VistA Imaging Exchange Administrator's Guide

Department of Veterans Affairs

Office of Information and Technology (OI&T)

VistA Imaging Exchange (VIX) Administrator's Guide
February 2018

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: REDACTED

VA intranet: REDACTED

Revision History

Date	Rev	Notes
02 February 2018	10	Additional updates for MAG*3.0*185. REDACTED
14 November 2017	9	Updated for MAG*3.0*185 and incorporated comments from reviewers. REDACTED
05 October 2017	8	Updated for P170 and 177, including VIX image viewer. REDACTED
9 September 2013	7	Added section ROI VIX Operation, Configuration and Statistics; REDACTED
01 August 2013	6	Renamed for joint rollup of MAG*3.0*34/116/118, MAG*3.0*119, MAG*3.0*127, MAG*3.0*129. REDACTED
15 July 2013	5	Updated for Imaging patch MAG*3.0*119. Updated sections on Related Information; The VIX Transaction Log; Caching of Metadata and Images. REDACTED
14 September 2012	4	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, Added new RPCs related to VIX/Importer II, REDACTED
14 Oct 2011	3	Updated for Imaging patch MAG*3.0*104 to reflect expanded image sharing and involvement of CVIX. Reorganized to support future revisions. REDACTED
20 Jan 2011	2	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 node in file #2006.95. Minor wording corrections. REDACTED
22 Apr 2010	1	Document created for Imaging patch MAG*3.0*83. REDACTED

Contents

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 as well as between VA and the Department of Defense (DoD) medical facilities. It is anticipated that the VIX's role will be expanded to support data sharing and exchange within a facility as well as between facilities.

Beginning with MAG*3.0*170, the VIX hosts a zero footprint viewer providing services to consuming application chiefly eHMP and JLV. These services are expected to be utilized by future applications. With these changes, the VIX becomes a more critical component as it is providing access not only to remote but local images as well. Maintenance of this component becomes more 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 the installation of 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 systems.

1.3. Document Conventions

This document uses the following typographic conventions.

Symbol/Typeface	Meaning/Use	Example
Bold	User input, selection, GUI element (menu item, button, field)	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	Access the Kernel Installation and Distribution System Menu [XPD MAIN]. ;;3.0;IMAGING;**[Patch List]**;Mar 19, 2002;Build 1989;Feb 21, 2011 MAG*3.0*<*PatchNumber*>.KID

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.

- **VIX Image Viewer** – A description of VIX operations specific to image viewing hosted by the VIX

- **ROI VIX Operation, Configuration and Statistics** – A description of how the VIX processes ROI requests.

- **VIX Reference/Software Description** – VIX technical information.

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

<mark>REDACTED</mark>

2. VIX Overview

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

2.1. The VIX and Image Sharing

The VIX implements image sharing between the Department of Veterans Affairs (VA) and 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 having to manually log 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

The following diagram shows how remote VA images and related metadata flow through a VIX.
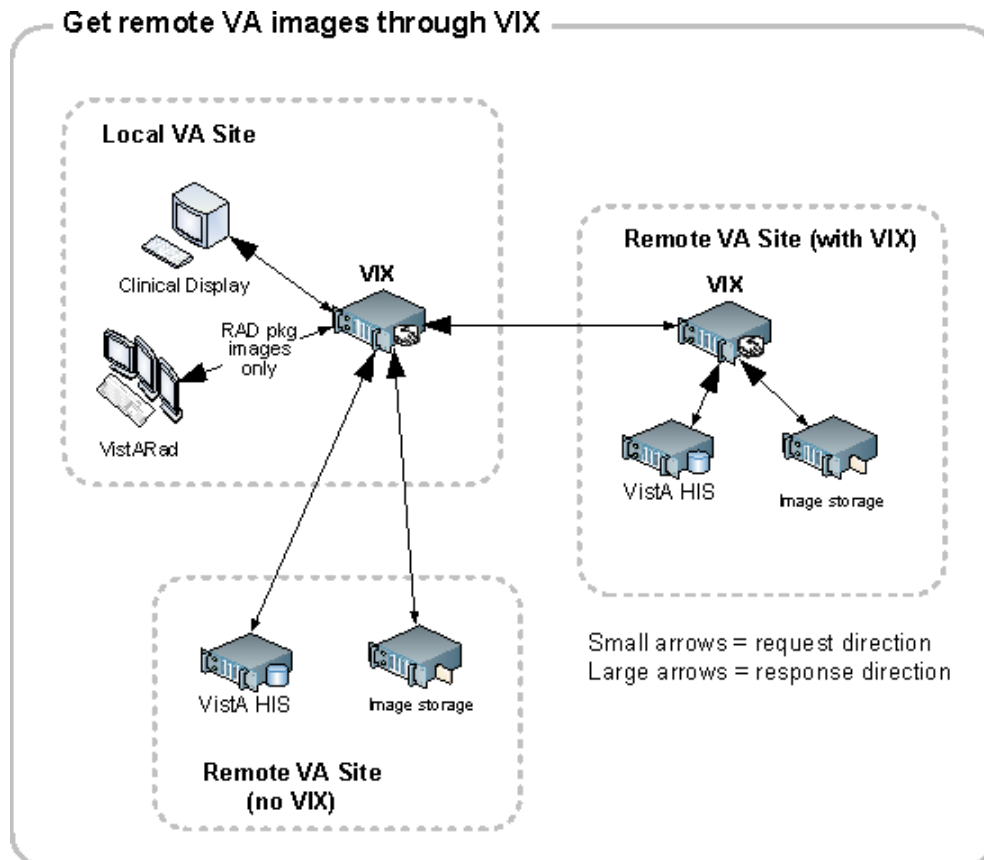
When the VIX is used for VA-to-VA image sharing, the VIX can handle anything stored in VistA Imaging. This includes radiology images, clinical images of all types, scanned documents, video, and audio.

> **Note:** MUSE EKG waveforms, commercial PACS images, and other images not stored in VistA Imaging cannot be retrieved using the VIX.

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

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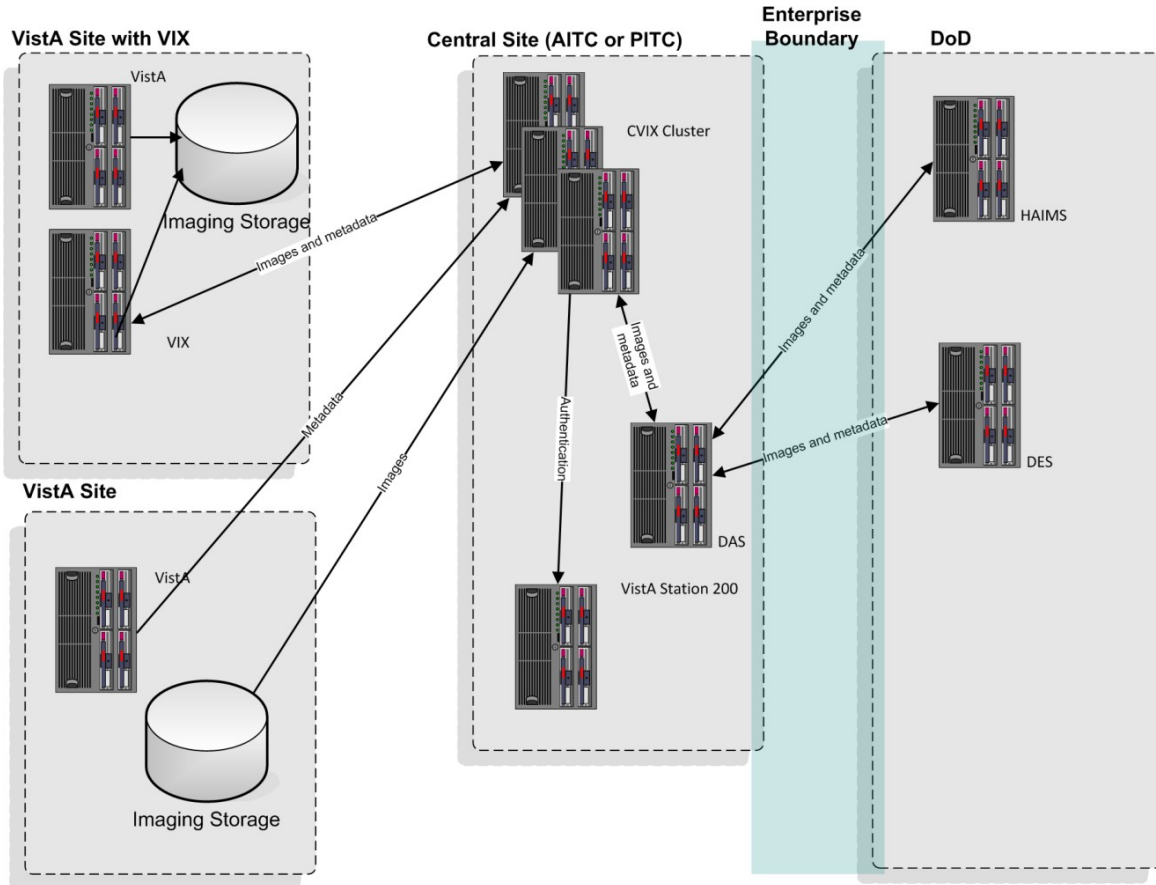
VA clinicians can access the following types of DoD images for shared patients if a local VIX is implemented and if the appropriate DoD image sources are online.

Image Category	Notes
DoD DICOM images	Available from participating DoD facilities via the CVIX and originating from the DAS Image Adapter.
	Note: There are a limited number of non-image DICOM objects that are not provided. For more information, see *DoD DICOM Object Filtering*.
DoD artifacts (non-radiology medical images, scanned documents, etc.)	Available if HAIMS (Health Artifact and Image Management Solution) servers are online and if HAIMS 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 DICOM images for VA/DoD shared patients. For additional details about the types of images involved, see *VA DICOM Images Provided to DoD*.
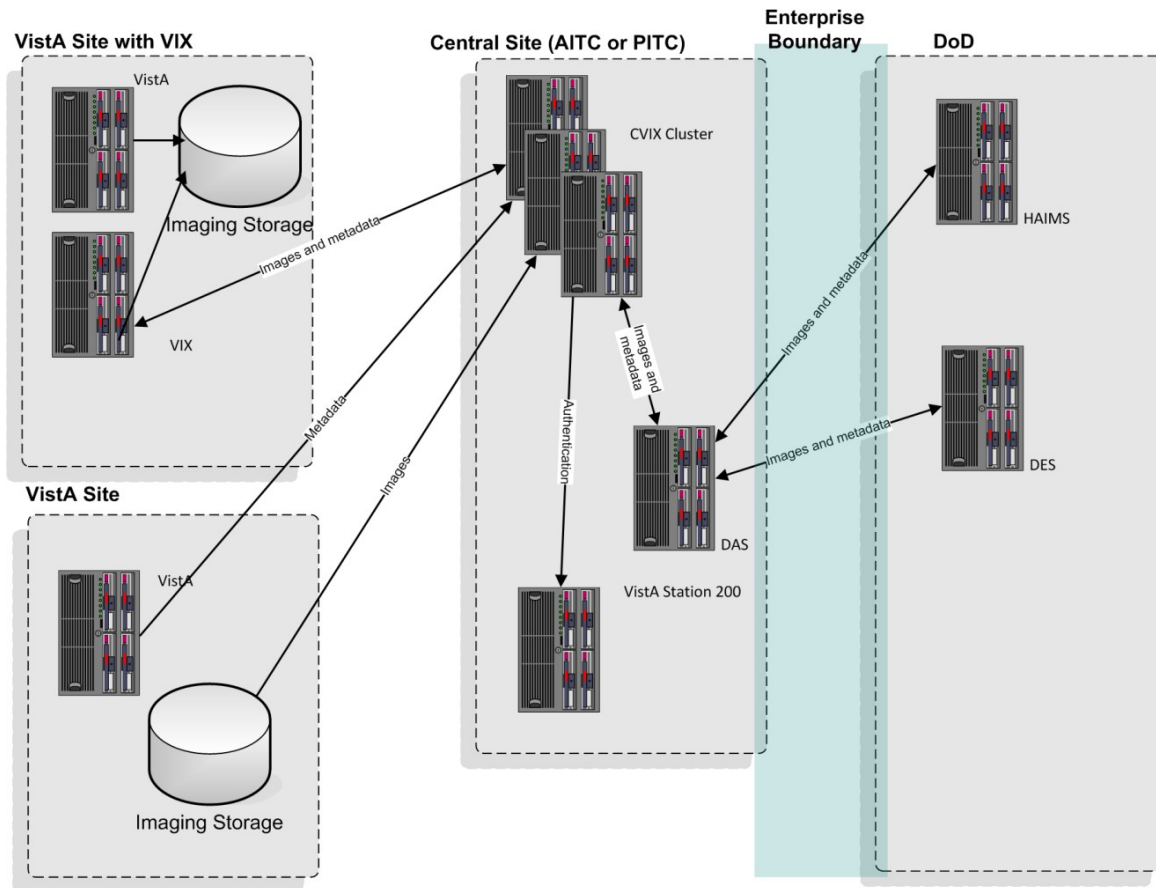
Note: DoD clinician image access requests are logged in the local VistA system.

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: MUSE EKG waveforms, commercial PACS images, and other images not stored in VistA Imaging cannot be accessed by DoD clinicians.

2.1.4. What is the CVIX?

The Centralized VistA Image Exchange (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

- Supports the Advanced Image Web Viewer (AWIV). For more information about the AWIV, see the *VistA Imaging AWIV User Guide*.

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 as well as at 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 will not be apparent to clinicians after VIXes are fully implemented, and clinicians do not have 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 PACS Integrator

If a participating DoD facility shares a direct network connection with a VA site that has a VIX, the DoD facility's PACS 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 <mark>REDACTED</mark>.

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. VIX Image Viewer

MAG*3.0*177 introduced new VIX services to support a zero-footprint web based image 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). It also introduces a specialized VIX called the rVIX to handle image and viewer requests from external applications such as eHMP and JLV. These external applications connect to the rVIX servers (currently located at the Austin Information Technology Center (AITC) and Philadelphia Information Technology Center (PITC)) for image and image related metadata queries.

The rVIX serves out images (through the zero-footprint viewer) if the site that the user logged in to has not upgraded their VIX to MAG*3.0*170 or later. Otherwise, the viewing of images to the zero-footprint viewer will be redirected and served out through the user's local VIX if the site has already installed MAG*3.0*170 or later. This arrangement keeps image traffic local to the facility as much as possible (for better performance) while continuing to provide access to images for users whose site VIX has not yet been upgraded. All image access using the zero-footprint image viewer, whether local or remote, goes through the VIX (and/or rVIX) and utilizes these new services.
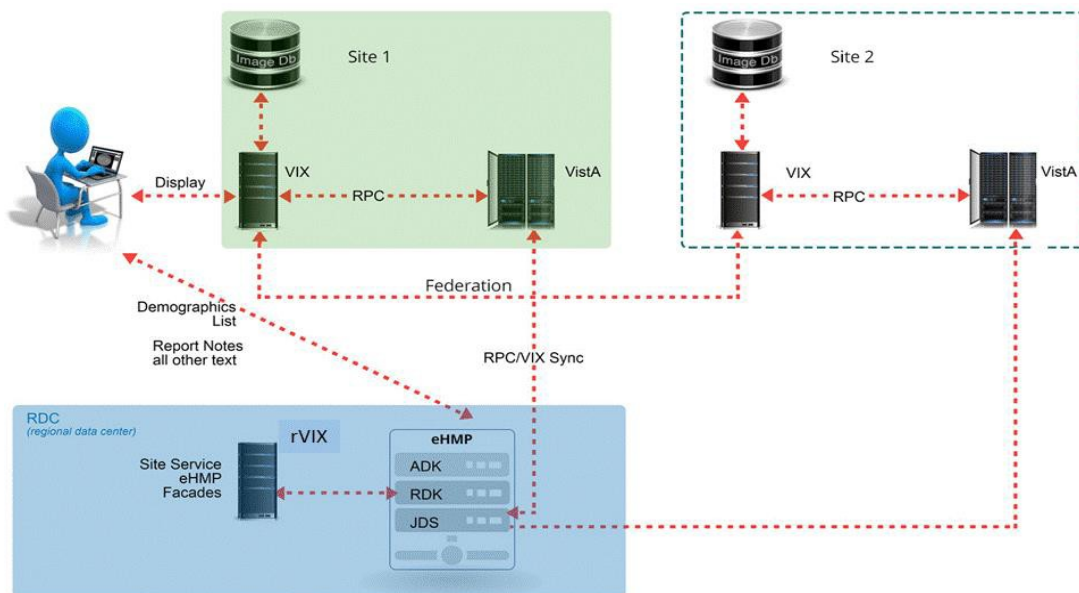
Image Viewer Data and Control flow Using eHMP as an Example Application

2.3.1.   New Services Introduced by MAG*3.0*170, 177 and 185:

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.

3. **Listener service:** The listener service is a generic TCPIP listener that was introduced to speed up the VIX connections to VistA.
4. **SQLEXPRESS:** SQLEXPRESS is a local database and associated services used to manage images in the cache.
5. **Supported SOP Classes** Newly supported SOP Classes are being made available with MAG*3.0*185. (see the MAG*3.0*185 patch description for a detailed listing)

2.3.2.   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. The listener service is a non-critical service as it is only used to help with performance of the VIX RPC calls.

All VIX services prior to patch MAG*3.0*170 run under the Apache Tomcat Windows service. The new services run under their own separate Windows services. See details below to verify the 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, CPU and memory are not exceeded.

2.3.3.   Windows Services

Ensure that Apache Tomcat, VIX Render Service, VIX Viewer Service, Listener Tool, and SQL Server (SQLEXPRESS) services are up and operational. See below for service details.
Note: The Apache Tomcat version may vary depending on which patch level is installed.
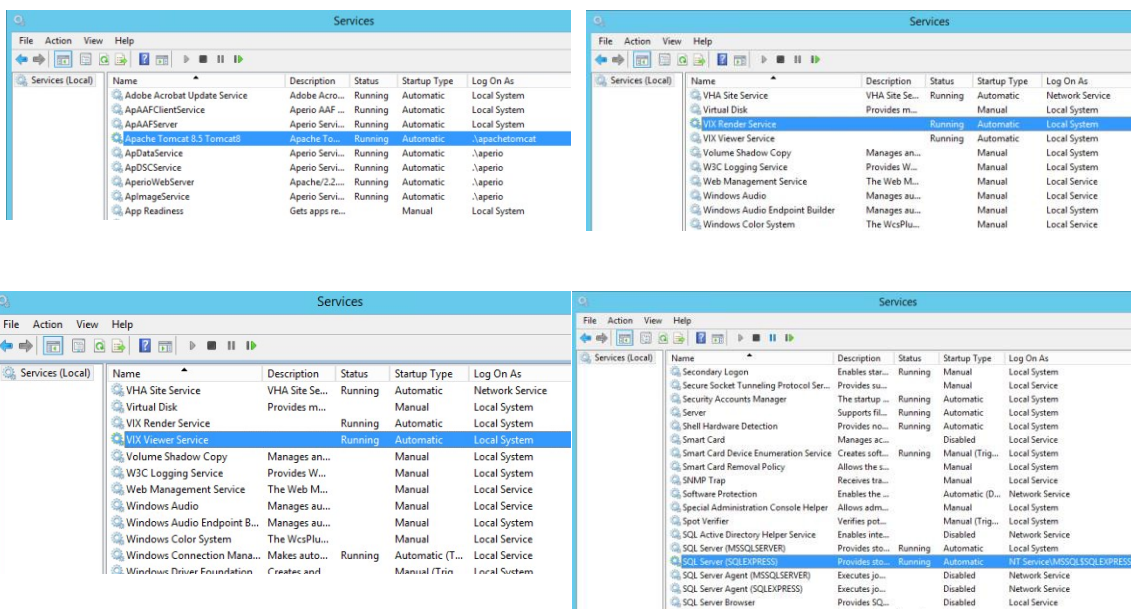
2.3.4. Windows Processes

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 (x10) - 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

2.3.5. Service Logging

If all related VIX Windows services and processes are running, the service logs can be reviewed to check for errors. By default, the logging level for the services is set to "Warn". This means that warnings and errors will appear in the log files. If a more granular level of logging is needed for troubleshooting, it can be changed from "Warn" to "Trace" in the rules section at the end of each config file listed below:
    a. VIX Viewer Service
        i. C:\Program Files\VistA\Imaging\Vix.Viewer.Service\NLog.config
        ii. C:\Program Files\VistA\Imaging\Vix.Viewer.Service\Worker.NLog.config
    b. VIX Render Service
        i. C:\Program Files\VistA\Imaging\Vix.Render.Service\NLog.config
        ii. C:\Program Files\VistA\Imaging\Vix.Render.Service\Processor.NLog.config

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

2.3.6. Viewer Image Caching

The zero-footprint image viewer uses pre-processed images and metadata that are stored in the VIX Render cache. The VIX render cache is a temporary cache of files that is 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. Stop the VIX Viewer and VIX Render services
2. Delete all folders in the top level Render cache folder located in*:*
        <Cache Drive> :\VIXRenderCache
3. Re-Install and configure SQL Express

a. Copy the SQL Express installation (SQLExpress_x64-12_0_2000_8.zip) to a local folder on the server

b. Extract all the files

c. In the command prompt window, navigate to the directory used for extracted files

d. Run the following command: Setup.exe /ConfigurationFile=ConfigurationFileInstall.ini
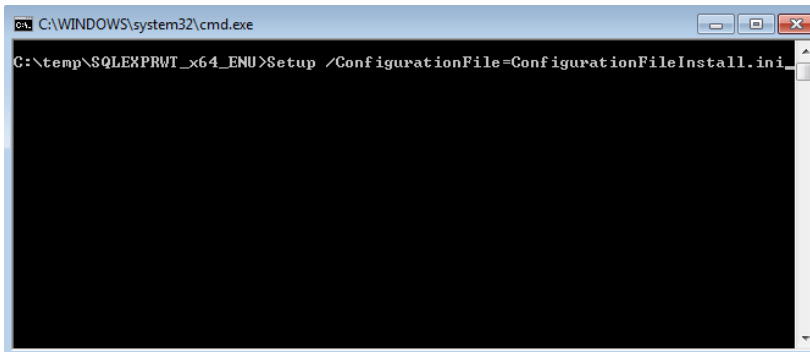
4. Review the console window and ensure no errors were reported

5. Restart the VIX Viewer and Render Services

6. Verify Viewer operations by opening a few studies by launching via zero-footprint Image Viewer in JLV.

2.3.7.   VIX Viewer Test Page

MAG*3.0*177 introduced a test page to access image viewer functionality without the need of running a consuming application. To utilize this functionality, the test page has to be manually enabled through the VIX Viewer configuration. To enable the test page, modify the Policies section of the C:\Program Files\VistA|imaging\Vix.Config\Vix.Viewer.Config file to include the line below:

<add name="Viewer.EnableTestPage" value="true" />

The resulting file will look similar to the example below:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="VistA" type="Hydra.VistA.VistAConfigurationSection, Hydra.VistA" />
  </configSections>
  <VistA WorkerPoolSize="10" WorkerThreadPoolSize="10">
    <VixServices>
      <VixService ServiceType="Local" RootUrl="http://localhost:8080"
      <VixService ServiceType="SiteService" RootUrl="http://localhost:8080" />
      <VixService ServiceType="Viewer" RootUrl="http://+:9911" />
      <VixService ServiceType="Render" RootUrl="http://localhost:9901" />
    </VixServices>
    <Policies>
      <add name="Security.EnablePromiscuousMode" value="true" />
      <add name="CPRS.ContextId.UseImageIndicator" value="true" />
      <add name="CPRS.ContextId.ImageIndicatorIndex" value="13" />
      <add name="Viewer.EnablePresentationState" value="true" />
      <add name="Viewer.EnableTestPage" value="true" />
      <add name="Viewer.EnableESignatureVerification" value="true" />
    </Policies>
  </VistA>
</configuration>
```

Warning: The Test page provides no security so it cannot be left open. Once the test event is complete, the configuration file must be altered to comment out the test page enable.

```
      <add name="CPRS.ContextId.ImageIndicatorIndex" value="13" />
      <add name="Viewer.EnablePresentationState" value="true" />
      <!-- <add name="Viewer.EnableTestPage" value="true" /> -->
      <add name="Viewer.EnableESignatureVerification" value="true" />
    </Policies>
  </VistA>
</configuration>
```

Restart the VIX Viewer Service.

The default test information can be added by modifying the c:\Program Files\VistA\Imaging\Vix.Viewer.Service\test.json file.

The file contains sections for making requests to the VIX Viewer. Below is an example of the file:

```
{
    "headers" : [
        {
            "name" : "default",
            "items" : [
                {
                    "key" : "Content-Type", "value" : "application/json"
                },
                {
                    "key" : "xxx-securityToken", "value" : "1XWBAS1620-423141_3"
                },
                {
                    "key" : "xxx-fullname", "value" : "USER, IMAGING"
                },
                {
                    "key" : "xxx-duz", "value" : "20095"
                },
                {
                    "key" : "xxx-ssn", "value" : "123456789"
                },
                {
                    "key" : "xxx-sitename", "value" : "CAMP MASTER"
                },
                {
                    "key" : "xxx-sitenumber", "value" : "500"
                }
            ]
        }
    ],
    "items" : [
        {
            "title" : "Patient 21 study query",
            "header" :
            {
                "name" : "default",
                "items" : []
            },
            "body" : {
                "patientICN": "10121",
                "siteNumber": "500"
            }
        },
        {
            "title" : "Patient 8 study query",
            "header" :
            {
                "name" : "default",
                "items" : []
            },
            "body" : {
                "patientICN": "10108",
                "siteNumber": "500"
            }
        }
    ]
}
```

The Header section of the file contains the user and login information while the Items section contain individual query parameters for items to be sent to the viewer service.

To access the Test page, enter the test page URL on the browser address bar:
http(s)://<Vix Host>:<viewer port>/vix/viewer/test
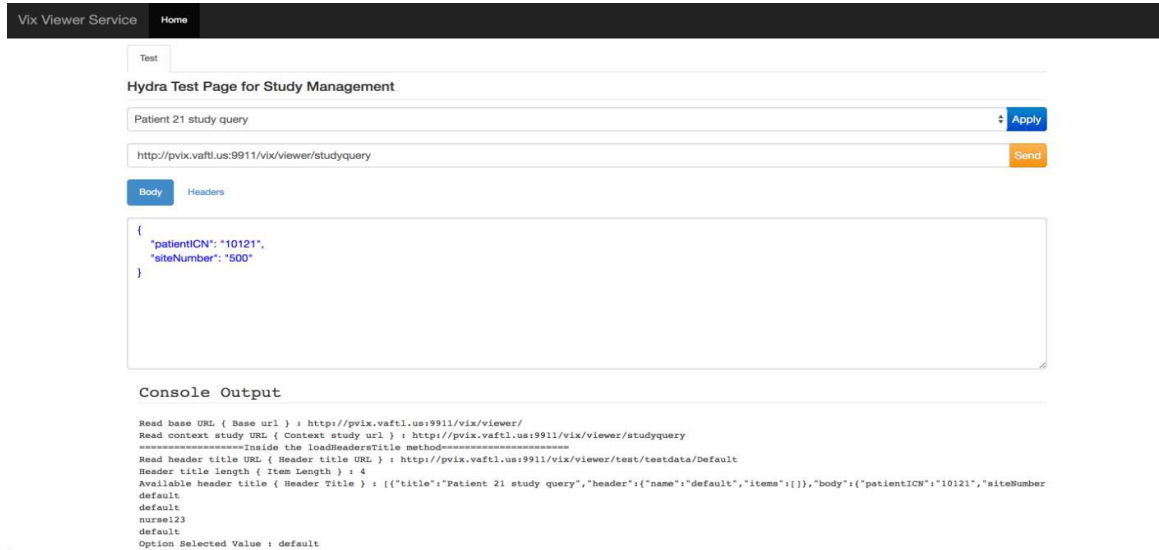
The user can edit the fields on the screen for both the body and the headings and submit them as different queries. When a query is submitted, the resulting page contains access to each study.
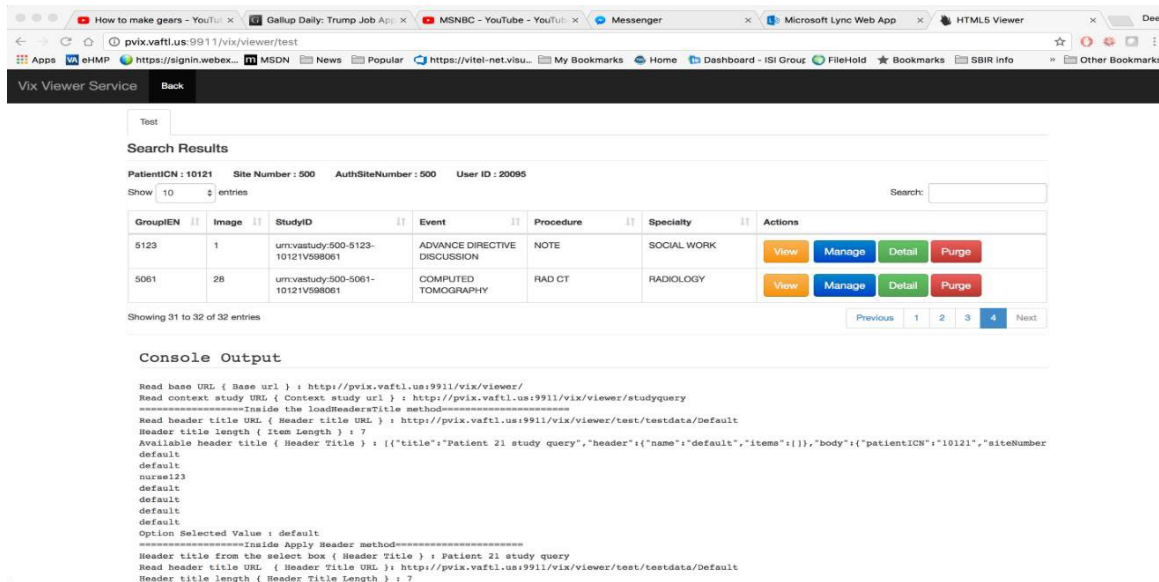
Selecting the View option will open the VIX Viewer. The Manage button will open the manage page and the details show the study level return views.

2.3.8. Currently Supported SOP Classes

SOP Classes Newly Supported in MAG*3.0*185	
SOP Class Name	SOP Class UID
Breast Tomosynthesis Image Storage	1.2.840.10008.5.4.1.1.13.1.3
Enhanced CT Image Storage	1.2.840.10008.5.4.1.1.2.1
Enhanced MR Image Storage	1.2.840.10008.5.4.1.1.4.1
12-lead ECG Waveform Storage	1.2.840.10008.5.4.1.1.9.1.1
General ECG Waveform Storage	1.2.840.10008.5.4.1.1.9.1.2

Table 1: SOP Classes

2.4. VIX Implementation and Configuration

The VIX is hosted on a dedicated VM. Careful considerations should be given when sizing the VIX. With the introduction of the VIX 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*.

Note: Radiology exams acquired before the release of MAG*3.0*50 do not have the information needed by DoD display applications to properly split exams into series.

VA sites that implement a VIX and that plan on sharing historic/related exams with DoD sites should execute the MagKat utility distributed with MAG*3.0*98. Doing so will populate DICOM series information for radiology exams acquired before the release of MAG*3.0*50. See the *VistA Imaging Storage Utilities Manual* for details.

2.5. VIX Dependencies

The following systems must be present for proper VIX operation.

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

Name/Location	Function	Interface Method
Local VistA	Provides metadata and image locations to requesting VIXes, control access to local VIX transaction log; VistA logging of VIX-mediated image accesses.	LAN/RPC
VIX cache	Provides cached images for improved speed.	LAN

Name/Location	Function	Interface Method
Remote VistA	Source of remotely stored VA images for local clinician access. (The VIX will continue 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 will continue 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 will use locally cached connection data if the VistA Site Service is not available.	WAN/http
RVIX	Metadata source for the consuming applications. The consuming application (eHMP, JLV or others) query the RVIX and the RVIX uses the federation to retrieve site specific information. The RVIX also has the ability to provide viewing for applications not authenticated against a specific site VIX.	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 server where the VIX is installed is shut down:

- Clinicians using Clinical Display will still be able to retrieve remote images (at reduced performance) using Remote Image Views, so 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 will not be able to 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 own operational priority assessment in this case.

- Clinicians viewing images in eHMP and JLV retrieve images using the RVIX and the site VIX. Loss of either resource will block image viewing. The RVIX is already running on a load balanced cluster.

- IMPORTER: DICOM Importer II/III users will be unable to login and import images

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 Enhancement (BSE) 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) and 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 that is 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 Internet Explorer 7 (or later) and Firefox 3 (or later). The main transaction log Web page can be used to display, filter, and export log entries of interest.

To access the transaction log you will need the following:

- A VistA account that has 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>/Vix/ssl/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>/Vix/ssl/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 will not work.

3. The VIX Transaction Log page will display.

   - 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 >| to show the next page of (older) entries.

   - Click |< to show the previous page of (newer) entries.

   - Click << 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 **Start Date** and **End Date** boxes, and then click **Show in Browser**.

- Dates are formatted as MM/DD/YYYY.

- The most recent log entries are shown first.

2. 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.**

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

1. On the Transaction Log page, use the date range boxes near the top of the page to specify the desired date range of entries to export.

   - 1,000 exported log entries will result in an approximately 0.5 megabyte file.

   - The **Transactions per Page** setting does not apply when log entries are supported.

2. Click **Save as CSV** for comma-separated values or **Save as TSV** for tab-separated values.

3. Use the browser Save dialog box to specify where the file will be stored.

4. 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 following fields are shown. These fields are also included when the transaction log is exported as a tab-separated (.TSV) or comma-separated (.CSV) file.

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

VIX Transaction Log Fields	
Name	**Description**
Date and Time	When the transaction was processed by the VIX. Formatted as MM-DD-YYYY, HH:MM:SS, AM/PM.
Time on VIX	The length of the transaction in milliseconds, beginning when the VIX receives a message and ending when the VIX begins to send the response.
ICN	The Integration Control Number used to uniquely identify the patient across the VA and DoD systems. (Note that the ICN is not equivalent to the VA patient ID, and is not considered Protected Health Information.)

VIX Transaction Log Fields	
Name	**Description**

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 will have 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.
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 will have 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."*

VIX Transaction Log Fields	
Name	**Description**
Throughput	The image transfer rate. Both the rate and the units of measurement (KB/sec, MB/sec are indicated). 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. 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 tracking purposes.
Data Source Protocol	The source of the data being handled: vistaimaging – Data from a VistA system mix,dx – DICOM data from a source outside of VistA (typically the DoD) vftp – Data from another VIX mix,ax – Non-DICOM (artifact) data from a source outside of VistA (typically the DoD)

VIX Transaction Log Fields	
Name	**Description**
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 PACS 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; 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 will be reflected 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).
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 the following table.

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 the DAS interface or HAIMS.
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 will be 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 will collect 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 will generate an email warning to data center administrator's (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 page 21 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 the following table:

Operation	When Performed
Purge Java logs	1 A.M. daily for Java log entries more than 30 days old.
Purge transaction log entries	2 A.M. daily for transaction log entries more than 30 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; when the VIX is implemented on the same cluster used for Imaging resources, the VIX is a part of the same resource group that is 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*.

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

| 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 will restart automatically once the server is restarted.
VIX service fatal error (server unaffected)	On a standalone server, the VIX service will restart itself automatically after 60 seconds, and continue 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 will automatically refresh any previously cached connections within 30 seconds to 1 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 will need 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 (8080 and 8443) 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 will increase 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 will restart automatically if the hosting server is restarted.

3.6.1. Checking the VIX Service: 2012 R2 Standalone Server

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**).

3. On the right side of the window, locate the Apache Tomcat service and verify that its status is **Started**.
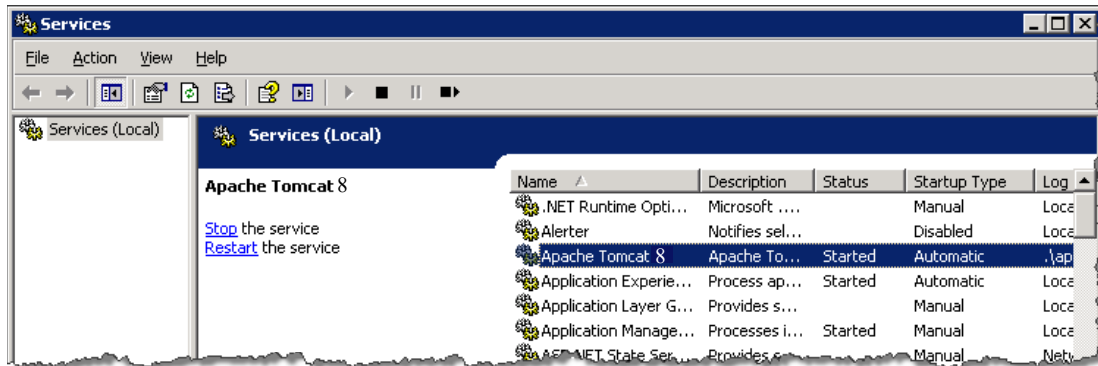
3.7.   Monitoring/Maintaining the VIX Viewer

The VIX Viewer hosts two independent services. These services show up as the VIX Viewer Service and the VIX Render Service.
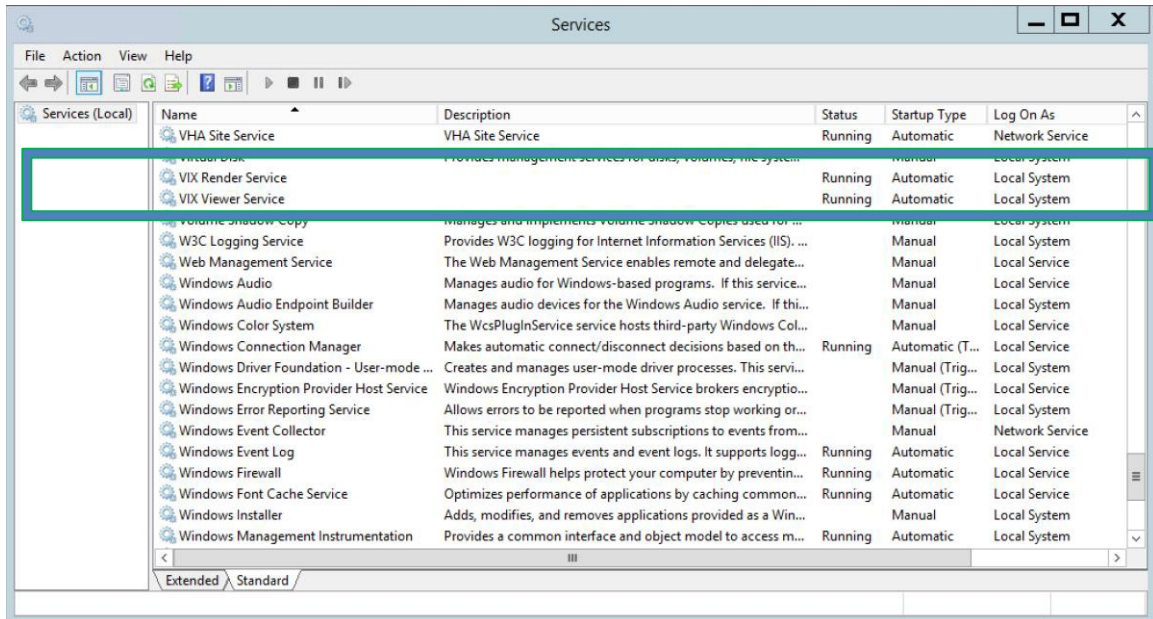
The Viewer and Render services must be operational for the site VIX to be able to provide viewing. To verify operation, one has to log into the consuming applications, select a patient with images, and display the images. If the operation fails, proceed to the trouble shooting section.

3.7.1.   Troubleshooting the VIX Viewer

Operation of the VIX 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

- The Microsoft SQL Express instance must up and 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 trouble shooting of VIX services.

To verify that that Microsoft SQL Express instance is operational, review the Render Service logs located in:

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

Look for any errors related to access to SQL server. In case the SQL server is failing, follow the steps outlined in Fixing the VIX Viewer Cache Errors.

3.7.1.1. Fixing the VIX Viewer Cache Errors

1. Stop the VIX Viewer and VIX Render Services
2. Delete all the files in the Viewer cache located in *<Cache Drive> :\VIXRenderCache*
3. Install and configure SQL Express

    a. Copy the SQL Express installation (SQLExpress_x64-12_0_2000_8.zip) to a local folder on the server

    b. Extract all the files

    c. Launch a command prompt window as a local Administrator

    d. In the command prompt window, navigate to the directory used for extracted files

    e. Run the following command: Setup/ConfigurationFile=ConfigurationFileInstall.ini
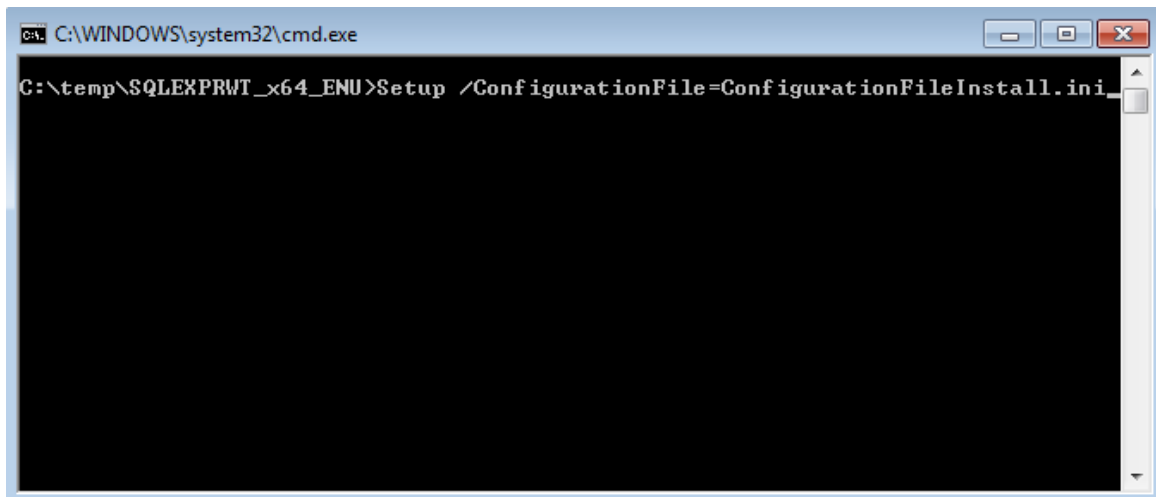
4. Review the console window and ensure no errors were reported
5. Restart the VIX Viewer and Render Services
6. Verify viewer operations by opening a few studies

3.7.1.2. Analyzing VIX 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 log for errors.

The logging level is controlled by the setting in the NLog.config file located in the directory above the logs.

```
<rules>

 <logger name="*" minlevel="Warn" writeTo="logfile" />

 </rules>

 </nlog>
```

To get more details, the minlevel property can be set to "Trace". The Trace level will generate a lot of logging, so it is advised to set it back to "Warn" for normal operation.

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 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 of it, 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:

4.1. Remote Metadata Retrieval

When a VIX is used to retrieve remote images, the image retrieval is always preceded by the retrieval of applicable metadata[*]. Also, in some cases such as the retrieval of an exam report, metadata retrieval is the only action needed to fulfill a clinician's data request.

Many Clinical Display or VistARad operations will 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 own local cache. If the metadata cannot be found locally, it is retrieved from the remote site.

Remote site type	How remote metadata is retrieved
VA site with VIX	The remote VIX retrieves the metadata, either from the remote VIX's own cache or from the remote site's VistA system.

---

[*]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.

Remote site type	How remote metadata is retrieved
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

The following table 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.

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 fresh 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

The following table 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.

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 will use whatever cached data is available and pull 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 as well.	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 New Image Viewer

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
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 own 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.

Remote Site Type	How Remote Image is Retrieved
VA site with VIX	The remote VIX retrieves the image, either from the remote VIX's own 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 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 or not there is a remote VIX involved can affect how a VIX fills a request for a remote image.

The following table 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).

Parameter	Requested by	VIX Compression Logic[*]
DIAGNOSTIC	Clinical Display Radiology Viewer and VistARad, VIX 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 of 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.

---

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

Parameter	Requested by	VIX Compression Logic[*]
DIAGNOSTIC UNCOMPRESSED	Clinical Display Full Resolution Viewer, VIX Viewer	If a remote VIX is present, it will automatically package 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.
REFERENCE	Clinical Display Radiology Viewer only, VIX 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 will be 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, VIX Viewer	The presence or absence of a remote VIX does not impact how thumbnail images are handled.

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.

The following table lists possible formats that the VIX can return based on image type. When multiple formats are listed, the VIX will check 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 will be converted to one of the possible formats before returning it to the requesting application.

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 will always attempt to convert the requested image to DICOM J2K if the header data is available.

> ** The local VIX will always attempt 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 from 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 will cache 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.

The following table lists retention periods based on the source and type of the data.

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

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 will need to re-run the VIX installation wizard to update your VIX's configuration information. For details, see the *VIX Installation Guide.*

4.5. Using the VIX Cache Manager

A VIX ache Manager function allows users to browse the VIX cache, identify corrupt data, and delete data as required. The cache browser is accessed using Internet Explorer 7 or later and Firefox 3 or later.

To access the VIX Cache Manager, go to http://<FQDN>:8080/CacheWeb (where <FQDN> is the fully qualified domain name of the individual host.

Note: The URL to the VIX Cache Manager is case sensitive.

4.5.1. Cache Organization

The data in the cache is arranged in a hierarchy with one or more of the following levels;

- data source (VA or DoD) and type (artifact, metadata, or image)

- repository (VA site or DoD facility)

- patient identifier (ICN for VA patients)

- study (group) identifier

- series and instance identifiers.

The source and type of the data are the most important factor in determining where an item is cached. When the VIX Cache Manager is opened in a browser the following screen displays:
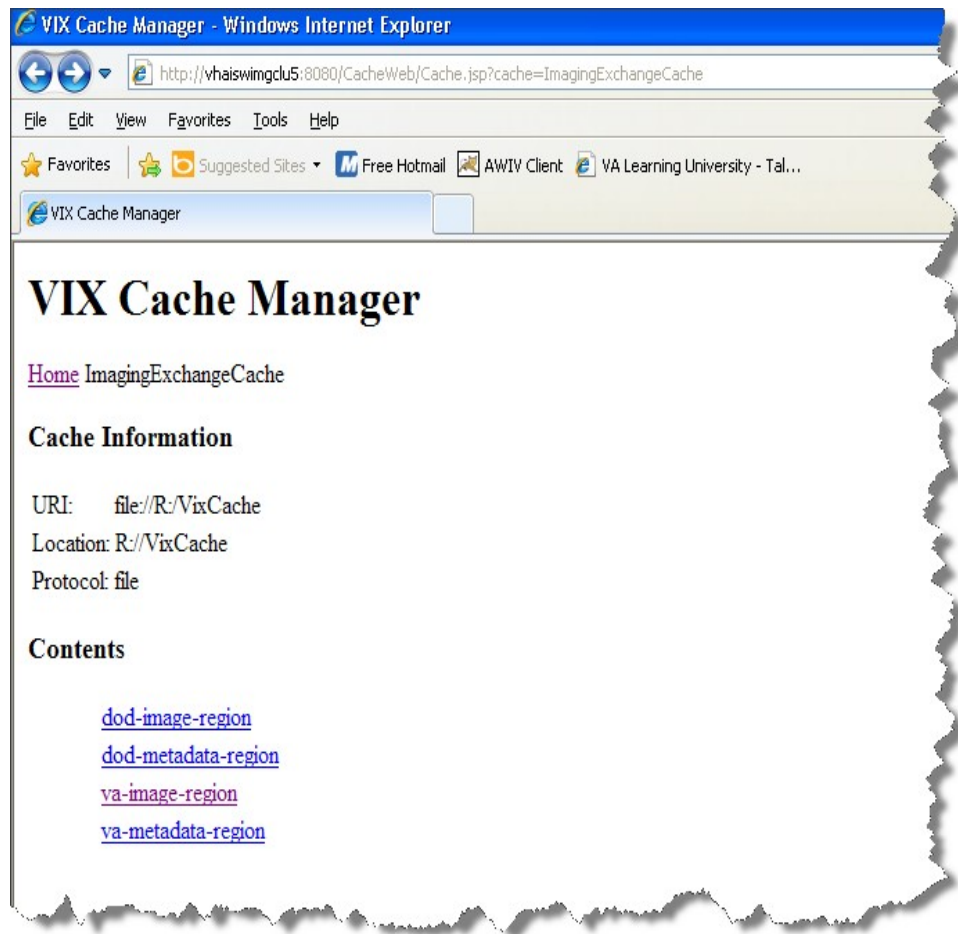
The items immediately under the cache name are called "regions" of the cache. Regions divide the items in the cache by the source of the item (VA versus anywhere else) and the type of the item (image versus anything else). A region defines the conditions under which a cache item is deleted from the cache.

Historically, it has been the case that anything that is not from the VA is from the DoD and anything that is not an image is metadata. Thus, a radiology image from the DoD will be found in the "dod-image-region" while the study text data from a VA site will be found in the "va-metadata-region".

4.5.1.1. Technical Specifics

The cache does not understand anything about sites, patients, or studies but operates on the concept of regions, groups, and instances. Regions are collections of similar items that have the same lifespan in the cache (i.e., 30 days since last use). Groups are collections of groups and instances. Instances are the cache items proper. Groups are

what is called a recursive data structure, a group can contain other groups, which in turn can contain still more groups. The cache limits that hierarchy to specific levels grouped by well-known business concepts (site, patient, etc.). Groups are also the basis that the cache deletes items. If no item in a group has been accessed within the region's lifespan then the entire group is deleted from the cache. If you think of the images in a study, then this makes more sense, if a study has not been accessed for 30 days, then the entire study is deleted from the cache. If none of the studies for a patient have been accessed within 30 days, then the whole patient is deleted from the cache.

Click the "va-image-region" region link and a list of cache groups will be displayed. You should see something like the next illustration, except that the cache contents will be different.
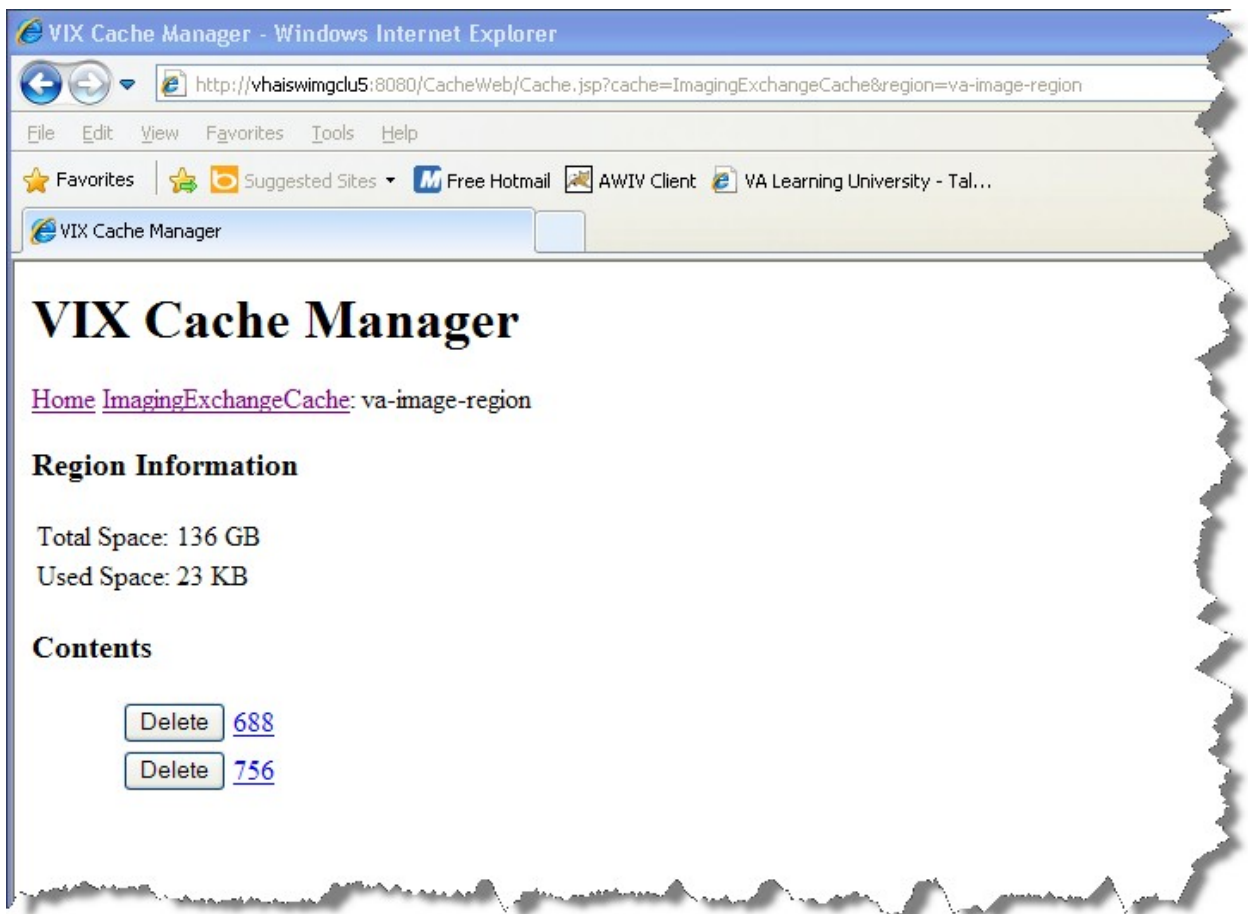
The VIX Cache Manager displays the name of the region in the breadcrumb at the top of the page, and a list of the image repositories in this region. To drill down into an image repository, click on the image repository number. To delete an entire image repository, click on the **Delete** button to the left.

You can drill down through the VIX cache using the links in the VIX Cache Manager. The levels of the cache–region, repository, patient, study, and image—appear as

hyperlinks in the breadcrumb at the top of the page. To delete an item in the cache at any level, click on the **Delete** button to the left.

4.5.1.2. The DoD Regions

DoD regions are organized by the community operation order identification (OID) number followed by the repository, the patient and then group identifiers of various sorts. The community OID is an identifier that an enterprise uses to identify itself on the Nationwide Health Information Network (NwHIN). For our purposes, the OIDs that you need are shown in the table below:

| OID	Enterprise
2.16.840.1.113883.3.42.10012.100001.207	DoD Radiology
2.16.840.1.113883.3.42.10012.100001.206	DoD Documents
2.16.840.1.113883.3.166 2.16.840.1.113883.6.233	VA Documents
1.3.6.1.4.1.3768	VA Radiology

Below the enterprise OID is a repository (a site in VA parlance). At this time, DoD documents always come from the Central HAIMS server and are identified as "central". Likewise, DoD radiology always comes from the DAS interface, identified as "200".

The DoD metadata region is only used for radiology study text data.

4.5.1.3. Cache Item Information

Clicking a cache item link will retrieve information about the item, such as the last time it was accessed and the size. This information may be useful in locating a specific item.

The size of a cache instance is the size of the file on disk (including its descendants); the size of a cache group is the sum of all of the groups and instances contained within it. The checksum, available only for cache instances, is the result of a mathematical calculation applied to the entire content of the instance. The checksum is used within the VIX to detect data errors. For an instance with the same identifiers, this value should always be the same on all VIX and on CVIX.
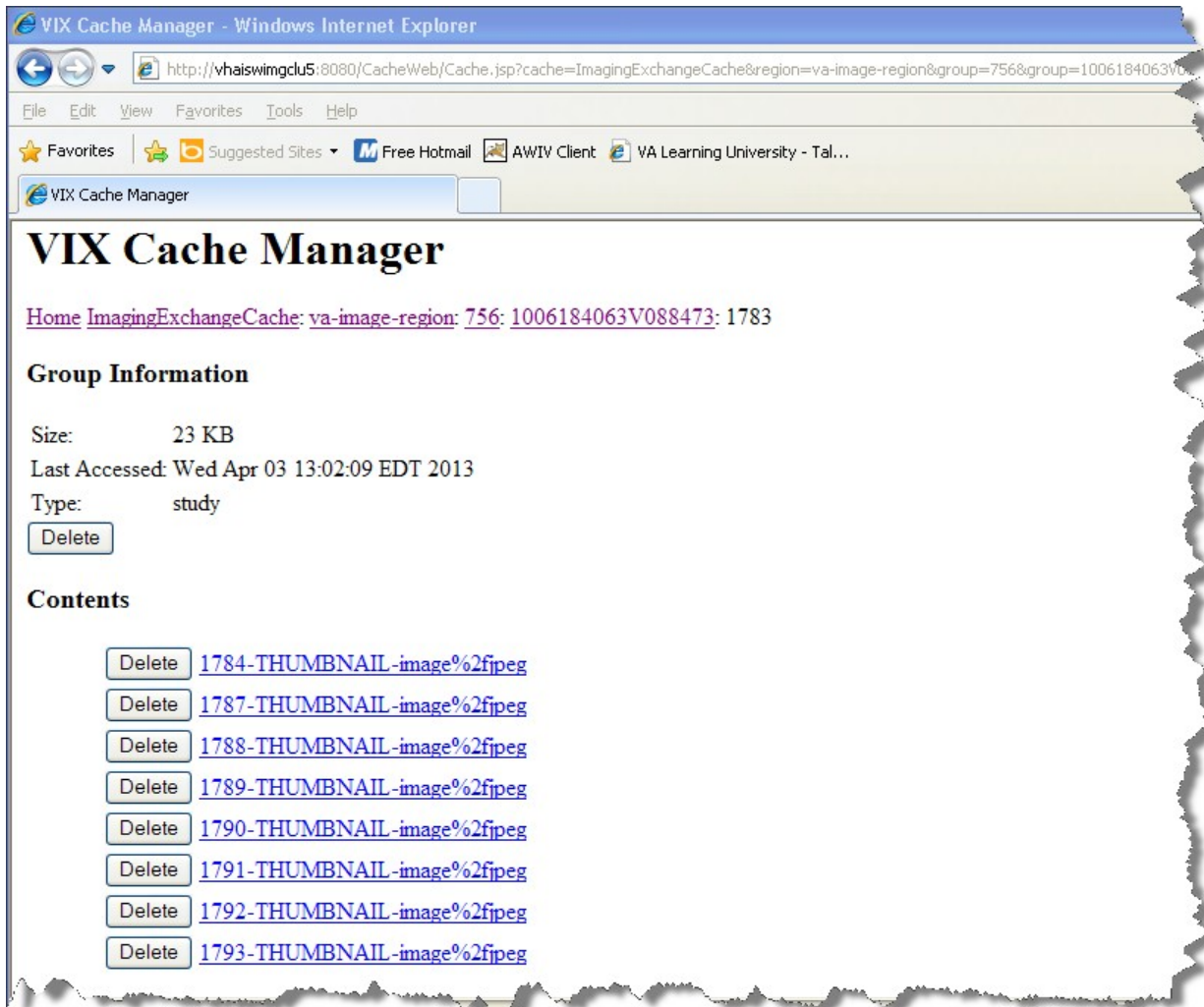
4.5.1.4. Cache Delete

Usually the cache is self-managing, determining the cached items that have not been used recently and deleting them. On rare occasions, a corrupt item may be cached. In this case, that corrupt data will be repeatedly served on request. Repeated requests are treated as user access and extend the time that the data stays in the cache. This cache item must be deleted from the cache manually.

To delete a cache item, collect as much identification information as you can. At a minimum, this must include whether the source is the VA or the DoD and, if it is a VA item, whether the image or a study (metadata) is causing problems and the site the data originated from. In addition the patient identifier must be known.

Once that information is collected, open the VIX Cache Manager and navigate through the hierarchy to either the corrupt item or to one of its parent groups (patient ID or study) if the item itself cannot be identified. Click on the **Delete** button to the left of the item and then confirm that you want the item deleted. The cache does not immediately delete

the item since it has to synchronize operations from all clients. It may take a few seconds or up to a minute before the item is actually deleted. Usually though, it will respond immediately that the item is deleted and the item will disappear from the VIX Cache Manager.

Finally, it is worth reinforcing that when an item is deleted from the cache it is not deleted from the original source of the data. If the VIX is asked for that item again it will simply notice that it is not in its cache and will retrieve it from the original data source and re-cache it. The effect to the user is a slight delay, nothing more.

The minimal deleterious effect of deleting a cache item may lead someone to delete "good" cache items to get all of the "bad" ones. This is not an issue, since the VIX will simply re-cache the items when they are requested again.

4.6.   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.

4.6.1.   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.

4.6.1.1.   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 listed below, 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.

Access Type Value	Description
RVVAVA	A locally stored image that a remote VA Clinical Display or AWIV 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.

Access Type Value	Description
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 actually 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.

4.6.1.2. VIX-Related Additional Data Values

The VIX will also populate the Additional Data field (#100) based on data provided by the requesting application.

Because the VIX adds a lot of information to this single free-text field, the VIX uses "|" characters to organize the Additional Data field into four "parts". Note that these parts exist for organizational purposes only, and are not considered discreet pieces in the FileMan sense.

If Access Type is...	Then Additional Data contains...			
	Part 1	**Part 2**	**Part 3**	**Part 4**
RVVAVA	empty	VIX transaction ID	Requesting VA site ID	empty
RVVADOD	empty	VIX transaction ID	Requesting DoD 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*			

4.6.1.3. 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|
```

4.6.1.4.

4.6.1.5.   Example – RVVADOD Access Type

```
^MAG(2006.95,610535,0)=610535^RVVADOD^1376^8820^DOD^XXX^3100302.094747^
1023^1^6557^660
^MAG(2006.95,610535,100)=|5aafabc4-2361-4a34-b843-5aad4163620c
XX.XXX.MIL/HP0000-PZ01|DoDUsername
```

4.6.1.6.   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|
```

4.6.1.7.   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}
```

4.6.2.   Additional Client Logging

4.6.2.1.   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.

- Certain details (such as 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.

4.6.2.2.   VistARad Logging of VIX Operations

Refer to VistARad documentation for details.

4.7.   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 will impact the time needed to complete the

retrieval. If a request for data cannot be completed in a timely manner, the local VIX will cancel its request. This prevents excessive delays in client applications (Clinical Display and VistARad) that use the VIX.

The following table summarizes VIX connection timeout parameters based on the type of remote system and data involved.

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 will wait up to 45 seconds to retrieve DoD metadata before sending a timeout message to the local VIX. For images, the CVIX will wait 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 will pass 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 will send a "Try Again" message to the local requesting application (such as Clinical Display or VistARad) In most cases, the requested data will be available within a minute or so and a subsequent request will be 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 will send a "partial" message to the local requesting application.

4.8.   Troubleshooting

The following information may help diagnose potential VIX-related image sharing problems.

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 8080 and 8443 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 will make Clinical Display use pre-VIX remote image views, which is not dependent on a VIX. However, pre-VIX remote image views cannot be used to access DoD images, and in some cases they will 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.
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 will 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 will use 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 will continue to retrieve images but will bypass its cache.) If the VIX cache is full, contact customer support.

Symptom	Check
	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 will still retrieve the image and store it in the VIX cache, but Clinical Display or VistARad may 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 will renew the request and the data will be retrieved by the VIX if it is available.
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 will send all available metadata back to local VIX, and will also use the "partial" flag to indicate that the data is potentially incomplete. If this issue persists, especially for multiple patients, contact customer support.

Symptom	Check
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 is shown 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 its configuration. By default both parameters are enabled and the VIX uses both ways to process ROI disclosure requests at the same time.

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 will not process ROI requests. It will display 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 will need 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 it is processing an ROI request because of a network disconnection or a VIX restart, the ROI disclosure will be completed only if periodic processing is enabled. If periodic processing is not enabled, the request will not be completed.

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 will 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, which is 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 will 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. The credentials can be the credentials of the same service account that the DICOM Gateway and the HDIG use.

For more information about setting the access and verify codes of the account, see the *VistA Imaging 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 the Release of Information (ROI) Configuration page. When there is a message, this means that there is a problem with the current configuration and you should take actions 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:
http://<*VIXHostName*>:8080/ROIWebApp
where <*VIXHostName*> is the name of the fully qualified domain name (FQDN) of the server on which the VIX is installed

The following image shows the ROI Processing 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.

The following table explains the information that the VIX provides for ROI processing.

Group	Field	Description
ROI Statistics		
	Disclosure Requests	The number of requests made to the VIX for ROI disclosures.
	Disclosures Completed Successfully	The number of successfully completed ROI disclosures.
	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).
	Disclosures Failed Processing	The number of ROI disclosures that did not complete successfully.
	Disclosures Cancelled	The number of ROI disclosures that were cancelled before completion.
Periodic Processing		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.
	Configuration Enabled	When this parameter is set to true, periodic processing is enabled and the VIX processes ROI requests periodically in the background.
	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.
Completed Disclosures Purge Processing		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.
	Configuration Enabled	Indicates if completed disclosures purge processing is enabled. When this parameter is set to true, completed disclosures purge processing is enabled.

| Group	Field	Description
	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 it gets the request. 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*.
	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		To change any of the VIX ROI configuration settings click on the Configure ROI Options link. Accessing this configuration page requires VistA credentials for a user with the MAG VIX ADMIN security key.
Invalid Credentials Email Notification		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 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 will come from the vix@va.gov email account. The values are specified when the VIX is installed. Users with the MAG VIX ADMIN key can modify these values.

Group	Field	Description
Update the Invalid Credentials Email Notification Addresses		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		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 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 with the ROI periodic processing credentials.

To change the ROI processing parameters of the VIX:

1. In your browser, open the URL for the ROI Statistics page:
   http://<*VIXHostName*>:8080/ROIWebApp
   where <*VIXHostName*> is the name of the fully qualified domain name (FQDN) of the computer on which the VIX is installed

2. In the ROI Processing Status page, click the link **Configure ROI Options**.

3. In the dialog box that displays, enter the access and verify code of the user with the MAG VIX ADMIN security key. Then, click **OK**.
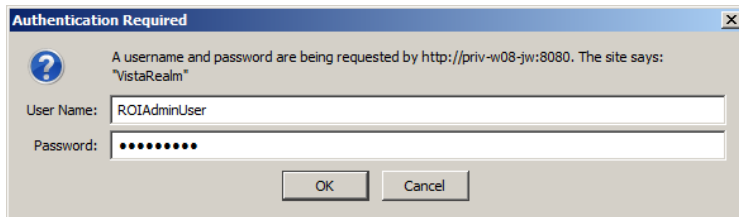
4. In the Configure Release of Information (ROI) page, modify the configuration parameters as desired. For information about the parameters, see *Information the ROI Processing Status Page Provides*.

5. Click the **Save Configuration** button to save the changes. The page will be refreshed 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 will come from the vix@va.gov 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:
   http://<*VIXHostName*>:8080/ROIWebApp
   where **<*VIXHostName*>** is the name of the fully qualified domain name (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, enter the access and verify code of the user with the MAG VIX ADMIN security key. Then, click **OK**.
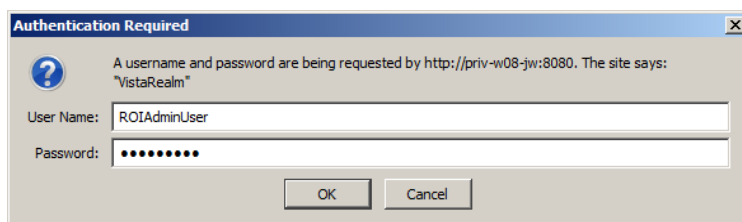
4. In the Configure Invalid Credentials Email Notification Addresses page, modify the list of addresses as desired. The list can contain multiple addresses separated by commas and/or an email group.
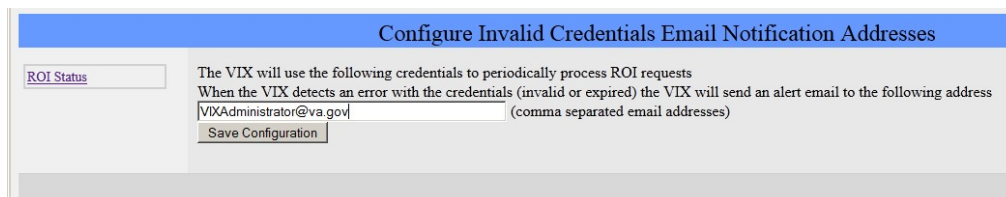
5. Click the **Save Configuration** button to save the changes. The page will be refreshed with a status message indicating if the changes were saved or if there was an error.

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. The following table summarizes each VIX interface.

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.

Interface Name	Description
MIX,DX Interface	Handles DICOM metadata and image requests from DoD providers.
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 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. The following table summarizes each VIX data source. These data sources are identified in the Data Source Protocol field in the VIX transaction log.

Data Source Name	Description
vistaimaging	Retrieves data from a VistA System using RPCs
mix,dx	Retrieves DICOM data from the DoD via the DAS framework's mix,dx interface.
vftp	Retrieves data from other VIXes (or the CVIX/RVIX) 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 DICOM Connectivity Framework (DCF) toolkit files

\Program Files\Apache Software Foundation\Tomcat 8.1.45

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\jre1.8.0_121

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 following Java logs reside in \Program Files\Apache Software Foundation\Tomcat 6.0\Logs. For active logs, a new instance is generated each day and the older instances are retained with the date appended to their filenames.

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.   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 below. RPCs from other packages are listed in the next section.

6.2.1.1.   MAG RPCs Used by the VIX

MAG RPCs used by the VIX	
RPC Name	**Description**
MAG BROKER SECURITY Routine: BSE^MAGS2BSE	Returns a BSE token from BSE (Broker Security Enhancement) XUS SET VISITOR.

MAG RPCs used by the VIX	
RPC Name	**Description**
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 will return an error message indicating the problem. Modified by MAG*3.0*118 to – optionally – filter out procedure types **B**road and **P**arent.
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 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.
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 will return 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).

MAG RPCs used by the VIX	
RPC Name	**Description**
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 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.
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.

MAG RPCs used by the VIX	
RPC Name	**Description**
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.
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.

MAG RPCs used by the VIX	
RPC Name	**Description**
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).

6.2.1.2. Non-MAG RPCs used by the VIX

The VIX uses the following RPCs from other VistA packages. 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*

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 parameter set to yes and 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 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 Integration Control Number (ICN), this will return the patient Internal Entry Number (IEN) from the PATIENT file (#2).
VAFCTFU GET TREATING LIST Routine: TFL^VAFCTFU1	Given a patient DFN, this will return a list of treating facilities.
XUS AV CODE Routine: VALIDAV^XUSRB	Checks to see whether a 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 DUZ(2) during sign-on.
XUS SIGNON SETUP Routine: SETUP^XUSRB	Establishes environment necessary for DHCP sign-on.
XWB CREATE CONTEXT Routine: CRCONTXT^XWBSEC	Establishes context on the server that the Broker will check before executing any other remote procedure.
XWB GET VARIABLE VALUE Routine: VARVAL^XWBLIB	Accepts the name of a variable that will be evaluated and its value returned to the caller.

6.2.2.   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 does this using 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.

6.2.3.   Exported Menu Options

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

6.2.4.   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, VIX 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*.

6.2.5.   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 that is 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](#)
- [Sun JRE](#)
- [Laurel Bridge DCF toolkit](#)
- [Aware JPEG2000 toolkit](#)

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.X framework is needed to install and update the VIX software.

Patches for .NET 4.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.   Sun JRE

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

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

6.3.4.   Laurel Bridge DCF Toolkit

The Laurel Bridge DICOM Connectivity Framework (DCF) toolkit, version 3.3.X, 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 will require an updated license from Laurel Bridge. If a new or updated license is needed, contact the REDACTED mail group.

Version 3.3.X 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.

This toolkit requires the presence of a compatible *Microsoft Visual C++ 2005 Redistributable Package (x86)*. If it is not present, C++ will be installed automatically as a part of the VIX setup process.

6.3.5.   Aware JPEG2000 Toolkit License

For information regarding the Aware Toolkit License, see the *VistA Imaging Exchange (VIX) Service Installation Guide.*

7.   Appendix: Image Sharing and DICOM Images

Images are delivered to VA sites by the CVIX and originate from the Data Access Service (DAS) framework.

7.1.   DoD DICOM Object Filtering

Study information (including reports) for studies associated with all DICOM modality types can be retrieved from the DoD by VA sites with a local VIX.

However, for certain DICOM object types, the associated objects are not actually images and Clinical Display and VistARad cannot display them. For these types of DICOM studies, the VIX will provide the metadata (including reports), but will not provide the image counts and/or image locations. The VIX blocks the following DICOM modality types, and only if the data originates from the DoD.

DoD objects not displayable at the VA (metadata and reports remain accessible)	
DICOM Modality Description	**DICOM Identifier**
Audio	AU
Document *(Used for DICOM encapsulated secondary captures and scanned documents. Not equivalent to MS Word .doc files)*	DOC
Cardiac Electrophysiology (waveforms)	EPS
Fiducials	FID
Hemodynamic Waveform	HD
Key Object Selection	KO
MR Spectroscopy	MS
Presentation State (all types)	PR
Respiratory Waveform	RESP
Radiotherapy Structure Set	RTSTRUCT
RT Treatment Record	RTRECORD
Radiotherapy Dose	RTDOSE
Radiotherapy Plan	RTPLAN
Structured Report (all types)	SR

7.2. VA DICOM Images Provided to DoD

DoD clinicians can request the following types of exams from the VA via the CVIX:

VA DICOM Objects 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
Radio Fluoroscopy	RF, RAD RF

VA DICOM Objects Provided to DoD	
DICOM Modality Description	**DoD Identifiers**
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

8. Index