SCU, ensure your local site code is not in the <siteCodeBlackList> section in the ScpConfiguration.config. List all the site codes to be blocked separately using string tags inside the opening and closing siteCodeBlackList section (<siteCodeBlackList > </siteCodeBlackList> - lines 40 and 45). Examples of site codes to include inside the string tags include the following:
    a. Set a string to 100 to exclude Claims system information.
    b. Set a string tag to 200CLMS to exclude 200 VHA Claims study information.
    c. Set a string tag to 200CORP to exclude the Claims site.
    d. Set a string tag to 741 to exclude Global Disability Examinations.

e. Set a string tag to LOCAL to signal the DICOM Service to replace it with the local site number and all of the sites in that Veterans Integrated Service Networks (VISN).

NOTE: If desired to exclude DoD studies information, set a string tag to 200 inside the opening and closing siteCodeBlackList section (<siteCodeBlackList > </siteCodeBlackList>.

27. List all the SOP class UIDs codes that will not be sent when processing C-MOVEs for studies containing DICOM files of this type to the parent calling AE title using string tags inside the opening and closing sopClassBlackList section (<sopClassBlackList> </sopClassBlackList> - lines 46 and 48). Examples of SOP class UIDs to include inside the string tags include the following:
    a. Set a string to 1.2.840.10008.5.1.4.1.1.66 to exclude Raw data.

Save the ScpConfiguration.Config file after updating the entries. After updating the DICOM SCP config file, the ScpConfiguration.Config file will look like (Figure 22):

Figure 22: DICOM SCP Configuration File (Example)

```
<gov.va.med.imaging.facade.configuration.ScpConfiguration>
  <dirty>false</dirty>
  <accessCode>[redacted]</accessCode>
  <verifyCode>[redacted]</verifyCode>
  <siteFetchTPoolMax>20</siteFetchTPoolMax>
  <siteFetchTimeLimit>45</siteFetchTimeLimit>
  <imageFetchTPoolMax>15</imageFetchTPoolMax>
  <imageFetchTimeLimit>1000000</imageFetchTimeLimit>
  <useRemoteImageFetch>true</useRemoteImageFetch>
  <useDirectFetch>true</useDirectFetch>
  <cacheLifespan>1</cacheLifespan>
  <preFetchSeries>true</preFetchSeries>
  <calledAETitle>ANY_0.0.0.0</calledAETitle>
  <imageQueueSize>10000</imageQueueSize>
  <cacheMetaHoursToLive>24</cacheMetaHoursToLive>
  <isFdtEnabled>true</isFdtEnabled>
  <fdtPort>[redacted]</fdtPort>
  <isGenRptFromImage>true</isGenRptFromImage>
  <useP34>true</useP34>
  <callingAEConfigs>
    <gov.va.med.imaging.facade.configuration.ScpCallingAE>
      <aeTitle>[redacted]aeTitle>
      <callingAeIp>[redacted]</callingAeIp>
      <buildReport>SC</buildReport>
      <returnQueryLevel>false</returnQueryLevel>
      <studyQueryFilter>radiology</studyQueryFilter>
      <sendKeepAlive>false</sendKeepAlive>
      <useMultiAssociations>false<useMultiAssociations>
      <cstoreTPoolMax>3</cstoreTPoolMax>
      <remotePatientResolution>true</remotePatientResolution>
      <modalityBlockList>
        <gov.va.med.imaging.facade.configuration.ScpModalityList>
          <dataSource>ALL</dataSource>
          <addImageLevelFilter>false</addImageLevelFilter>
          <modalities>
            <string>none</string>
          </modalities>
        </gov.va.med.imaging.facade.configuration.ScpModalityList>
      </modalityBlockList>
      <siteCodeBlackList>
        <string>100</string>
        <string>200CLMS</string>
        <string>200CORP</string>
        <string>741</string>
      </siteCodeBlackList>
      <sopClassBlackList>
        <string>1.2.840.10008.5.1.4.1.1.66</string>
      <sopClassBlacklist>
    </gov.va.med.imaging.facade.configuration.ScpCallingAE>
  </callingAEConfigs>
</gov.va.med.imaging.facade.configuration.ScpConfiguration>
```

For additional DICOM SCU calling AE titles, insert an additional block of code (see Figure 23) containing the elements from lines 21 to 49 before current line 50 and then repeat steps 1 to 27 inside these additional lines that have been added.

Figure 23: DICOM SCP Configuration File with Multiple DICOM SCU Calling AE Titles (Example)

```
38          </gov.va.med.imaging.facade.configuration.ScpModalityList>
39        </modalityBlockList>
40        <siteCodeBlackList>
41          <string>100</string>
42          <string>200CLMS</string>
43          <string>200CORP</string>
44          <string>741</string>
45        </siteCodeBlackList>
46        <sopClassBlackList>
47          <string>1.2.840.10008.5.1.4.1.1.66</string>
48        <sopClassBlacklist>
49      </gov.va.med.imaging.facade.configuration.ScpCallingAE>
50      <gov.va.med.imaging.facade.configuration.ScpCallingAE>
51        <aeTitle>[redacted]aeTitle>
52        <callingAeIp>[redacted]</callingAeIp>
53        <buildReport>SC</buildReport>
54        <returnQueryLevel>false</returnQueryLevel>
55        <studyQueryFilter>radiology</studyQueryFilter>
56        <sendKeepAlive>false</sendKeepAlive>
57        <useMultiAssociations>false<useMultiAssociations>
58        <cstoreTPoolMax>3</cstoreTPoolMax>
59        <remotePatientResolution>true</remotePatientResolution>
60        <modalityBlockList>
61          <gov.va.med.imaging.facade.configuration.ScpModalityList>
62            <dataSource>ALL</dataSource>
63            <addImageLevelFilter>false</addImageLevelFilter>
64            <modalities>
65              <string>none</string>
66            </modalities>
67          </gov.va.med.imaging.facade.configuration.ScpModalityList>
68        </modalityBlockList>
69        <siteCodeBlackList>
70          <string>100</string>
71          <string>200CLMS</string>
72          <string>200CORP</string>
73          <string>741</string>
74        </siteCodeBlackList>
75        <sopClassBlackList>
76          <string>1.2.840.10008.5.1.4.1.1.66</string>
77        <sopClassBlacklist>
78      </gov.va.med.imaging.facade.configuration.ScpCallingAE>
79    </callingAEConfigs>
80  </gov.va.med.imaging.facade.configuration.ScpConfiguration>
```

After updating the ScpConfiguration.Config file, as described above, it is necessary to restart the Apache Tomcat service. One way this can be performed is by executing the restart script (Restart_VIX_Services.ps1) as described in the VIX Installation Guide.

8.3. Laurel Bridge DICOM SCP Configuration

This section provides details on the Laurel Bridge DICOM file located in the cfg folder within the Laurel Bridge installation directory (C:\DCF_RunTime_x64\cfg by default). Updates to this file are useful for debugging purposes but the details on how to change this are beyond the scope of this document. For typical VIX operation, no changes are necessary to the Laurel Bridge DICOM file.

Open the DicomScpConfig file to perform edits. Run Notepad, Notepad++, or WordPad as an administrator and then open the file. Numerous entries can be updated in the DicomScpConfig configuration file (Figure 24). Save the DicomScpConfig file after updating the entries.

Figure 24: DicomScpConfig Configuration File (Template)

```
[ application_info ]
name = DicomScp
description = Java server app that demonstrates use of QRServer and DicomSCP in DCS lib.
app_component_name = java_app/DicomScp
#app_component_name = cfg_app_name
execution_state = STOPPED

[ required_components ]
component = java_lib/LOG_a
component = java_lib/DCF
component = java_lib/LOG
component = java_lib/APC
component = java_lib/CDS
component = java_lib/APC_a
component = java_lib/CDS_a
component = java_lib/DCS
component = idl_lib/DDCS
component = java_lib/DSS
component = java_lib/DDS
component = java_lib/DDS_a
[ java_app ]

#================================================================================
# per-instance information for the DicomScp component
#================================================================================
[ java_app/DicomScp ]
#debug_flags = 0x0000f
debug_flags = 0x00000

#
# if true, demostrate the DataSetByteReader class for making
# a a decoded, and re-encoded network C-Store-Request look like
# a ReadableByteChannel or InputStream object.
#
use_byte_reader = YES

image_directory =
make_new_uids = FALSE
test_cfg_name = dcms.cfg
dicom_files_dir = dcms.cfg


[ java_lib ]

#================================================================================
# per-instance information for the LOG_a component
#================================================================================
[ java_lib/LOG_a ]
debug_flags = 0
```

9. Configure ID Conversion

The Id Conversion Configuration calls VA's Master Veteran Index (MVI) to do the ID Conversion from ICN to Electronic Data Interchange Personal Identifier (EDIPI) or from EDIPI to ICN. On a VIX, DICOM SCP needs this functionality.

The VIX install populates the IdConversionConfiguration.config file in C:\VixConfig with the host, username, and password for the destination of ID conversion lookup.

If additional changes to the defaults for the ID Conversion Configuration are needed, open the IdConversionConfiguration.config file in C:\VixConfig. It is suggested to run Notepad++ or WordPad as an administrator and then open the file.

The following entries can be updated for the ID Conversion Configuration (refer to Figure 25 for line numbers):

1. Set the protocol for the destination of ID conversion lookup (inside <protocol> </ protocol> - line 3).
2. Set the entry for the host for the destination of ID conversion lookup (inside <host> </host> - line 4).
3. Set the port for the destination of ID conversion lookup (inside <port> </ port > - line 5).
4. Set the urlResource for the destination of ID conversion lookup (inside <urlResource> </ urlResource> - line 6) (only if a change is needed).
5. Set the username for the destination of ID conversion lookup (inside <username> </username > - line 7).
6. Set the password for the destination of ID conversion lookup (inside <password > </password > - line 8).
7. Set the trustStoreFilePath (inside <trustStoreFilePath> </trustStoreFilePath> - line 9) (only if a change is needed).
8. Set the trustStorePassword (inside <trustStorePassword> </trustStorePassword> - line 10) (only if a change is needed).

Save the IdConversionConfiguration.config file after updating the entries. The IdConversionConfiguration.config should look like (Figure 25):

Figure 25: IdConversionConfiguration.config file (Template)

```
1  <gov.va.med.imaging.facade.configuration.IdConversionConfiguration>
2      <dirty>false</dirty>
3      <protocol>https</protocol>
4      <host>NEED.TO.CHANGE.HOST</host>
5      <port>[redacted]</port>
6      <urlResource>[redacted]</urlResource>
7      <username>**ADD USERNAME**</username>
8      <password>**ADD PASSWORD**<</password>
9      <trustStoreFilePath>C:\VixCertStore\federation.truststore</trustStoreFilePath>
10     <trustStorePassword>**ADD PASSWORD**</trustStorePassword>
11 </gov.va.med.imaging.facade.configuration.IdConversionConfiguration>
```

10. Appendix A: Image Sharing and DICOM Images

Images are delivered to VA sites by the CVIX.

10.1. VA DICOM Images Provided to DoD

DoD clinicians can request the types of exams from the VA listed in Table 26 via the CVIX:

Table 26: DICOM Modality Types Provided to DoD

DICOM Modality Description	DoD Identifiers
Angioscopy (retired)	AS, RAD AS
Biomagnetic Imaging	BI, RAD BI
Color flow Doppler (retired)	CD, RAD CD
Cinefluorography (retired)	CF, RAD CF
Culposcopy (retired)	CP, RAD CP
Computed Radiography	CR, RAD CR
Cystoscopy (retired)	CS, RAD CS
Computed Tomography	CT, RAD CT
Duplex Doppler (retired)	DD, RAD DD
Diaphanography	DG, RAD DG
Digital Microscopy (retired)	DM, RAD DM
Digital Radiography	DR, RAD DR, DX, RAD DX
Digital Subtraction Angiography	DS, RAD DS
Echocardiography (retired)	EC, RAD EC
Endoscopy	ES, RAD ES
Fluorescein Angiography (retired)	FA, RAD FA
Fundoscopy	FS, RAD FS
General Microscopy	GM, RAD GM
Intra-oral Radiography	IO, RAD IO
Laparoscopy (retired)	LP, RAD LP
Laser Surface Scan	LS, RAD LS
Magnetic Resonance Angiography (retired)	MA, RAD MA
Mammography	MG, RAD MG
Magnetic Resonance	MR, RAD MR
Nuclear Medicine	NM, RAD NM
Positron Emission Tomography	PT, RAD PT

DICOM Modality Description	DoD Identifiers
Radio Fluoroscopy	RF, RAD RF
Radiographic Imaging	RG, RAD RG
Single-Photon Emission Computed Tomography (retired)	ST, RAD ST
Thermography	TG, RAD TG
Ultrasound	US, RAD US
X-ray Angiography	XA, RAD XA
External-Camera Photography	XC, RAD XC

11. Appendix B: VIX Tools

There are numerous tools the system administrator executes to monitor and manage the VIX server. Table 27 lists the VIX Tools available.

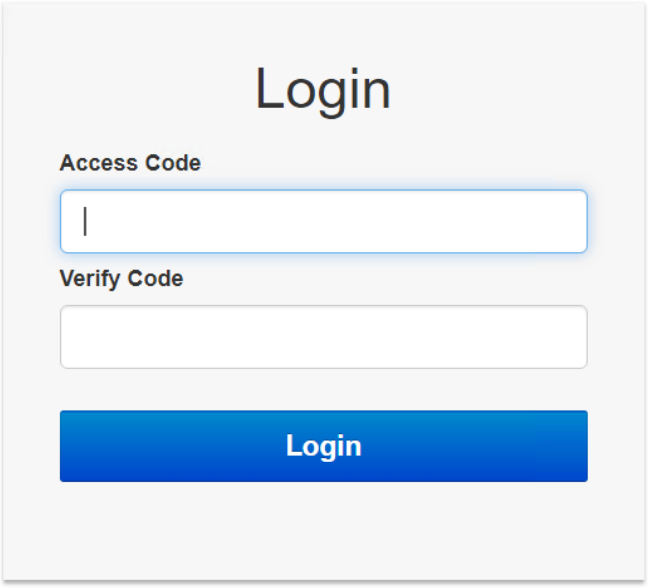
NOTE: In Table 27, please replace ***FQDN*** with your server's fully qualified domain name. For example: https://REDACTED/VixServerHealthWebApp/secure/MyVix.jsp

Table 27: List of URLs

URL	Description
https://*FQDN*:REDACTED/Vix/ssl/JavaLogs.jsp	Displays information for Java Logs: • Filename • File Size • Date Modified
https://*FQDN*:REDACTED/ROIWebApp/secure/ConfigureROI.jsp	To configure an ROI request and ROI options. Also, to re-set the access and verify codes of the service account with the ROI periodic processing and DICOM (Q/R) credentials.
https://*FQDN*:REDACTED/ROIWebApp/	To verify the status of an ROI request and get information about ROI statistics on the ROI Processing Status page.
https://*FQDN*/VixServerHealthWebApp/secure/MyVix.jsp	Displays information for the VIX: • Start Time • Up Time • Status • Realm Configuration • Tomcat Thread Details • Transaction Log • Site Service • Release of Information (ROI) • DICOM Services Transmit Failures
https://*FQDN*:REDACTED/Vix/secure/VixLog.jsp	To access the VIX transaction log while the VIX is running, which contains information about every image and metadata transfer handled by the VIX.

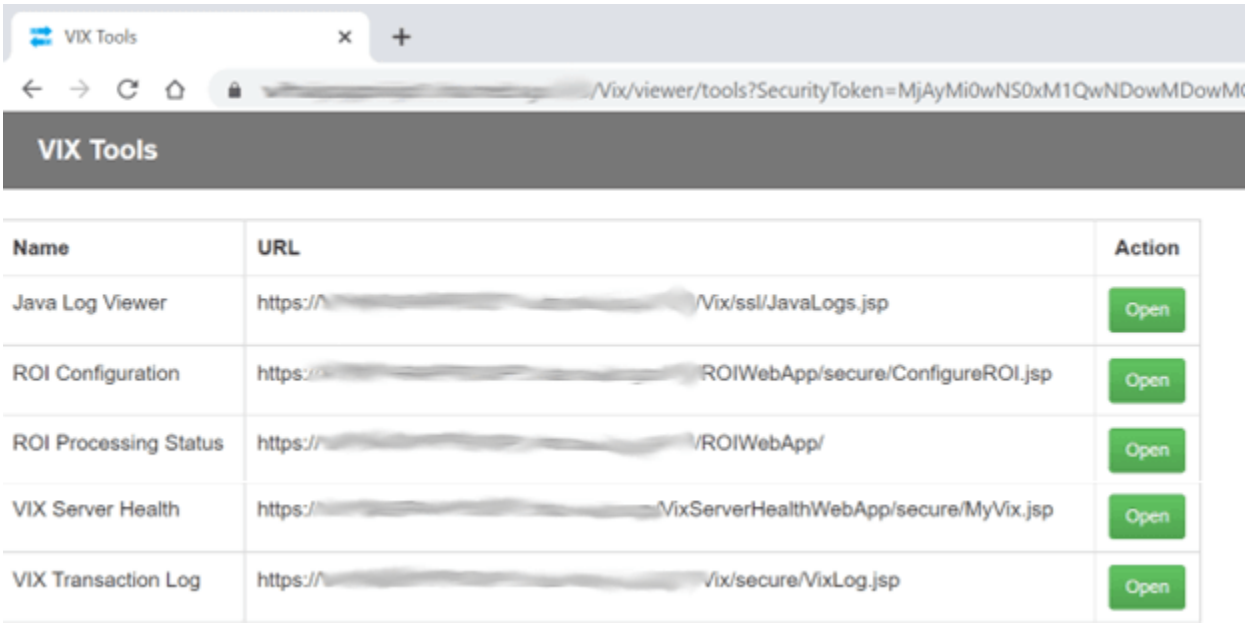
To access the tools, navigate to https:// REDACTED/vix/viewer/tools to be prompted to login (Figure 26). Use a VistA account with the MAG VIX ADMIN security key and INITIAL to log in.

Figure 26: Login Page



Once logged in, a tools page will appear (Figure 27). Access a VIX tool by clicking Open.

Figure 27: VIX Tools Page



12. Appendix C: VIX Utility Scripts

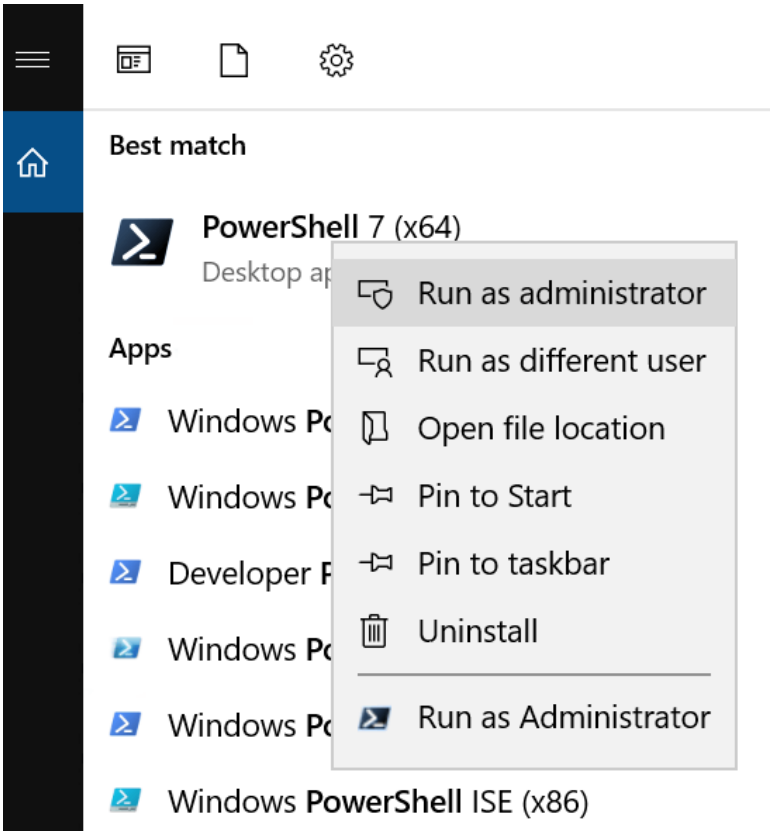
There are numerous PowerShell scripts the system administrator can use to help manage the VIX server. These scripts are located in C:\Program Files\VistA\Imaging\Scripts. Refer to the powershell_readme.txt file located C:\Program Files\VistA\Imaging\Scripts for a full listing of scripts and their purpose. Several scripts are described in detail in this appendix in the sections that follow.

NOTE: Please use PowerShell 7 to run the scripts in this Appendix. Once done with using a script, close PowerShell.

12.1. Run PowerShell as an Administrator

1. Run PowerShell as an administrator (Figure 28).
    a. Right-click **Start**.
    b. Left-click **Search**.
    c. Type **powershell**.
    d. Right-click **PowerShell 7 (x64)**.
    e. Left-click Run as administrator.

Figure 28: Execute Windows PowerShell

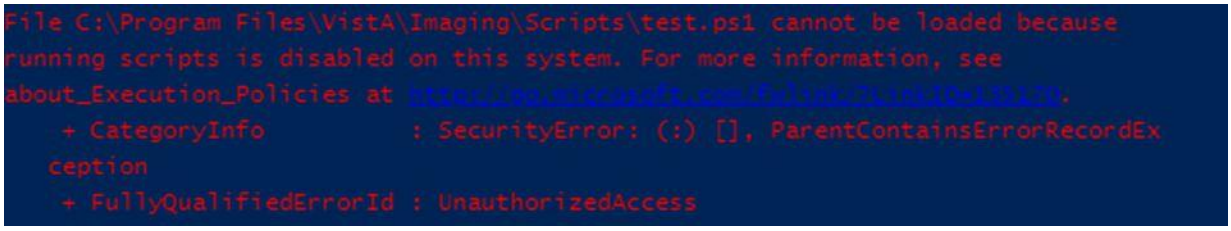


2. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes**.

12.2. PowerShell Configuration

If encountering a PowerShell error (Figure 29) preventing scripts from running, perform the following steps:

Figure 29: PowerShell Script Error



1. Run PowerShell as an administrator.
2. Once PowerShell launches, type the command:
   `Set-ExecutionPolicy RemoteSigned -Force`
   Press **[ENTER]** to set the policy to allow scripts to run, then close PowerShell.

12.3. Restart Script

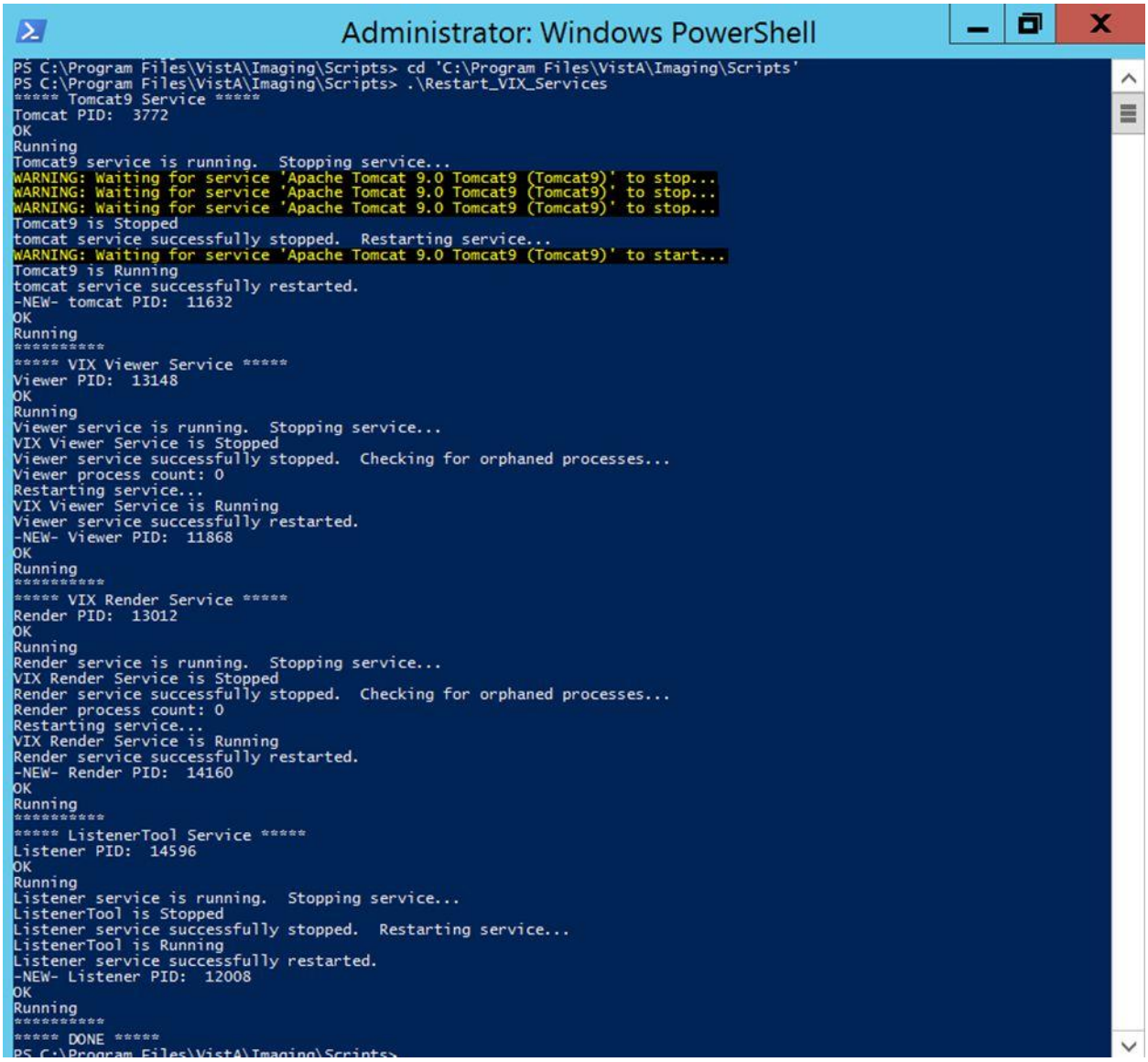
This section describes how to execute the restart script (Restart_VIX_Services.ps1) to restart the Apache Tomcat service, VIX Viewer service, and VIX Render service.

If a restart of any of the services is needed, perform the following:

1. Run PowerShell as an administrator.
2. Once PowerShell launches, **type** the command:
   `cd "C:\Program Files\VistA\Imaging\Scripts"`
   Then press **[ENTER]** to change the working directory to the Scripts folder.
3. Then **type** the command:
   `.\Restart_VIX_Services.ps1`

And press **[ENTER]** to execute the restart script. Wait for the script to complete (Figure 30).

Figure 30: Windows PowerShell Restart Script



12.4. Tomcat Permissions Script

Due to the VA group policy restriction or rules, there may be an issue found while the VIX installer wizard is setting file system access rules - i.e.: ...error denying access to apachetomcat account to c:\...

If encountering file system access errors, to resolve this, run the tomcat permissions script (permission_fixer.ps1). Perform the following:

1. Run PowerShell as an administrator.
2. Once PowerShell launches, **type** the command:

   ```
   cd "C:\Program Files\VistA\Imaging\Scripts"
   ```

Then press **[ENTER]** to change the working directory to the Scripts folder.

3. Then **type** the command:
   `.\permission_fixer.ps1`
   And press **[ENTER]** to execute the permission fixer script. Wait for the script to complete.
4. Follow the steps in Section 12.3 to execute the restart script.

NOTE: The permission fixer script updates the Apache Tomcat account [apachetomcat] permissions on the following folders

- C:\dicom\temp
- C:\Program Files\Apache Software Foundation\Tomcat 9.0\
- C:\Program Files\java\Jre...
- C:\DCF_Run Time_x64
- C:\Vixconfig
- C:\VixCertStore
- YOUR_DRIVE_LETTER:\VixCache
- YOUR_DRIVE_LETTER:\VixTxDb

NOTE: The permission fixer script does not update apachetomcat permissions on YOUR_DRIVE_LETTER:\VixRenderCache as this is no longer needed.

12.5. Purge Render Database (Cache Curator) Script

This section describes how to purge the VIX Render database (C:\Program Files\VistA\Imaging\VIX.Render.Service\Db\SQLiteDb.db). The CacheCurator.ps1 script stops the Viewer and Render services, restores the VIX Render SQLite database to a version with empty tables, completely removes the VIX Render cache contents, and starts the Viewer and Render services. This script can be run if during installation a message “Please manually purge ViewRender database” displays.

To use the purge render database script, perform the following:

1. Run PowerShell as an administrator,
2. Once PowerShell launches, **type** the command:
   `cd "C:\Program Files\VistA\Imaging\Scripts"`
   Then press **[ENTER]** to change the working directory to the Scripts folder.
3. Then **type** the command:
   `.\CacheCurator.ps1`
   And press **[ENTER]** to execute the script.

12.6. Java Management Extensions (JMX) Script

The jmxremote.password file (located in C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf) enables authentication for Java Management Extensions (JMX) and requires special

permissions in order for the VIX to function properly. The apachetomcat user needs ownership of the jmxremote.password file and also the only user with read permissions.

In the event the Tomcat service fails to start, this section describes how to set the required read permissions on the jmxremote.password file for the apachetomcat user. This section also describes how to revert the permissions on the jmxremote.password file to full control for administrators if modifications are required or if errors occur during VIX installation.

To use the JMX script, perform the following:

1. Run PowerShell as an administrator.
2. Once PowerShell launches, **type** the command:
   ```
   cd "C:\Program Files\VistA\Imaging\Scripts"
   ```
   Then press **[ENTER]** to change the working directory to the Scripts folder.
3. Then **type** the command:
   ```
   .\set_jmx_permissions.ps1
   ```
   And press **[ENTER]** to execute the script.
4. When prompted with "Please choose option (1 to set Read for apachetomcat only, 2 to set Full Control for administrators, or Q to Quit)" do one of the following:
   a. To set read control for apachetomcat only for the jmxremote.password file, when prompted, enter 1 and press **[ENTER]**.

   NOTE: Option 1 is the state that enables authentication for JMX.

   b. To set full control for administrators for the jmxremote.password file, when prompted, enter 2 and press **[ENTER]**.

   NOTE: Option 2 should only be used temporarily if modifying the jmxremote.password file or errors during VIX installation occur. The Tomcat service will not start if the jmxremote.password file has full control for administrators.

12.7. Delete VixCache Script

This section describes how to delete the contents of the VIX Cache (YOUR_DRIVE_LETTER:\VixCache) folder. The delete_cache.ps1 script clears the contents of the YOUR_DRIVE_LETTER:\VixCache folder.

To use the delete vixcache script, perform the following:

1. Run PowerShell as an administrator.
2. Once PowerShell launches, **type** the command:
   ```
   cd "C:\Program Files\VistA\Imaging\Scripts"
   ```
   Then press **[ENTER]** to change the working directory to the Scripts folder.
3. Then **type** the command:
   ```
   .\delete_vixcache.ps1
   ```
   And press **[ENTER]** to execute the script.

13. Appendix D: McAfee/Trellix Exclusions

NOTE: McAfee/Trellix Exclusions are now managed by the enterprise and only some administrators will have the ability to view and edit the On-Access Scan Properties.

The directories which are excluded in On-Access Scan Properties are:

- C:\DCF_RunTime_x64\
- C:\dicom\temp
- C:\Program Files\Java*****\lib\
- C:\Program Files\Apache Software Foundation\Tomcat*\lib\
- C:\Program Files\Apache Software Foundation\Tomcat*\logs\
- C:\Program Files\VistA\Imaging\VIX.Render.Service\log\
- C:\Program Files\VistA\Imaging\VIX.Viewer.Service\log\
- ?:\VixCache\
- ?:\VIXRenderCache\
- ?:\ImagingArchivedLogs\
- ?:\VixTxDb\

The “Also exclude subfolders” is also checked, so subfolders are excluded as well.

NOTE: The wildcard * is interchangeable with wildcard ? for the folder exclusions.

14. Definitions, Acronyms, and Abbreviations

Table 28: Definitions, Acronyms, and Abbreviations

Term	Definition
AE	Application Entity
BP	Background Processor
BSE	Broker Security Exchange
CPRS	Computerized Patient Record System
CPU	Central Processing Unit
CRUD	Create, Read, Update, and Delete
CSV	Comma-Separated Values
CT	Computerized Tomography
CVIX	Centralized VistA Imaging eXchange
DES	Data Exchange Service
DAS	Data Access Service
DICOM	Digital Imaging and Communications in Medicine
DCF	DICOM Connectivity Framework
DFN	Data File Number
DoD	Department of Defense
DUZ	Designated User
ECIA	Enterprise Clinical Imaging Archive
EDIPI	Electronic Data Interchange Personal Identifier
FDA	Food and Drug Administration
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
GUID	Globally Unique Identifier
HAIMS	Healthcare Artifact and Imagery Management Solution
HDIG	Hybrid DICOM Gateway
HIPAA	Health Insurance Portability and Accountability Act
IAM	Identity and Access Management
ICN	Integration Control Number
IEN	Internal Entry Number
ICR	Integration Control Registrations
IVS	Integrated Visualization System

Term	Definition
JLV	Joint Legacy Viewer / Joint Longitudinal Viewer
JMX	Java Management Extensions
JRE	Java Runtime Environment
MAG	VistA Imaging
MVI	Master Veteran Index
OI&T	Office of Information and Technology
PACS	Picture Archiving and Communication System
Q/R	Query Retrieve
ROI	Release of Information
RPC	Remote Procedure Calls
RTF	Rich Text Format
SCP	Service Class Provider
SCU	Service Class User
SOP	Service-Object Pair
SMB	Server Message Block
STS	Secure Token Service
TCP/IP	Transmission Control Protocol/Internet Protocol
TIU	Text Integration Utility
TSV	Tab-Separated Values
UID	Unique Identifier
URN	Universal Resource Name
VA	Department of Veterans Affairs
VIX	VistA Imaging eXchange
VM	Virtual Machine
VISN	Veterans Integrated Service Networks
WAN	Wide Area Network