

# **VistA Imaging Exchange (VIX) VIX Enhancements**

**MAG\*3.0\*348**

## **Central VistA Imaging Exchange (CVIX) Administrator's Guide and Product Operations Manual (POM)**



**July 2023**

**Version 16.0**

**Department of Veterans Affairs (VA)**

**Office of Information and Technology (OIT)**

# CVIX Administrator's Guide and Product Operations Manual

## July 2023

### 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  
Veterans Affairs Internet:  
<http://www.va.gov/imaging>

VA intranet **REDACTED**

### Revision History

Date	Revision	Description	Author
07/01/2023	16.0	Initial draft for MAG*3.0*348.	VA IT VistA Imaging Technical team
05/03/2023	15.0	Initial draft for MAG*3.0*329.	VA IT VistA Imaging Technical team
11/03/2022	14.0	Initial draft for MAG*3.0*303.	VA IT VistA Imaging Technical team
06/01/2022	13.6	Updates for MAG*3.0*269 release date.	VA IT VistA Imaging Technical team
05/02/2022	13.5	Updates for P269 T5.	VA IT VistA Imaging Technical team
04/20/2022	13.4	Updates for P269 T4.	VA IT VistA Imaging Technical team
02/07/2022	13.3	Updates for P269 T3.	VA IT VistA Imaging Technical team
12/21/2021	13.2	Updates for P269 T2.	VA IT VistA Imaging Technical team

Date	Revision	Description	Author
11/30/2021	13.1	Updates for P269 based on feedback from review.	VA IT VistA Imaging Technical team
05/31/2021	13.0	Initial draft for P269.	VA IT VistA Imaging Technical team
02/28/2021	12.1	Updates for MAG*3.0*254 to include DoD images to VA Clinicians section.	VA IT VistA Imaging Technical team
01/31/2021	12.0	Updates for MAG*3.0*254.	VA IT VistA Imaging Technical team
07/31/2020	11.0	MAG*3.0*249 Updates.	REDACTED
03/31/2019	10.0	Additional MAG*3.0*205 Updates.	REDACTED
02/28/2019	9.0	Additional MAG*3.0*205 Updates.	REDACTED
08/31/2018	8.0	Additional MAG*3.0*205 Updates.	REDACTED
07/31/2018	7.0	Additional MAG*3.0*205 Updates.	REDACTED
05/31/2018	6.0	Additional MAG*3.0*205 Updates.	REDACTED
04/30/2018	5.0	Revised for MAG*3.0*205.	REDACTED
09/30/2017	4.0	Revised for MAG*3.0*171.	REDACTED
08/31/2013	3.0	Revised for MAG*3.0*34/116/118, 119, 127, 129. Revised sections Using the Cache Browser and Cache Delete.	REDACTED
07/31/2013	2.0	Revised for MAG*3.0*124. Revised sections Using the Cache Browser and Cache Delete.	REDACTED
03/31/2013	1.0	Document created for Imaging patch MAG*3.0*124. Expanded CVIX Transition Log section with step-by-step instructions.	REDACTED

## Table of Contents

<b>1. Introduction .....</b>	<b>11</b>
1.1. Terms of Use .....	11
1.2. Intended Audience .....	11
1.3. Document Conventions .....	11
1.4. Related Information .....	12
<b>2. CVIX Overview.....</b>	<b>13</b>
2.1. CVIX Major Functions .....	13
2.1.1. Provide DoD Images to VA Clinicians .....	13
2.1.2. Provide VA images to DoD requestors.....	16
2.1.3. Provide VA and DoD images to Image Viewer.....	17
2.1.4. Host the VistA Site Service .....	18
2.2. CVIX Physical and Logical Description.....	18
2.3. CVIX Operational Priority .....	19
2.4. CVIX Dependencies .....	19
2.5. The CVIX, VIXes, and Multidivisional VA Sites .....	20
2.6. CVIX Connection Security .....	21
<b>3. CVIX General Operations .....</b>	<b>22</b>
3.1. CVIX Monitoring .....	22
3.2. Using the CVIX Transaction Log.....	22
3.2.1. CVIX Transaction Log Fields .....	24
3.2.2. CVIX Transaction Log Fields (Export Only) .....	27
3.2.3. Logging on Remote VistA Systems.....	28
3.3. Using the Cache Manager .....	28
3.3.1. Cache Organization .....	29
3.3.2. Technical Specifics .....	30
3.3.3. The DoD Regions .....	31
3.3.4. Cache Item Information.....	32
3.3.5. Cache Delete .....	32
3.4. User Notifications .....	33
3.5. Cluster-related Activities .....	33
3.5.1. CVIX cluster: take the node offline .....	33
3.5.2. CVIX cluster: bring the node online.....	33
3.6. CVIX Planned Startup and Shutdown.....	33
3.6.1. Planned Full CVIX Shutdown.....	33

3.6.2.	Planned Full CVIX Startup .....	34
<b>3.7.</b>	<b>CVIX Data Retention and Purges .....</b>	<b>34</b>
<b>3.8.</b>	<b>CVIX and Backups .....</b>	<b>34</b>
<b>3.9.</b>	<b>Critical Metrics .....</b>	<b>35</b>
<b>3.10.</b>	<b>CVIX and User Management.....</b>	<b>35</b>
<b>3.11.</b>	<b>Configurations for DoD images Provided to VA Clinicians.....</b>	<b>35</b>
3.11.1.	Additional Configurations for ECIA only for DoD images Provided to VA Clinicians.....	36
<b>3.12.</b>	<b>Configure DICOM SCP Functionality.....</b>	<b>41</b>
3.12.1.	AE Titles Configuration .....	41
3.12.2.	Laurel Bridge AE Titles Configuration on CVIX.....	42
3.12.3.	AE Titles Configuration on DICOM SCU .....	43
3.12.4.	Tomcat DICOM SCP Configuration.....	43
3.12.5.	Laurel Bridge DICOM SCP Configuration .....	52
<b>3.13.</b>	<b>Configure ID Conversion .....</b>	<b>53</b>
<b>4.</b>	<b>VistA Site Service .....</b>	<b>55</b>
4.1.	VistA Site Service Overview.....	55
4.2.	Checking the Site Service .....	55
4.3.	Updating Site Service Data.....	55
<b>5.</b>	<b>CVIX Image Sharing .....</b>	<b>57</b>
5.1.	Remote Metadata Retrieval .....	57
5.2.	Remote Image Retrieval.....	58
5.3.	Caching of Metadata and Images .....	59
5.3.1.	Cache Retention Periods .....	59
5.3.2.	Cache Location and Structure.....	60
5.4.	Image Sharing and CVIX Timeouts .....	60
<b>6.</b>	<b>VIX Log Collector Service .....</b>	<b>62</b>
6.1.	VIX Log Collector Overview .....	62
6.2.	Log Collector Automatic Emails .....	62
6.3.	Archived Transaction Log Storage Area.....	63
6.4.	Excluding a VIX from Log Collection .....	63
<b>7.</b>	<b>CVIX Troubleshooting.....</b>	<b>65</b>
7.1.	Routine Errors .....	65
7.1.1.	Connectivity .....	65
7.1.2.	Timeouts .....	65

7.1.3.	Security .....	65
7.1.4.	Station 200 Issues .....	66
<b>7.2.</b>	<b>Significant Errors .....</b>	<b>66</b>
7.2.1.	Error Logs .....	66
<b>7.3.</b>	<b>Unplanned Shutdowns .....</b>	<b>66</b>
7.3.1.	Recovering after unplanned restart of a single CVIX server .....	66
7.3.2.	Recovering after unplanned reboot of a single load balancer .....	67
7.3.3.	Recovering after an unscheduled power loss to all components .....	67
<b>7.4.</b>	<b>System Recovery .....</b>	<b>67</b>
7.4.1.	Back-out Procedures.....	67
7.4.2.	Rollback Procedures .....	69
<b>7.5.</b>	<b>CVIX Support .....</b>	<b>69</b>
<b>8.</b>	<b>CVIX Reference/Software Description .....</b>	<b>70</b>
<b>8.1.</b>	<b>CVIX Java Components .....</b>	<b>70</b>
8.1.1.	CVIX Servlet Container .....	70
8.1.2.	CVIX Security Realms.....	70
8.1.3.	CVIX Interfaces.....	70
8.1.4.	CVIX Core.....	71
8.1.5.	CVIX Data Sources .....	71
<b>8.2.</b>	<b>Java Installation Locations .....</b>	<b>71</b>
8.2.1.	CVIX folders on the System Drive.....	71
8.2.2.	Java Logs.....	72
<b>8.3.</b>	<b>VistA/M Information .....</b>	<b>73</b>
8.3.1.	RPCs used by the CVIX.....	73
8.3.2.	Non-MAG RPCs used by the CVIX.....	75
8.3.3.	Database Information.....	76
8.3.4.	Exported Menu Options .....	76
8.3.5.	Security Keys .....	76
<b>8.4.</b>	<b>Other VIX Components .....</b>	<b>76</b>
8.4.1.	CVIX Security Certificates .....	77
8.4.2.	.NET .....	77
8.4.3.	JRE .....	77
8.4.4.	Laurel Bridge DCF Toolkit.....	77
8.4.5.	SQLite .....	78
8.4.6.	Aware JPEG2000 Toolkit.....	78
8.4.7.	LibreOffice.....	78

<b>9. Operations and Maintenance Responsibilities/RACI .....</b>	<b>79</b>
<b>10. Appendix A: Image Sharing and DICOM Images.....</b>	<b>81</b>
10.1. DoD DICOM Object Filtering.....	81
<b>11. Appendix B: CVIX Tools .....</b>	<b>82</b>
<b>12. Appendix C: VIX Viewer Dashboard.....</b>	<b>84</b>
12.1. VIX Viewer Dashboard: Homepage.....	85
12.2. VIX Viewer Dashboard: Logs .....	85
12.3. VIX Viewer Dashboard: Search .....	86
12.4. VIX Viewer Dashboard: System Preferences .....	86
12.4.1. Annotation Preferences.....	87
12.4.2. Cine Preferences .....	91
12.4.3. Layout Preferences .....	92
12.4.4. Copy Attributes.....	92
12.4.5. Log Preferences.....	93
12.5. VIX Viewer Dashboard: Status .....	93
<b>13. Definitions, Acronyms, and Abbreviations.....</b>	<b>94</b>

## Table of Figures

Figure 1: DoD-to-VA Image Sharing .....	14
Figure 2: VA-to-DOD Image Sharing .....	16
Figure 3: Data Flow for VIX Viewer Applications .....	17
Figure 4: VIX Cache Manager Initial Screen Display .....	29
Figure 5: VIX Cache Manager Region Information Display Example .....	30
Figure 6: VIX Cache Manager DOD Region Display with Delete Function.....	31
Figure 7: Sample MIXDataSource-1.0.config file - Bottom Portion .....	36
Figure 8: Sample MIXDataSource-1.0.config file - Top Portion .....	39
Figure 9: Sample MIXDataSource-1.0.config file - Middle Portion.....	40
Figure 10: Sample AE Titles Configuration File .....	42
Figure 11: Sample AE Titles Configuration File Filled .....	43
Figure 12: Sample DICOM SCP Configuration File .....	45
Figure 13: Example DICOM SCP Configuration File .....	46
Figure 14: Sample DICOM SCP Configuration File .....	50
Figure 15: Sample DICOM SCP Configuration File with Multiple DICOM SCU Calling AE Titles .....	51
Figure 16: Sample DicomScpConfig Configuration File.....	52
Figure 17: Sample IdConversionConfiguration.config file .....	54
Figure 18: CVIX Folder Structure.....	60
Figure 19: Transaction Log File Display Example .....	63
Figure 20: Login Page.....	83
Figure 21: VIX Viewer Dashboard: Homepage.....	85
Figure 22: VIX Viewer Dashboard: Logs.....	85
Figure 23: VIX Viewer Dashboard: Search .....	86
Figure 24: Annotation Preferences: Annotation .....	87
Figure 25: Annotation Preferences: Measurement .....	88
Figure 26: Annotation Preferences: Eclipse and Rectangle .....	89
Figure 27: Annotation Preferences: Label .....	89
Figure 28: Annotation Preferences: Text .....	90
Figure 29: Annotation Preferences: Mitral and Aortic .....	91
Figure 30: Cine Preferences .....	91
Figure 31: Layout Preferences.....	92
Figure 32: Copy Attributes Preferences.....	92
Figure 33: Log Preferences .....	93



Figure 34: VIX Viewer Dashboard: Status .....93

## Table of Tables

Table 1: DoD Images Available by Type and Source for VA Viewer .....	15
Table 2: Anticipated Operational Priority of the CVIX Broken Out by Function .....	19
Table 3: CVIX System Requirements .....	20
Table 4: Data Path Based on Number of Site VIXes .....	20
Table 5: Descriptions of CVIX Transaction Log Fields .....	24
Table 6: Descriptions of CVIX Transaction Log Fields for Export Only .....	27
Table 7: DoD Image Order Identification Numbers (OIDs) .....	31
Table 8: CVIX Purge Schedule .....	34
Table 9: Critical Metrics .....	35
Table 10: Types and Sources of Metadata requested by Application.....	57
Table 11: VIX Image Quality Parameters .....	59
Table 12: Image Data Retention Periods .....	60
Table 13: CVIX Connection Timeout Parameters .....	61
Table 14: CVIX Interfaces .....	70
Table 15: CVIX Data Sources .....	71
Table 16: MAG (VistA Imaging) RPCs Used by the CVIX .....	73
Table 17: Non-MAG RPCs used by the CVIX.....	75
Table 18: Types of Support with Production Environment Location(s) as Appropriate.....	79
Table 19: DICOM Modality Types Blocked at the VA if Originating from the DoD.....	81
Table 20: List of URLs .....	82
Table 21: Definitions, Acronyms, and Abbreviations .....	94

# 1. Introduction

This document explains how to maintain and administer the Central VistA Imaging Exchange (CVIX) service.

The CVIX is a special implementation of the VistA Imaging Exchange (VIX) that resides in the VA AWS cloud. The CVIX facilitates data sharing with the Department of Defense (DoD) across organizational boundaries. The CVIX also supports image data access for VA users not associated with a specific VistA (MyHealtheVet, VBA Claims, Joint Legacy Viewer (JLV), etc.).

This document assumes that the CVIX is installed and configured. For information about installation and initial configuration, contact the VistA Imaging development group.

## 1.1. Terms of Use

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

**Caution:** 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 CVIX (as a component of VistA Imaging) as a medical device. Unauthorized modifications to VistA Imaging, including the CVIX, such as installing unapproved software, will adulterate the medical device. The use of an adulterated medical device violates US federal law (21CFR820).

Because software distribution/inventory management tools can install inappropriate or unapproved software without a local administrator's knowledge, sites must exclude the CVIX from such system management tools.

## 1.2. Intended Audience

This document is intended for the VA data center personnel responsible for managing and monitoring the CVIX.

This document presumes a working knowledge of the VistA environment and VistA Imaging components. It presumes intermediate-to-advanced knowledge of Windows server administration and Windows cluster administration.

## 1.3. Document Conventions

This document uses the following typographic conventions:

- Controls, options, and button names are shown in **Bold**.

- A vertical bar is used to separate successive menu choices. For example: “Click **File** | **Open**” means: “Click the **File** menu; then click the **Open** option.”
- Keyboard key names are shown in bold and in brackets.
- Sample output is shown in monospace.
- Important or required information is shown in a **Note**.

## 1.4. Related Information

In addition to this manual, the following documents contain information about the CVIX:

MAG\*3.0\*83 DoD VistA Imaging Exchange Service Patch Description, available at **REDACTED**

MAG\*3.0\*104 Central VistA Imaging Exchange (CVIX) Patch Description available at **REDACTED**

MAG\*3.0\*129 CVIX Patch Description available at **REDACTED**

MAG\*3.0\*165 CVIX Patch Description available at **REDACTED**

MAG\*3.0\*171 Patch Description available at **REDACTED**

MAG\*3.0\*205 Patch Description available at **REDACTED**

MAG\*3.0\*249 Patch Description available at **REDACTED**

MAG\*3.0\*254 Patch Description available at **REDACTED**

VIX Installation Guide available at **REDACTED**

**NOTE:** This manual serves as both a Product Operations Manual (POM) and a System Administrator’s Guide.

## 2. CVIX Overview

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

- CVIX Major Functions
- CVIX Physical and Logical Description
- CVIX Operational Priority
- CVIX Dependencies
- The CVIX, VIXes, and Multidivisional VA Sites
- CVIX Connection Security

### 2.1. CVIX Major Functions

The CVIX's major functions are:

- Provide the Department of Defense (DoD) images to VA clinicians.
- Provide VA images to DoD clinicians.
- Provide VA/ DoD images to JLV/ Image Viewer users.
- Host the VistA Site Service, the repository of connection information used by various Imaging components.
- Host the VIX log collector.
- Host the VIX functionality to allow consuming applications to obtain metadata and images.

Each of these functions is described in the following sections.

**NOTE:** The VIX Log Collector Service is installed on the same hardware allocated for the CVIX but is completely independent of the CVIX. For more information about the VIX Log Collector, see *VIX Log Collector Service*.

#### 2.1.1. Provide DoD Images to VA Clinicians

The CVIX provides a single point of access to the DoD image sources for shared VA/DoD patients (patients with IDs correlated in the VistA Master Veteran Index). At sites that have implemented a VIX, VA clinicians can access these images via the CVIX using the Clinical Display, JLV/ Image Viewer, and VistARad applications.

The flow of DoD images through a CVIX is illustrated in Figure 1. This complexity is not evident to the VA clinicians; they simply use Clinical Display or VistARad to select the desired images.

**Figure 1: DoD-to-VA Image Sharing**

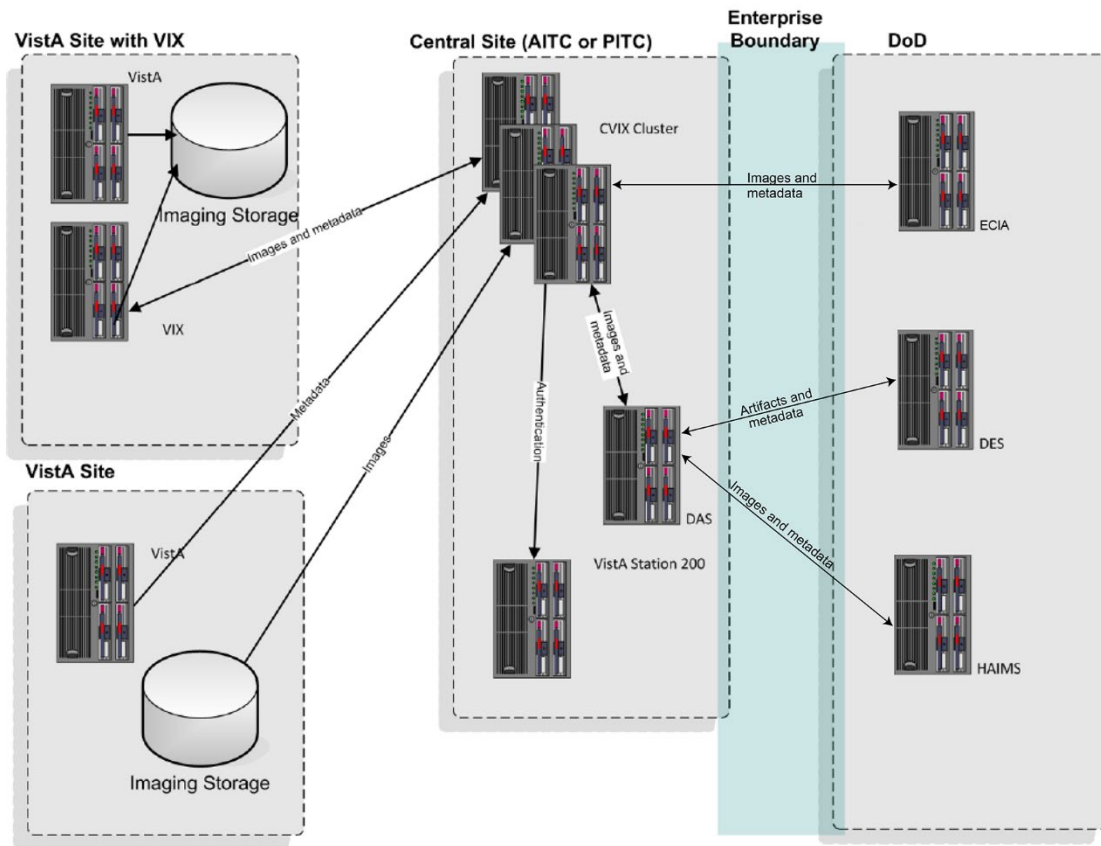


Table 1 details the types of DoD images that can be retrieved and where they originate from.

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

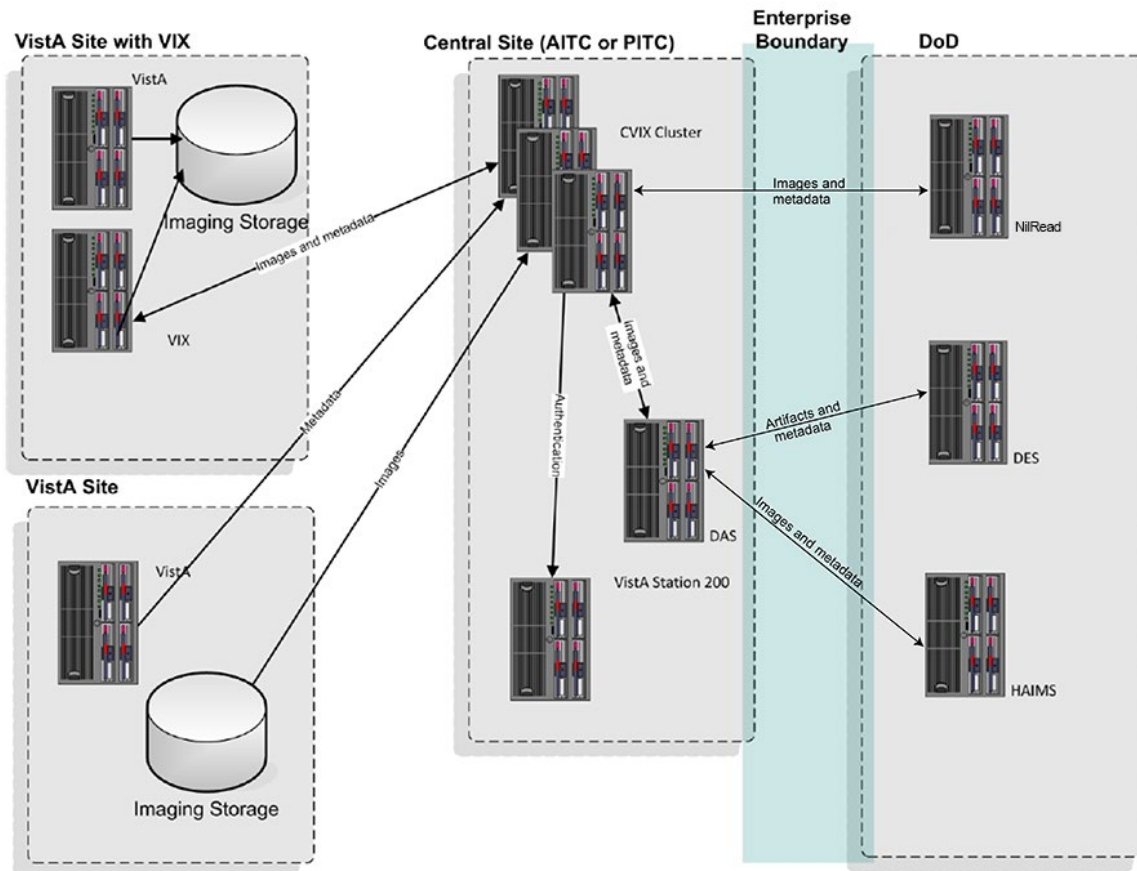
**Table 1: DoD Images Available by Type and Source for VA Viewer**

DoD Image category	DoD source	Viewable in VA VistA using
DoD DICOM (radiology)	Available from participating DoD facilities via the ECIA, which is through the CVIX. Note: For a list of DoD participating facilities and information about the types of DICOM objects that can be retrieved, see the <a href="#">VIX Administrator's Guide</a> .  Metadata for these images is provided by ECIA and the actual images come from ECIA.	Clinical Display, JLV/ Image Viewer and VistARad
DoD artifacts (non-radiology)	Available if the Defense Medical Information Exchange (DMIX) Data Exchange Service (DES) servers are online accessible through DAS (Data Access Service) and if DAS servers are capable of communicating with the CVIX.	Clinical Display, JLV/ Image Viewer

## 2.1.2. Provide VA images to DoD requestors

The CVIX is also the portal used by all DoD clinicians to access VA images for shared VA/DoD patients. The flow of VA images through a CVIX is illustrated in Figure 2.

Figure 2: VA-to-DoD Image Sharing



DoD clinicians can access non-DICOM medical images and scanned documents from all VA sites via the CVIX.

**NOTE:** DoD clinicians cannot access images not stored in VistA Imaging at a VA site or images on a non-integrated 3rd party appliance (i.e., local).

If a VA site implements a local VIX, DoD clinicians also can access locally stored DICOM (radiology) images. For additional details about the types of images that can be accessed, see the [VIX Administrator's Guide](#).

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

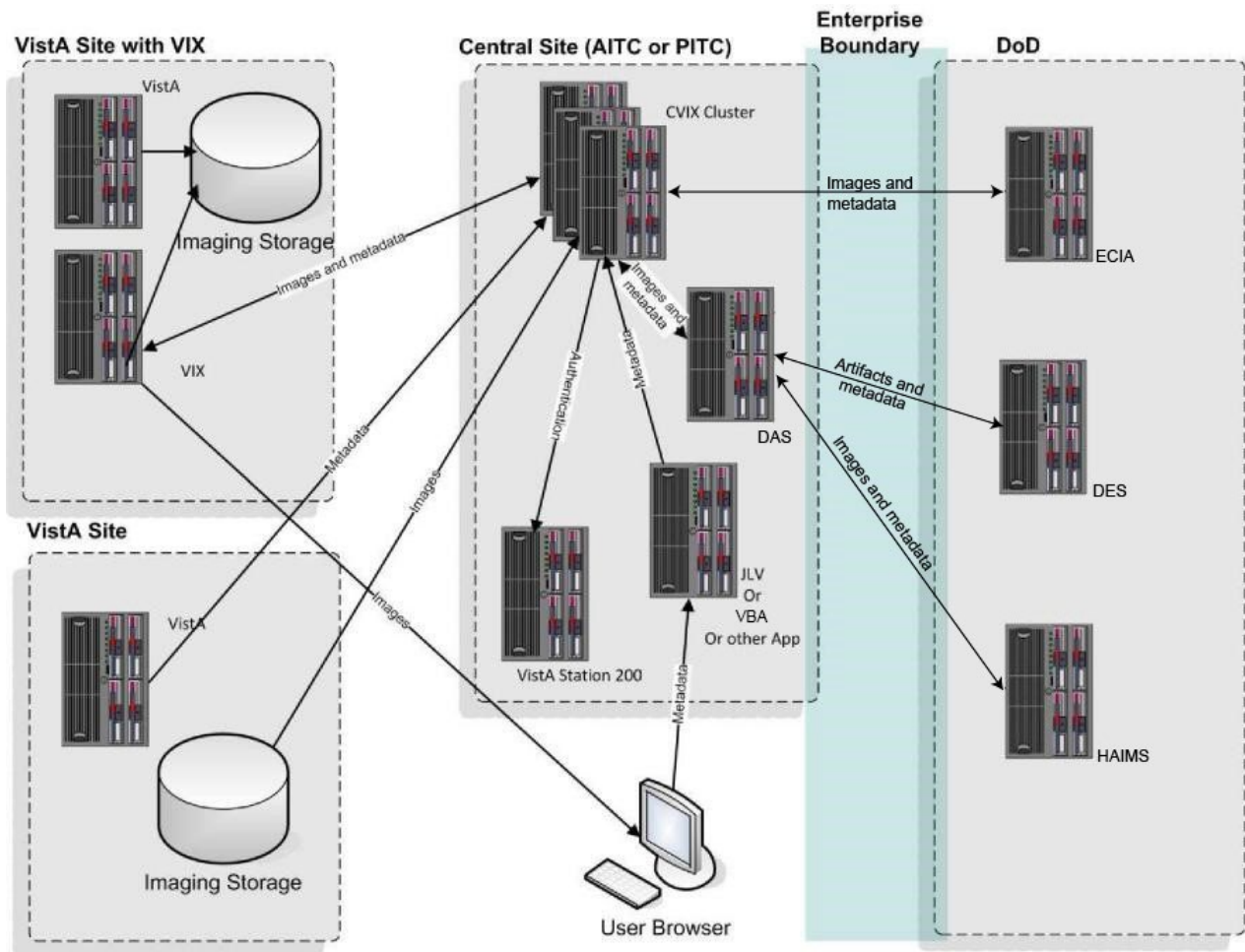
**NOTE:** At the VA sites where the image is stored, DoD clinician access requests are logged in the local VistA system. This logging is described in detail in the [VIX Administrator's Guide](#).



### 2.1.3. Provide VA and DoD images to Image Viewer

The CVIX hosts all the components needed to provide the image metadata access portal and an embedded Zero footprint image viewer. Data flow between the Image Viewer and a consuming application like JLV is depicted in Figure 3.

Figure 3: Data Flow for VIX Viewer Applications



JLV (clinical and VBA users), not associated with a specific VistA/ VIX, can access any image or report associated with a VA Progress Note or a VA Radiology package report, or DoD images via the CVIX. The CVIX handles all connections with VA sites, insulating the JLV from connection information changes.

**NOTE:** JLV users cannot access images and other images not stored in VistA Imaging at a VA site.

The Image Viewer itself is described in the [Enhanced Image Viewer User Guide](#).

**NOTE:** The Image Viewer is hosted in a separate application (JLV) that handles user authentication, patient selection, and progress note/report selection. For information about JLV, see <https://www.va.gov/vdl/application.asp?appid=224>

The Image Viewer also accommodates VBA access. Authentication information (username and password) for VBA is configurable in the Viewer\_config.xml file.

#### **2.1.4. Host the VistA Site Service**

The VistA Site Service is the repository of connection information used by various imaging components to connect to other VistA systems and VIXes. The CVIX itself also uses it. The VistA Site Service is described in *VistA Site Service*.

## **2.2. CVIX Physical and Logical Description**

The CVIX cluster is located in the VA Enterprise Cloud (VAEC) AWS environment. The CVIX cluster is made up of:

- Locally load-balanced VMs in AWS Availability Zone 1 (AZ1) and locally load-balanced VMs in AWS Availability Zone 2 (AZ2).
- The enterprise F5 load balancers provide local and global load balancing.
- Each VM is configured with 8 GB RAM per server, 3 Core CPU, each running Windows 2012 R2 x64, 2016, or 2019.

The configuration is virtualized. The hardware was sized to service the estimated user demand based on an estimated number of requests during peak usage.

**NOTE:** The existing CVIX hardware is actively monitored to ensure that adequate capacity is available. CVIX hardware has completed the migration to the VA VAEC AWS environment to increase capacity and elasticity.

## 2.3. CVIX Operational Priority

The CVIX is designed for continuous availability. Table 2 summarizes the anticipated operational priority of the CVIX broken out by function (if the CVIX server is offline, all functions are unavailable).

**Table 2: Anticipated Operational Priority of the CVIX Broken Out by Function**

CVIX Function	Priority	Notes
Host site service	High	If the site service is not available, Clinical Display or VistARad will not work for remote access because they cannot find their local VIX. (They will still work for local image access, and they can still do a remote login into a specific site if they know which site the images are at.)  Some 3 <sup>rd</sup> party apps such as TeleReader will not function properly until their access to the site service is restored.
Image Viewer	High	If the Viewer is not running, the CVIX is considered offline and removed from the F5 Load Balancer's list of nodes to use (The F5 monitors two services on each CVIX node for declaring online status: Apache Tomcat and the VIX Image Viewer). The Viewer depends on the VIX Render service, which depends on a local SQLite VixRender database.
VA/DoD	High	The CVIX provides access to remote data that may be relevant or highly valuable for patient care.

**NOTE:** Datacenter and Capacity redundancy is established – AZ1 and AZ2 are geographically distant. Both are active and ready at any time, with no intervention needed to handle the CVIX load. This configuration ensures Continuity of Operations (COOP) for the CVIX or disaster recovery. AZ1 and AZ2 are each other's failover sites, and the F5 Traffic Manager is configured to detect failures and automatically redirect traffic between sites and nodes as required.

## 2.4. CVIX Dependencies

Table 3 shows the systems that must be present for proper CVIX operation. One or more of these systems being absent will reduce CVIX capabilities, but not eliminate all of them.

**Table 3: CVIX System Requirements**

<b>System</b>	<b>Function</b>	<b>Interface method</b>	<b>CVIX behavior if “System” is not available</b>
Local VistA (Station 200)	Provides CVIX with a list of VA facilities that have treated a shared VA/DoD patient. Also provides security tokens that the CVIX uses to access VA sites to fulfill DoD requests.	LAN/RPC	DoD clinicians, JLV, Blue Button, and VBA users will not be able to access VA or DoD images for VA/DoD shared patients.
Site VIXes	Provide metadata and images to the CVIX.	WAN/HTTP	DoD clinicians, JLV, Blue Button, and VBA users will not be able to access site-specific radiology images via CVIX, but non-radiology images will still be available.
Remote VistA	Source of remotely stored VA images for DoD clinician access.	WAN/RPC	The CVIX cannot provide images from that site.
DAS	Gateway to DoD DICOM images for VA clinician access.	WAN/HTTP	The CVIX cannot provide DoD DICOM images to the VA.
ECIA	DoD metadata and image repository.	DICOM SCU	The CVIX cannot provide DoD DICOM images to the VA.
DES	Source of DoD artifacts and non-DICOM metadata for VA clinician access.	WAN/HTTP	The CVIX cannot provide DoD artifacts (scanned documents and non-radiology images) to the VA.

## 2.5. The CVIX, VIXes, and Multidivisional VA Sites

When a CVIX requests images and metadata from a VA multidivisional site, the path the data takes depends on how many VIXes are present at that site (Table 4).

**Table 4: Data Path Based on Number of Site VIXes**

<b># of VIXes</b>	<b>Data retrieval path</b>
2 or more	The CVIX gets metadata from the VIX at the primary division. If a subdivision has local image storage and a VIX, the CVIX requests the image from that VIX. If a subdivision has local image storage but does not have a VIX, the CVIX requests the image from the VIX at the primary division.
1	The CVIX gets all images and metadata from the VIX at the primary division.

0	<p>The CVIX gets metadata and image locations directly from the VistA System at the primary site and images directly from their storage locations.</p> <p><b>Note:</b> At non-VIX-sites, DICOM (radiology) images cannot be retrieved by the CVIX for DoD requestors.</p>
---	---

## 2.6. CVIX Connection Security

- The CVIX only responds to requests from authenticated applications. Application-level authentication is invisible to the clinical user who initiated the request.
- When communicating with VistA Remote Procedure Call (RPC) brokers, the CVIX supports Broker Security Enhancement (BSE), Identity and Access Management (IAM) STS (Secure Token Service) tokens, and pre-BSE-style remote logins. The CVIX will use BSE remote logins if BSE is enabled on the remote system and BSE authenticated is being utilized.
- CVIX-to-VIX communications require a valid security certificate.

## 3. CVIX General Operations

This section covers:

- CVIX Monitoring
- Using the CVIX Transaction Log
- Using the Cache Manager
- User Notifications
- Cluster-related Activities
- CVIX Planned Startup and Shutdown
- CVIX Data Retention and Purges
- CVIX and Backups
- CVIX and User Management

### 3.1. CVIX Monitoring

CVIX monitoring/ alert capabilities are fully automated via custom VistA Imaging monitoring utilities and SolarWinds enterprise monitor. In addition, the CVIX admins routinely perform the following manual monitoring and maintenance activities to verify automated tools.

- Once a day, access the transaction log on each CVIX node to verify that the CVIX is running.
- Once a week, check available cache space on each CVIX node.
- Review the CVIX processing load and available capacity by using the Windows Task Manager to determine the CPU cycles being consumed by the Apache Tomcat task.
- On rare occasions, corrupt metadata or image data may be cached and must be manually deleted. One possible indication is the inability to load an image/exam without an error being presented.

If an instance of the CVIX service encounters a fatal error or if a server node in the CVIX cluster reboots unexpectedly, the CVIX service will self-recover.

### 3.2. Using the CVIX Transaction Log

The CVIX transaction log records information about every image and metadata transfer handled by the CVIX. Entries in the log are retained for 90 days and then purged. A permanent backup copy of the CVIX transaction log is also stored in the failover cluster described in *VIX Log Collector Service*.

An instance of the CVIX transaction log resides on each active server in the CVIX cluster. The log itself is accessed via a web browser.

To access the CVIX transaction log, go to **https://FQDN:REDACTED/Vix/secure/VixLog.jsp** (where **FQDN** is the fully qualified domain name of the cluster on which the CVIX is installed).

The main transaction log Web page can be used to display, filter, and export log entries of interest. By default, the page displays the 100 most recent transactions for the current day with the newest entries at the top. For detailed information about each field in the log, see *CVIX Transaction Log Fields*.

**NOTE:** The CVIX is set up as a load-balanced cluster without server affinity. Check multiple CVIX nodes to see all log entries related to a given transaction (that is, receipt and fulfillment of a specific data request).

To view the CVIX transaction log, complete the following steps:

1. Navigate to **https://FQDN:REDACTED/Vix/secure/VixLog.jsp**.
2. Enter the vixlog username and password in the 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 CVIX 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.
  - For detailed information about each field in the log, see CVIX Transaction Log Fields.
4. 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 last page of (oldest) 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 **From Date/Time** and **To Date/Time** boxes, and then click **Show in Browser**.
2. Dates are formatted as YYYY-MM-DD HH-MM.
3. The most recent log entries are shown first.
4. 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 export entries.
2. One thousand exported log entries will result in an approximately 0.5-megabyte file.
3. The Transactions per Page setting does not apply when log entries are supported.
4. Click **Save as CSV** for comma-separated values or **Save as TSV** for tab-separated values.
5. Use the browser Save dialog box to specify where the file will be stored.
6. Use a spreadsheet program or a text editor to open the resulting file.

### 3.2.1. CVIX Transaction Log Fields

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

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

**Table 5: Descriptions of CVIX Transaction Log Fields**

Name	Description
Date and Time	When the transaction was processed. Formatted as MM-DD-YYYY, HH:MM: SS, AM/PM.
Time on VIX	The length of the transaction in milliseconds begins when the CVIX receives a message and ends when the CVIX begins to respond.
ICN	The Integration Control Number (ICN) uniquely identifies 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.)
Query Type	A multi-part field that indicates [handler method receiving site <- sending site].  <i>handler</i> identifies the VIX Web application that handled the request, for details, see the <i>CVIX Interfaces</i> .  <i>method</i> identifies the specific operation performed.  <i>receiving site &lt;- sending site</i> 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 a date was transferred.
Asynchronous	Indicates whether the transaction was performed asynchronously (true) or synchronously (false).



Name	Description
Items Returned	<p>The number of items returned to the requester.</p> <p>For study metadata, it 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.</p> <p>For other operations, this column is not populated.</p>
Items Received	<p>The number of items retrieved from the remote site.</p> <p>For study metadata, it 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.</p> <p>If the CVIX 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."</p>
Bytes Returned	<p>If populated, the amount of data returned in the request. In the exported log, this field is labeled "Façade Bytes Returned."</p>
Bytes Received	<p>If populated, the amount of data received in the request.</p> <p>In the exported log, this field is labeled "Data Source Bytes Received."</p>
Throughput	<p>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.</p>
Quality	<p>Populated for images only. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• THUMBNAIL</li> <li>• REFERENCE</li> <li>• DIAGNOSTIC</li> <li>• DIAGNOSTIC UNCOMPRESSED</li> </ul> <p>For more information about these parameters, see <i>Remote Image Retrieval</i>.</p>
Command Class Name	<p>Internal CVIX command used for debugging and support.</p>
Originating IP Address	<p>The IP address of the workstation that initiated the image or metadata request. (The same IP address will be reported for all requests originating from the DAS.)</p>
User	<p>The name of the End User that initiated the request.</p>

Name	Description
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.
Datasource Protocol	The source of the data being handled:  vistaimaging – Data from a VistA system  MIX – Radiology data from a source outside of VistA (from the DoD) or from Vista (to the DoD), both through DAS  Vftp – Data from another VIX  DX – Non-radiology data from a source outside of VistA (from the DoD) through DAS/DES  AX – VistA Imaging Documents served by the CVIX (to DoD) through DAS/DES
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 CVIX. Typical values include:  200 – OK (success)  401 – Unauthorized  404 – Not found  409 – Image exists but is not yet available on DoD side and/or Imaging jukebox  412 – BSE token expired  415 – Image conversion exception  500 – Internal server error
Realm Site Number	The STATION NUMBER (field (#99) of the INSTITUTION file (#4) of the site that the requester's credentials are authenticated against.
URN	Only populated for image transactions. Universal Resource Name (URN); the unique name of the image being requested.

Name	Description
Transaction Number	The Globally Unique Identifier (GUID) for an image or metadata transaction. For transactions that originate from Clinical Display or the DAS, the same identifier will be reflected in the Image Access log at the site where the images are stored. If a transaction crosses the CVIXDAS boundary, the originator's transaction ID is used on the other side as well (interagency transactions tracking support)
VIX Software Version	The software version of the CVIX.
VistA Login Method	The login 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, Claims, or LOCAL.
Client Version	If the source of the image or metadata request is VistA Imaging Clinical Display, the version number of the Clinical Display software will be recorded here and not populated for other requestors.
Data Source Method	Identifies the specific operation performed by the data source.
Data Source Version	The version number of the data source.
Data Source Response Server	The name of the server that responded to the metadata or image request; useful for determining which node in a clustered VIX handled the request. Only populated for requests directed to a 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 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).

### 3.2.2. CVIX Transaction Log Fields (Export Only)

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

**Table 6: Descriptions of CVIX Transaction Log Fields for Export Only**

Name	Description
Façade Bytes Retrieved	The number of bytes returned to the requestor, where the requestor could be JLV, Clinical Display, VistARad, another VIX, or the CVIX.

Name	Description
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 or DES, or ECIA.
Machine Name	Name of the CVIX 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 CVIX 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 is used for debugging and support.
Thread ID	The name of the thread that processed the transaction.

### 3.2.3. Logging on Remote VistA Systems

If the CVIX retrieves images and metadata from a VA site that does not have a VIX, the CVIX will log the image access information in that site's local IMAGE ACCESS LOG file (#2006.95) the same way a VIX would.

For details about how this information is logged, see the [VIX Administrator's Guide](#).

## 3.3. Using the Cache Manager

A Cache Manager function allows users to browse a CVIX node's local cache and delete data as required. The Cache Manager is accessed using Chrome or Edge.

To access the CVIX Cache Manager, go to **https://FQDN:REDACTED/VixCache** (where **FQDN** is the fully qualified domain name of the individual host within the cluster the VIX is installed on).

**NOTE:** The URL to the CVIX Cache Manager is case-sensitive.

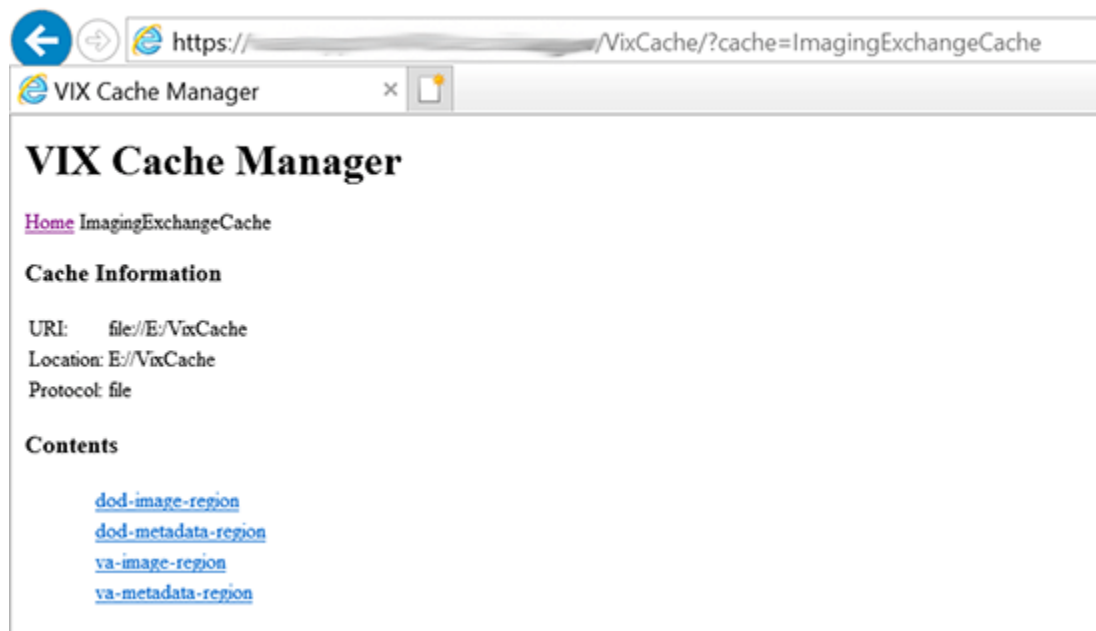
### 3.3.1. Cache Organization

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 data are the most important factor in determining where an item is cached. When the CVIX Cache Manager is started, the following screen displays (Figure 4):

**Figure 4: VIX Cache Manager Initial Screen Display**



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 item (image versus anything else). A region defines the conditions under which a cache item is deleted from the cache.

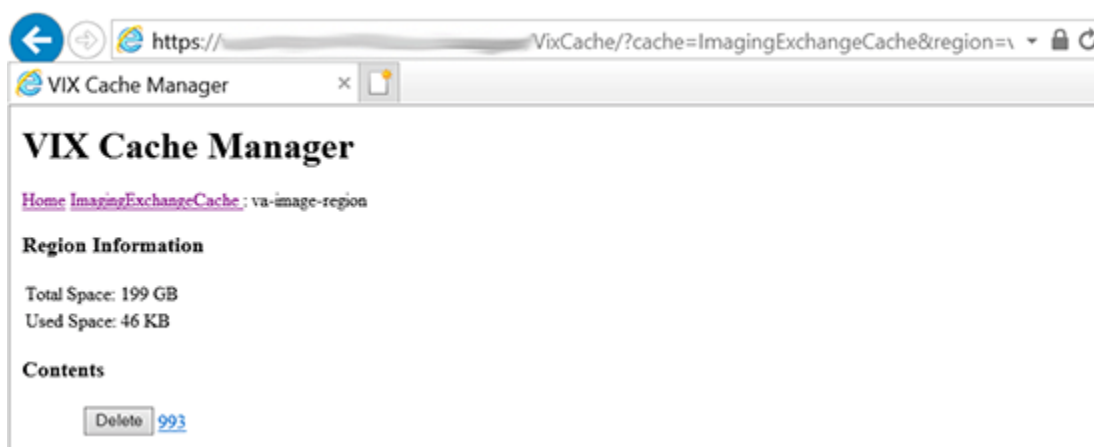
Historically, it has been the case that anything that is not from the VA is from the Department of Defense and anything that is not an image is metadata. Thus, a radiology image from the DoD will be found in the “dod-image-region” while the study text data from a VA site will be found in the “va-metadata-region”.

### 3.3.2. 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 with 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, *ad infinitum* or at least *ad out-of-memoriam*. 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. This is similar to images in a study. 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 (Figure 5)

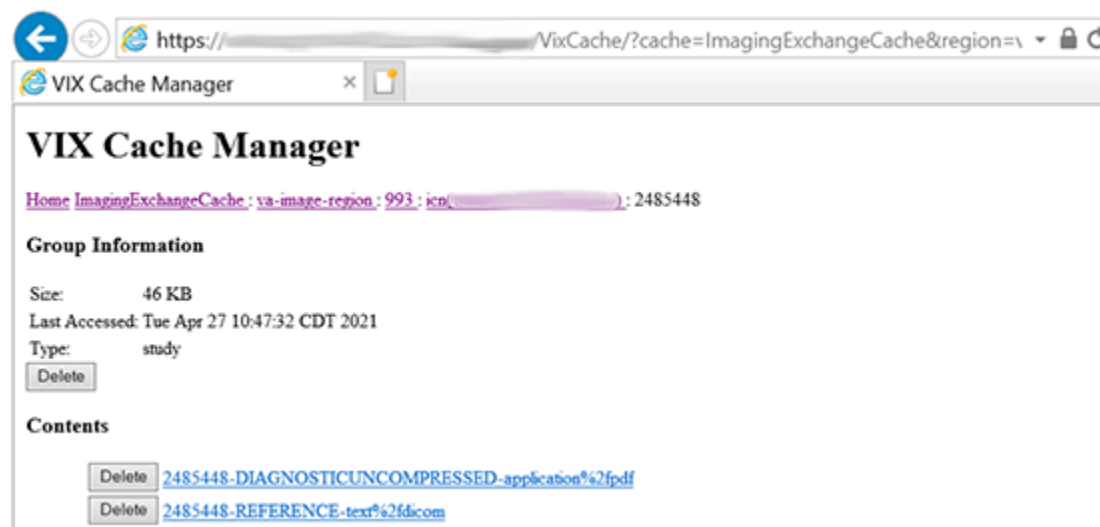
Figure 5: VIX Cache Manager Region Information Display Example



The CVIX Cache Manager displays the region's name 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.

Drill down through the CVIX cache using the links in the CVIX 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 of the item (Figure 6).

**Figure 6: VIX Cache Manager DOD Region Display with Delete Function**



### 3.3.3. 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 eHealth Exchange. For our purposes, the OIDs are shown in Table 7.

**Table 7: DoD Image Order Identification Numbers (OIDs)**

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 DES server. Likewise, DoD radiology comes from either HAIMS or ECIA, identified as “200”.

Below the repository identifier is a patient identifier (the patient ICN), and then instances related to that patient.

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

### 3.3.4. 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; the size of a cache group is the sum of all the groups and instances contained within it. The checksum, available only for cache instances, results from a mathematical calculation applied to the entire content of the instance. The checksum is used within the VIX to detect data errors. For instance, with the same identifiers, this value should always be the same on all VIX and CVIX.

### 3.3.5. 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.

Separate and distinct instances of the CVIX cache component reside on each server in the CVIX cluster. A cache item may be cached on one or more servers within the cluster, although the Cache Cluster option eliminates multiple copies of the same item. Without using this option, it is even possible for a cache item to be correct in one server and corrupt in another, leading to difficulty in diagnosing errors. In general, if repeated attempts to access a specific datum through the CVIX fail or present corrupt data, then the item should be in all the cache instances and deleted.

To delete a cache item, collect as much identifying information as possible. At a minimum, this must include whether the source is VA or 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 ICN must be known.

Once that information is collected, open the 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 and then confirm that the item is to be deleted. The cache does not immediately delete the item since it must synchronize operations from all clients. It may take a few seconds or up to a minute before the item is deleted. Usually, however, it will respond immediately that the item is deleted, and the item will disappear from the 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 CVIX 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, along with difficulty in tracking down an item in one or more cache instances in a cluster, may lead someone to delete “good” cache



items to get all the “bad” ones. This is not an issue since the CVIX will simply re-cache the items when requested again.

### 3.4. User Notifications

A CVIX outage (planned or unplanned) should be announced using the Automated Notification Report (ANR) system. Log an ANR directly at **REDACTED** or by contacting the National Help Desk.

For ongoing connectivity issues with DAS, contact the **VA IT DAS Technical** mail group at **REDACTED**.

### 3.5. Cluster-related Activities

The following sections cover:

- CVIX cluster: take the node offline.
- CVIX cluster: bring the node online.

#### 3.5.1. CVIX cluster: take the node offline

This action will require a Service Request (SR) or Service Now ticket to the network team to take a fully functional node out of the cluster. To temporarily take a node out of the cluster, stop Apache Tomcat, which will cause the F5 port monitors to declare the node inaccessible.

#### 3.5.2. CVIX cluster: bring the node online

This action will require a SR to the network team to add a fully functional node to the cluster. To place a temporarily disabled node back in the cluster, start Apache Tomcat, which will cause the F5 port monitors to declare the node accessible.

### 3.6. CVIX Planned Startup and Shutdown

The CVIX is designed to be running at all times. For procedures about taking individual servers offline for maintenance, please see the Cluster-related Activities section above. Operations procedures dictate rolling updates to avoid a full shutdown. If necessary, fully shut down and restart all CVIX hardware, using the steps below.

#### 3.6.1. Planned Full CVIX Shutdown

1. Review *CVIX Dependencies* to ensure that all the implications of a full CVIX shutdown can be planned for.
2. File an ANR at **REDACTED** or by contacting the National Help Desk to file an ANR.
3. Bring down each CVIX VM as the plan requires.

### 3.6.2. Planned Full CVIX Startup

1. Bring up each VM as started.
2. Verify that Apache TomCat, Vix Viewer and Vix Render services have started.
3. If there is an open ANR for the CVIX, update the ANR to indicate that the service interruption is over.

## 3.7. CVIX Data Retention and Purges

The CVIX runs a daily purge process for locally stored data, as described in Table 8.

**Table 8: CVIX Purge Schedule**

Operation	When Performed
Purge Java logs	1 A.M. daily for Java log entries more than 5 days old.
Purge transaction log entries	2 A.M. daily for transaction log entries more than 5 days old.
Purge CVIX cache	3 A.M. daily for images more than 30 days old for DoD images, but more than seven days old for VA images.  Once per minute for old VA metadata, once per hour for old DoD metadata
Purge CVIX Render Cache and DB	12 A.M. (midnight) daily for data older than two days or larger than 1024 MB.

## 3.8. CVIX and Backups

Table 8 represents the data retention values set at the time of release. The location to alter these settings are:

- Tomcat Java logs – adjust days in C:\VixConfig\JavaLogConfiguration.Config, under <retentionPeriodDays> and restart Apache Tomcat.
- VIX Transaction logs – adjust days in C:\VixConfig\TransactionLoggerLocalDataSource-1.0.Config, under <retentionPeriodDays> and restart Apache Tomcat.
- VixCache – C:\VixConfig\cache-config\ImagingExchangeCache-cache.xml under va-image-region, dod-image-region, and scip-region respectively adjust the ...-lifespan value (make sure the value is defined above in the same file) and restart Apache Tomcat.
- VixRenderCache and VIX SQLite DB – C:\Program Files\Vista\Imaging\VIX.Config\Vix.Render.config under the <Purge> entry the MaxAgeDays= and MaxCacheSizeMB= values; when done and restart Viewer and Render services.

The CVIX does not need to be explicitly backed up:

- The VIX log collector service automatically backs up CVIX transaction logs.

- CVIX cache is transitory and does not need to be backed up.
- CVIX-specific configuration settings are minimal and can be reestablished by rerunning the CVIX installer. Contact the VIX Development Group by email for details.  
(REDACTED)

### 3.9. Critical Metrics

Critical metrics of the CVIX are shown in Table 9.

**Table 9: Critical Metrics**

System Accessibility	24/7
System Uptime	Based on VistA uptime
Online Operational Performance	Aggregate image throughput >5 Mb/s
Production Incidents	Fewer than 1/month

### 3.10. CVIX and User Management

CVIX administrators access and maintain the CVIX using NEMA zero token-enabled accounts.

VA clinicians requesting data via the CVIX use local VistA site credentials or authorized VA application credentials (i.e. MHV, JLV, etc). These are independent of the CVIX.

DoD clinicians requesting data via the CVIX authenticate through DoD EHR authentication (i.e. AHLTA, HAIMS, etc). System-to-system access occurs via a service account (named CVIX, USER) defined for DoD on the Station 200 VistA System.

### 3.11. Configurations for DoD images Provided to VA Clinicians

DoD images that can be retrieved from the VA can originate from HAIMS or ECIA. A configuration change to the MIXDataSource-1.0.config file in C:\VixConfig can be made to switch the source of the DoD Images provided to VA clinicians. This configuration is performed as part of the CVIX Installation, see the [CVIX Installation Guide](#). This section is provided in the event a change needs to be made to this configuration.

The ability to enable the CVIX to collect DoD images from the ECIA requires the following information:

- The connection to AcuoMed, AcuoAccess, and ID lookup software/application.
- The Digital Imaging and Communications in Medicine (DICOM) modality types not to be returned from the DoD.
- Receive the blacklists for three different imaging display applications (VistA Imaging Clinical Display, JLV, VistARad).

Open the MIXDataSource-1.0.config file in C:\VixConfig. Run Notepad, Notepad++, or WordPad as an administrator, and then open the file. Set the value of useEcia to true or false.

- **Set useEcia to true**, if DoD images provided to VA clinicians are to use ECIA.
- **Set useEcia to false**, if DoD images provided to VA clinicians are to use HAIMS.

Update the MIXDataSource-1.0.config file to set useEcia to either true or false (see Figure 7), (if not already set to the correct value) (inside <useEcia> </useEcia>).

**Figure 7: Sample MIXDataSource-1.0.config file - Bottom Portion**

```
<useEcia>true</useEcia>
```

If DoD images provided to VA clinicians are to use HAIMS:

- **No, additional configuration is needed.** Do not perform the steps in *Additional Configurations for ECIA only for DoD images Provided to VA Clinicians*.

If DoD images provided to VA clinicians are to use ECIA:

- **Additional configuration is needed.** Perform all the steps in *Additional Configurations for ECIA only for DoD images Provided to VA Clinicians*.

### **3.11.1. Additional Configurations for ECIA only for DoD images Provided to VA Clinicians**

This describes additional configuration steps **only to be performed** when CVIX collection of DoD medical images from **ECIA is enabled** (i.e. <useEcia>true</useEcia>).

Perform this step to further configure the CVIX collection of DoD medical images to ECIA via the MIXDataSource-1.0.config file.

**NOTE:** Before moving forward with the instructions for this step, it is expected that the site administrator is aware of all needed entries in the configuration including <host>, <callingAE>, and <calledAE> for AcuoMed and <host>, <port>, and <protocol> for AcuoAccess.

**NOTE:** The configuration including <host>, <callingAE>, and <calledAE> for AcuoMed and <host> for AcuoAccess are set based on the server type (i.e. test or production) during the end of the install via the PowerShell script utility. If these values are not the same as the values you have for these in the installation prerequisites, change them according to the values for these in the prerequisites; otherwise, leave them as they are.

Open the MIXDataSource-1.0.config in C:\VixConfig. Run Notepad, Notepad++, or WordPad as an administrator, and then open the file.

To enable the ECIA configuration, further update the MIXDataSource-1.0.config like Figure 8 and Figure 9:

1. Set the entry for the host for AcuoMed, (inside <host> </host>).

2. Set the entry for the port for AcuoMed (inside <port> </port>).
3. Set the entry for the client identification for AcuoMed (inside <callingAE> </callingAE>).
4. Set the entry for the server identification for AcuoMed (inside <calledAE> </calledAE>).
5. Set the entry for the host for AcuoAccess (inside <host> </host>).
6. Set the port for AcuoAccess (inside <port> </port>).
7. Set the protocol for AcuoAccess (inside <protocol> </ protocol>).
8. Verify the <string>SR</string> line is NOT present inside the <emptyStudyModalities> </emptyStudyModalities>. (If present, remove this line).
9. Set the DICOM modality types that will not be returned from the DoD (inside <string> </string> tags).

**NOTE:** The <string> </string> tags inside the vistaRadModalityBlacklist are set during the end of the install via the PowerShell script utility. If these values are not the same as the values you have for these in the installation prerequisites, change them according to the values for these in the prerequisites; otherwise, leave them as they are.

**NOTE:** Inside the <string> </string> tags, insert the DICOM Identifier for the modality. For example, if an “SR” is inserted inside the <string> </string> tag, then a Structured Report will not be returned from the DoD.

**NOTE:** If more or less DICOM modality types (referred to as a modality blacklist) are not to be returned from the DoD, add or remove additional <string> </string> lines (within the opening and closing tags for vistaRadModalityBlacklist). Inside the <string> </string> tags, insert the DICOM Identifier for the modality.

10. Set the DICOM Service-Object Pair (SOP) Class UUIDs (referred to as SOP blacklists) that represent image types and that will be replaced with a static image file for three different image viewer applications (Vista Imaging Clinical Display, JLV, VistaRad). For the blacklist changes, add or remove the DICOM SOP Class UUIDs according to the prerequisites. (inside <string> </string> tags for Vista Imaging Clinical Display; inside <string> </string> tags for JLV; inside <string> </string> tags for VistaRad).

**NOTE:** The <string> </string> tags inside the SOP blacklists (i.e. sopBlacklistForClinicalDisplay, sopBlacklistForVixViewer, or sopBlacklistForVistaRad) are set during the end of the install via the PowerShell script utility. If these values are not the same as the values you have for these in the installation prerequisites, change them according to the values for these in the prerequisites; otherwise, leave them as they are.

**NOTE:** For example, if a “1.2.840.10008.5.1.4.1.1.88.11” is inserted inside the <string> </string> tag, then the Basic Text SR that the SOP Class UID represents will be replaced with a static image file for Vista Imaging Clinical Display.

**NOTE:** For example, if a “1.2.840.10008.5.1.4.1.1.88.11” is inserted inside the <string> </string> tag, then the Basic Text SR that the SOP Class UID represents will be replaced with a static image file for JLV.

**NOTE:** For example, if a “1.2.840.10008.5.1.4.1.1.88.11” is inserted inside the <string> </string> tag, then the Basic Text SR that the SOP Class UID represents will be replaced with a static image file for VistaRad.

**NOTE:** Inside the <string> </string> tags, insert the DICOM SOP Class UIDs according to the prerequisites.

**NOTE:** If more or less DICOM SOP Class UIDs are needed, add or remove additional <string> </string> lines within the opening and closing tags for the appropriate viewer (i.e. sopBlacklistForClinicalDisplay, sopBlacklistForVixViewer, or sopBlacklistForVistaRad). Inside the <string> </string> tags, insert the DICOM SOP Class UIDs to blacklist.

Save the MIXDataSource-1.0.config file after updating the entries.

**Figure 8: Sample MIXDataSource-1.0.config file - Top Portion**

```
<gov.va.med.imaging.url.mix.configuration.EciaDicomSiteConfiguration>
  <username></username>
  <siteNumber>200D</siteNumber>
  <mixApplication></mixApplication>
  <metadataPath1></metadataPath1>
  <metadataPath2></metadataPath2>
  <imagePath1></imagePath1>
  <imagePath2></imagePath2>
  <useVersioning>>false</useVersioning>
  <host>*SET HOST ACUOMED*/host>
  <port>*SET PORT ACUOMED*</port>
  <protocol></protocol>
  <callingAE>*SET CLIENT ID ACUOMED*</callingAE>
  <calledAE>*SET SERVER ID ACUOMED*</calledAE>
  <connectTimeOut>60000</connectTimeOut>
  <cfindRspTimeOut>300000</cfindRspTimeOut>
</gov.va.med.imaging.url.mix.configuration.EciaDicomSiteConfiguration>
<gov.va.med.imaging.url.mix.configuration.MIXSiteConfiguration>
  <username></username>
  <siteNumber>200W</siteNumber>
  <mixApplication>AcuoRest</mixApplication>
  <metadataPath1></metadataPath1>
  <metadataPath2></metadataPath2>
  <imagePath1></imagePath1>
  <imagePath2></imagePath2>
  <useVersioning>>false</useVersioning>
  <host>*SET HOST ACUOACCESS*/host>
  <port>*SET PORT ACUOACCESS*</port>
  <protocol>*SET PROTOCOL ACUOACCESS*</protocol>
</gov.va.med.imaging.url.mix.configuration.MIXSiteConfiguration>
</configurations>
<emptyStudyModalities>
  <string>AU</string>
  <string>DOC</string>
  <string>EPS</string>
  <string>FID</string>
  <string>HD</string>
  <string>KO</string>
  <string>PR</string>
  <string>RESP</string>
  <string>RTSTRUCT</string>
  <string>RTRECORD</string>
  <string>RTDOSE</string>
  <string>RTPLAN</string>
  <string>MS</string>
</emptyStudyModalities>
```

**Figure 9: Sample MIXDataSource-1.0.config file - Middle Portion**

```

<vistaRadModalityBlacklist>
  <string>DOC</string>
  <string>IO</string>
  <string>OAM</string>
  <string>OCT</string>
  <string>OP</string>
  <string>OPM</string>
  <string>OPT</string>
  <string>OPV</string>
  <string>OSS</string>
  <string>PX</string>
</vistaRadModalityBlacklist>
<sopBlacklistForClinicalDisplay>
  <string>1.2.840.10008.5.1.4.1.1.88.11</string>
  <string>1.2.840.10008.5.1.4.1.1.88.22</string>
  <string>1.2.840.10008.5.1.4.1.1.88.33</string>
  <string>1.2.840.10008.5.1.4.1.1.88.40</string>
  <string>1.2.840.10008.5.1.4.1.1.88.50</string>
  <string>1.2.840.10008.5.1.4.1.1.88.59</string>
  <string>1.2.840.10008.5.1.4.1.1.88.65</string>
  <string>1.2.840.10008.5.1.4.1.1.88.67</string>
  <string>1.2.840.10008.5.1.4.1.1.11.1</string>
</sopBlacklistForClinicalDisplay>
<sopBlacklistForVixViewer>
  <string>1.2.840.10008.5.1.4.1.1.128.1</string>
  <string>1.2.840.10008.5.1.4.1.1.104.2</string>
  <string>1.2.840.10008.5.1.4.1.1.82.1</string>
  <string>1.2.840.10008.5.1.4.1.1.81.1</string>
  <string>1.2.840.10008.5.1.4.1.1.66.4</string>
  <string>1.2.840.10008.5.1.4.1.1.11.5</string>
  <string>1.2.840.10008.5.1.4.1.1.11.4</string>
  <string>1.2.840.10008.5.1.4.1.1.11.3</string>
  <string>1.2.840.10008.5.1.4.1.1.11.2</string>
  <string>1.2.840.10008.5.1.4.1.1.11.1</string>
  <string>1.2.840.10008.5.1.4.1.1.9.6.1</string>
  <string>1.2.840.10008.5.1.4.1.1.9.5.1</string>
  <string>1.2.840.10008.5.1.4.1.1.9.4.2</string>
  <string>1.2.840.10008.5.1.4.1.1.9.4.1</string>
  <string>1.2.840.10008.5.1.4.1.1.9.3.1</string>
  <string>1.2.840.10008.5.1.4.1.1.9.1.3</string>
  <string>1.2.840.10008.5.1.4.1.1.7.4</string>
  <string>1.2.840.10008.5.1.4.1.1.7.3</string>
  <string>1.2.840.10008.5.1.4.1.1.7.2</string>
  <string>1.2.840.10008.5.1.4.1.1.7.1</string>
  <string>1.2.840.10008.5.1.4.1.1.4.4</string>
  <string>1.2.840.10008.5.1.4.1.1.2.2</string>
</sopBlacklistForVixViewer>
<sopBlacklistForVistaRad>
  <string>1.2.840.10008.5.1.4.1.1.88.11</string>
  <string>1.2.840.10008.5.1.4.1.1.88.22</string>
  <string>1.2.840.10008.5.1.4.1.1.88.33</string>
  <string>1.2.840.10008.5.1.4.1.1.88.40</string>
  <string>1.2.840.10008.5.1.4.1.1.88.50</string>
  <string>1.2.840.10008.5.1.4.1.1.88.59</string>
  <string>1.2.840.10008.5.1.4.1.1.88.65</string>
  <string>1.2.840.10008.5.1.4.1.1.88.67</string>
  <string>1.2.840.10008.5.1.4.1.1.11.1</string>
  <string>1.2.840.10008.5.1.4.1.1.104.1</string>
</sopBlacklistForVistaRad>

```



## 3.12. Configure DICOM SCP Functionality

This section provides details on the DICOM Service Class Provider (SCP) configuration. The DICOM SCP is a service provider on the VIX/CVIX that transfers DICOM files between the VA and DoD. The DICOM SCP is used to allow VA clinicians to use Commercial PACS, or other query retrieve devices, and DoD clinicians to use NilRead™ or other query retrieve devices, to get remote VistA images through the use of DICOM C-FIND and C-MOVE.

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

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

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

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

**NOTE:** To update access and verify codes for the account with VistA credentials, plain text versions can be entered directly into the configuration file and are encrypted after restarting the Apache Tomcat service. The access and verify codes can also be updated in the configuration file with a reconfigure installation described see the [CVIX Installation Guide](#) or use the ImagingUtilities-0.1.jar in C:\VixConfig\Encryption to assist with generating encrypted forms of plain text access and verify codes.

**NOTE:** If updates are needed to the local drive for the VIX cache, see the [CVIX Installation Guide](#) and perform a reconfigure installation.

### 3.12.1. AE Titles Configuration

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

**NOTE:** The port for the DICOM SCP client where the DICOM SCP is used must be configured as a bi-directional open port in any firewall.

### 3.12.2. Laurel Bridge AE Titles Configuration on CVIX

The mapping of external Application Entities (AE) Titles to TCP/IP addresses and ports is configurable and set at the time of installation by installation/administration personnel on the CVIX server. This mapping is necessary for resolving the IP address and port of C-MOVE Destination AE and must be correctly configured for the Laurel Bridge SCP AE to correctly function as a C-MOVE SCP.

**NOTE:** The configuration is set for use with NilRead™ based on the server type (i.e. test or production) during the end of the install via the PowerShell script utility. If these values are not the same as the values you have for these in the installation prerequisites, change them according to the values for these in the prerequisites; otherwise, leave them as they are.

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

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

For each DICOM SCP client, the AE Title name and its host/port attributes must be set. For each DICOM SCP client, update the following entries for the AE Titles configuration file (refer to Figure 10 for line numbers):

1. Set the IP address for the host for the DICOM SCP client (after `host =` - line 7).
2. Set the port for the DICOM SCP ad client where the DICOM SCP is used for the C-STORE operation (after `port =` - line 8).
3. Set the AE title the DICOM SCP client is using to communicate with the DICOM SCP (calling AE) (inside `[ ]` - line 6 and after `ae_title =` - line 9).

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

**Figure 10: Sample AE Titles Configuration File**

---

```
1 #
2 # map between an Application Entity Title and a full address
3 # i.e. host:port:called-ae-title
4 #
5
6 [ **Insert SCU AE Title** ]
7 host = **Insert SCU IP Address**
8 port = **Insert SCU Port**
9 ae_title = **Insert SCU AE Title**
```

A more specific example using NilRead™ with some AE Titles filled in is shown in Figure 11. This example is for illustrative purposes only.

**Figure 11: Sample AE Titles Configuration File Filled**

```
1 #
2 # map between an Application Entity Title and a full address
3 # i.e. host:port:called-ae-title
4 #
5
6 # [ **Insert AE Title the NilRead client is using to communicate with the DICOM SCP** ]
7 # host = **Insert IP Address for the host for the NilRead client**
8 # port = **Insert port for the NilRead client where the DICOM SCP is used for the C-STORE operation**
9 # ae_title = **Insert AE Title the NilRead client is using to communicate with the DICOM SCP**
10
11 [ ***** ]
12 host = *****
13 port = *****
14 ae_title = *****
15
16 [ ***** ]
17 host = *****
18 port = *****
19 ae_title = *****
20
21 [ ***** ]
22 host = *****
23 port = *****
24 ae_title = *****
25
26 [ ***** ]
27 host = *****
28 port = *****
29 ae_title = *****
```

After updating the ae\_title\_mappings file, as described above, it is necessary to restart the Apache Tomcat service. One way this can be performed is by executing the restart script (Restart\_VIX\_Services.ps1) as described in the [CVIX Installation Guide](#).

### 3.12.3. AE Titles Configuration on DICOM SCU

This section describes the AE Titles configuration on the AE Titles on the DICOM Service Class User (SCU). Installation/administration personnel on the CVIX server may not be able to perform this configuration and instead must provide the necessary information to the DICOM SCU administration personnel to perform.

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

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

### 3.12.4. Tomcat DICOM SCP Configuration

This section provides details on the ScpConfiguration.Config file located in C:\VixConfig. To update access and verify codes for the account with VistA credentials, plain text versions can be

entered directly into the configuration file and are encrypted after restarting the Apache Tomcat service. The access and verify codes can also be updated in the configuration file with a reconfigure installation described see the [CVIX Installation Guide](#) or use the ImagingUtilities-0.1.jar in C:\VixConfig\Encryption to assist with generating encrypted forms of plain text access and verify codes.

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

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

Update the following entries for the DICOM SCP functionality (refer to Figure 12 for line numbers):

1. Set the DICOM SCU calling AE title, inside opening and closing aeTitle tags (inside <aeTitle> </aeTitle> - line 21). Change the value from the default setting of ALL.
2. Set the DICOM SCU IP address inside the opening and closing callingAeIp tags (inside <callingAeIp> </callingAeIp> - line 22). Change the value from the default setting of 0.0.0.0.

**Figure 12: Sample DICOM SCP Configuration File**

```

1 <gov.va.med.imaging.facade.configuration.ScpConfiguration>
2   <dirty>false</dirty>
3   <accessCode>XXXXXXXXXXXXXXXXXXXX</accessCode>
4   <verifyCode>XXXXXXXXXXXXXXXXXXXX</verifyCode>
5   <siteFetchTPoolMax>20</siteFetchTPoolMax>
6   <siteFetchTimeLimit>45</siteFetchTimeLimit>
7   <imageFetchTPoolMax>15</imageFetchTPoolMax>
8   <imageFetchTimeLimit>1000000</imageFetchTimeLimit>
9   <useRemoteImageFetch>true</useRemoteImageFetch>
10  <useDirectFetch>true</useDirectFetch>
11  <cacheLifespan>1</cacheLifespan>
12  <preFetchSeries>true</preFetchSeries>
13  <calledAETitle>ANY_0.0.0.0</calledAETitle>
14  <remotePatientResolution>true</remotePatientResolution>
15  <imageQueueSize>10000</imageQueueSize>
16  <cacheMetaHoursToLive>24</cacheMetaHoursToLive>
17  <isFdtEnabled>true</isFdtEnabled>
18  <fdtPort>2762</fdtPort>
19  <callingAEConfigs>
20    <gov.va.med.imaging.facade.configuration.ScpCallingAE>
21      <aeTitle>ALL</aeTitle>
22      <callingAeIp>0.0.0.0</callingAeIp>
23      <buildReport>SC</buildReport>
24      <returnQueryLevel>false</returnQueryLevel>
25      <studyQueryFilter>radiology</studyQueryFilter>
26      <sendKeepAlive>false</sendKeepAlive>
27      <modalityBlockList>
28        <gov.va.med.imaging.facade.configuration.ScpModalityList>
29          <dataSource>ALL</dataSource>
30          <addImageLevelFilter>false</addImageLevelFilter>
31          <modalities>
32            <string>none</string>
33          </modalities>
34        </gov.va.med.imaging.facade.configuration.ScpModalityList>
35      </modalityBlockList>
36      <siteCodeBlackList>
37        <string>100</string>
38        <string>200CLMS</string>
39        <string>200CORP</string>
40        <string>741</string>
41        <string>LOCAL</string>
42      </siteCodeBlackList>
43    </gov.va.med.imaging.facade.configuration.ScpCallingAE>
44  </callingAEConfigs>
45 </gov.va.med.imaging.facade.configuration.ScpConfiguration>

```

An example of the ScpConfiguration.Config file with updates for NilRead™ is shown in Figure 13. This example is for illustrative purposes only.

**Figure 13: Example DICOM SCP Configuration File**

```

1 <gov.va.med.imaging.facade.configuration.ScpConfiguration>
2   <dirty>>false</dirty>
3   <accessCode>C</accessCode>
4   <verifyCode>C</verifyCode>
5   <siteFetchTPoolMax>20</siteFetchTPoolMax>
6   <siteFetchTimeLimit>45</siteFetchTimeLimit>
7   <imageFetchTPoolMax>15</imageFetchTPoolMax>
8   <imageFetchTimeLimit>1000000</imageFetchTimeLimit>
9   <useRemoteImageFetch>true</useRemoteImageFetch>
10  <useDirectFetch>true</useDirectFetch>
11  <cacheLifespan>1</cacheLifespan>
12  <preFetchSeries>true</preFetchSeries>
13  <calledAETitle>ANY_0.0.0.0</calledAETitle>
14  <remotePatientResolution>true</remotePatientResolution>
15  <imageQueueSize>10000</imageQueueSize>
16  <cacheMetaHoursToLive>24</cacheMetaHoursToLive>
17  <isFdtEnabled>true</isFdtEnabled>
18  <fdtPort>2762</fdtPort>
19  <callingAEConfigs>
20    <gov.va.med.imaging.facade.configuration.ScpCallingAE>
21      <aeTitle>AE_SCP_HOST/aeTitle>
22      <callingAeIp>10.10.10.10</callingAeIp>
23      <buildReport>SC</buildReport>
24      <returnQueryLevel>>false</returnQueryLevel>
25      <studyQueryFilter>radiology</studyQueryFilter>
26      <sendKeepAlive>>false</sendKeepAlive>
27      <modalityBlockList>
28        <gov.va.med.imaging.facade.configuration.ScpModalityList>
29          <dataSource>ALL</dataSource>
30          <addImageLevelFilter>>false</addImageLevelFilter>
31          <modalities>
32            <string>none</string>
33          </modalities>
34        </gov.va.med.imaging.facade.configuration.ScpModalityList>
35      </modalityBlockList>
36      <siteCodeBlackList>
37        <string>100</string>
38        <string>200CLMS</string>
39        <string>200CORP</string>
40        <string>741</string>
41        <string>LOCAL</string>
42      </siteCodeBlackList>
43    </gov.va.med.imaging.facade.configuration.ScpCallingAE>
44  </callingAEConfigs>
45 </gov.va.med.imaging.facade.configuration.ScpConfiguration>

```

You can update the following entries for the DICOM SCP functionality as desired beyond the reasonable defaults that are pre-populated (refer to Figure 14 for line numbers):



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

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

12. If desired to query patient identifiers unknown to the local VistA set `remotePatientResolution` to true inside the opening and closing `remotePatientResolution` tags, otherwise set false (inside `<remotePatientResolution> </remotePatientResolution>` - line 14). The default setting is false. When true the VIX will fall back to querying CVIX with any patient identifiers it receives that cannot be resolved locally.
  13. Set the entry for the maximum number of images able to be queued to download at once (inside `<imageQueueSize> </imageQueueSize>` - line 15). The default setting is to 10,000 images.
  14. Set the entry for the number of hours cached metadata is considered valid (metadata older than this time can be overwritten) (inside `<cacheMetaHoursToLive> </cacheMetaHoursToLive>` - line 16). The default setting is to 24 hours.
  15. If desired to enable fast data transfer set `isFdtEnabled` to true inside the opening and closing `isFdtEnabled` tags, otherwise set false (inside `<isFdtEnabled> </isFdtEnabled>` - line 17). The default setting is true.
  16. If desired to change the port for fast data transfer set the port inside the opening and closing `fdtPort` tags (inside `<fdtPort> </fdtPort>` - line 18). The default port is 2762.
- NOTE:** The selected port for fast data transfer must be visible to other VIX across the VA.
17. If desired to see the VA reports as Secondary Capture images, set `buildReport` to SC inside the opening and closing `buildReport` tags (inside `<buildReport> </buildReport>` - line 23). To see VA reports as Structured Reports, set `buildReport` to SR inside the opening and closing `buildReport` tags (inside `<buildReport> </buildReport>` - line 23). To turn off VA report generation, set `buildReport` to NONE inside the opening and closing `buildReport` tags (inside `<buildReport> </buildReport>` - line 23).
  18. If desired to return study query level in C-FIND responses set `returnQueryLevel` to true inside the opening and closing `returnQueryLevel` tags, otherwise set false (inside `<returnQueryLevel> </returnQueryLevel>` - line 24).
  19. The default setting for `studyQueryFilter` is radiology inside the opening and closing `studyQueryFilter` tags (inside `<studyQueryFilter> </studyQueryFilter>` - line 25).

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



for any other modality not included in other filters available, cl\_radiology filters for any radiology related study modality.

20. If desired to not have actively serviced C-MOVE timeouts, set sendKeepAlive to true inside the opening and closing sendKeepAlive tags, otherwise set false (inside `<sendKeepAlive> </ sendKeepAlive >` - line 26). The default setting is false.
21. If desired to not fetch certain modality images, set the entries inside the opening and closing modalityBlockList tags for different dataSources.
  - a. For each dataSource (DoD or VA), set different modality lists if necessary, by inserting DoD or VA inside the opening and closing dataSource tags (`<dataSource> </dataSource>` - line 29), by default the value is ALL.
  - b. The modalities will be filtered at study and series levels. If needed, set at the image level. To do so, set true at the image level when needed by inserting true inside the opening and closing addImageLevelFilter tags, otherwise set false (`<addImageLevelFilter> </addImageLevelFilter>` - line 30).
  - c. List all the modalities to be blocked for that dataSource separately using string tags inside the opening and closing modalities section (`<modalities> </modalities>` - lines 31 and 33). Examples of modalities to potentially include inside the string tags include SR and PR.
22. The installer automatically generates a default blacklist consisting of site codes that configured DICOM SCUs do not receive data from. Your local site code and the site codes of your Veterans Integrated Service Network (VISN) appear in the `<siteCodeBlackList>` section in the file ScpConfiguration.config located in the C:\VixConfig folder. If you want your site's data to be available to the configured DICOM SCU, ensure your local site code is not in the `<siteCodeBlackList>` section in the ScpConfiguration.config. List all the site codes to be blocked separately using string tags inside the opening and closing siteCodeBlackList section (`<siteCodeBlackList > </siteCodeBlackList >` - lines 36 and 42). Examples of site codes to include inside the string tags include the following:
  - a. Set a string to 100 to exclude Claims system information.
  - b. Set a string tag to 200CLMS to exclude 200 VHA Claims study information.
  - c. Set a string tag to 200CORP to exclude the Claims site.
  - d. Set a string tag to 741 to exclude Global Disability Examinations.
  - e. Set a string tag to LOCAL to signal the DICOM Service to replace it with the local site number and all of the sites in that Veterans Integrated Service Networks (VISN).

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

Save the ScpConfiguration.Config file after updating the entries. After updating the DICOM SCP config file, the ScpConfiguration.Config file will look like (Figure 14):

**Figure 14: Sample DICOM SCP Configuration File**

```

1 <gov.va.med.imaging.facade.configuration.ScpConfiguration>
2   <dirty>false</dirty>
3   <accessCode>[REDACTED]</accessCode>
4   <verifyCode>[REDACTED]</verifyCode>
5   <siteFetchTPoolMax>20</siteFetchTPoolMax>
6   <siteFetchTimeLimit>45</siteFetchTimeLimit>
7   <imageFetchTPoolMax>15</imageFetchTPoolMax>
8   <imageFetchTimeLimit>1000000</imageFetchTimeLimit>
9   <useRemoteImageFetch>true</useRemoteImageFetch>
10  <useDirectFetch>true</useDirectFetch>
11  <cacheLifespan>1</cacheLifespan>
12  <preFetchSeries>true</preFetchSeries>
13  <calledAETitle>ANY_0.0.0.0</calledAETitle>
14  <remotePatientResolution>true</remotePatientResolution>
15  <imageQueueSize>10000</imageQueueSize>
16  <cacheMetaHoursToLive>24</cacheMetaHoursToLive>
17  <isFdtEnabled>true</isFdtEnabled>
18  <fdtPort>2762</fdtPort>
19  <callingAEConfigs>
20    <gov.va.med.imaging.facade.configuration.ScpCallingAE>
21      <aeTitle>AE_SCP_HOST</aeTitle>
22      <callingAeIp>10.10.101.101</callingAeIp>
23      <buildReport>SC</buildReport>
24      <returnQueryLevel>false</returnQueryLevel>
25      <studyQueryFilter>radiology</studyQueryFilter>
26      <sendKeepAlive>false</sendKeepAlive>
27      <modalityBlockList>
28        <gov.va.med.imaging.facade.configuration.ScpModalityList>
29          <dataSource>ALL</dataSource>
30          <addImageLevelFilter>false</addImageLevelFilter>
31          <modalities>
32            <string>none</string>
33          </modalities>
34        </gov.va.med.imaging.facade.configuration.ScpModalityList>
35      </modalityBlockList>
36      <siteCodeBlackList>
37        <string>100</string>
38        <string>200CLMS</string>
39        <string>200CORP</string>
40        <string>741</string>
41        <string>LOCAL</string>
42      </siteCodeBlackList>
43    </gov.va.med.imaging.facade.configuration.ScpCallingAE>
44  </callingAEConfigs>
45 </gov.va.med.imaging.facade.configuration.ScpConfiguration>

```

For additional DICOM SCU calling AE titles, insert an additional block of code containing the elements from lines 19 to 43 before current line 44 and then repeat steps 1 to 22 inside these additional lines that have been added, see Figure 15.

**Figure 15: Sample DICOM SCP Configuration File with Multiple DICOM SCU Calling AE Titles**

```

19  <callingAEConfigs>
20    <gov.va.med.imaging.facade.configuration.ScpCallingAE>
21      <aeTitle>ALL/aeTitle>
22      <callingAeIp>0.0.0.0</callingAeIp>
23      <buildReport>SC</buildReport>
24      <returnQueryLevel>>false</returnQueryLevel>
25      <studyQueryFilter>radiology</studyQueryFilter>
26      <sendKeepAlive>>false</sendKeepAlive>
27      <modalityBlockList>
28        <gov.va.med.imaging.facade.configuration.ScpModalityList>
29          <dataSource>ALL</dataSource>
30          <addImageLevelFilter>>false</addImageLevelFilter>
31          <modalities>
32            <string>none</string>
33          </modalities>
34        </gov.va.med.imaging.facade.configuration.ScpModalityList>
35      </modalityBlockList>
36      <siteCodeBlackList>
37        <string>100</string>
38        <string>200CLMS</string>
39        <string>200CORP</string>
40        <string>741</string>
41        <string>LOCAL</string>
42      </siteCodeBlackList>
43    </gov.va.med.imaging.facade.configuration.ScpCallingAE>
44    <gov.va.med.imaging.facade.configuration.ScpCallingAE>
45      <aeTitle>ALL/aeTitle>
46      <callingAeIp>      </callingAeIp>
47      <buildReport>SC</buildReport>
48      <returnQueryLevel>>false</returnQueryLevel>
49      <studyQueryFilter>radiology</studyQueryFilter>
50      <sendKeepAlive>>false</sendKeepAlive>
51      <modalityBlockList>
52        <gov.va.med.imaging.facade.configuration.ScpModalityList>
53          <dataSource>ALL</dataSource>
54          <addImageLevelFilter>>false</addImageLevelFilter>
55          <modalities>
56            <string>none</string>
57          </modalities>
58        </gov.va.med.imaging.facade.configuration.ScpModalityList>
59      </modalityBlockList>
60      <siteCodeBlackList>
61        <string>100</string>
62        <string>200CLMS</string>
63        <string>200CORP</string>
64        <string>741</string>
65        <string>LOCAL</string>
66      </siteCodeBlackList>
67    </gov.va.med.imaging.facade.configuration.ScpCallingAE>
68  </callingAEConfigs>
69  </gov.va.med.imaging.facade.configuration.ScpConfiguration>

```

After updating the ScpConfiguration.Config file, as described above, it is necessary to restart the Apache Tomcat service. One way this can be performed is by executing the restart script (Restart\_VIX\_Services.ps1) as described in the [CVIX Installation Guide](#).

### 3.12.5. Laurel Bridge DICOM SCP Configuration

This section provides details on the Laurel Bridge DICOM file located in the cfg folder within the Laurel Bridge installation directory (C:\DCF\_RunTime\_x64\cfg by default) are desired. This is useful for debugging purposes but the details on how to change this are beyond the scope of this document. For typical CVIX operation, no changes are necessary to the Laurel Bridge DICOM file.

Open the DicomScpConfig file to perform edits. Run Notepad, Notepad++, or WordPad as an administrator, and then open the file. Numerous entries can be updated in the DicomScpConfig configuration file (Figure 16). Save the DicomScpConfig file after updating the entries.

**Figure 16: Sample DicomScpConfig Configuration File**

```

1 [ application_info ]
2 name = DicomScp
3 description = Java server app that demonstrates use of QRServer and DicomSCP in DCS lib.
4 app_component_name = java_app/DicomScp
5 #app_component_name = cfg_app_name
6 execution_state = STOPPED
7
8 [ required_components ]
9 component = java_lib/LOG_a
10 component = java_lib/DCF
11 component = java_lib/LOG
12 component = java_lib/APC
13 component = java_lib/CDS
14 component = java_lib/APC_a
15 component = java_lib/CDS_a
16 component = java_lib/DCS
17 component = idl_lib/DDCS
18 component = java_lib/DSS
19 component = java_lib/DDS
20 component = java_lib/DDS_a
21 [ java_app ]
22
23 #=====
24 # per-instance information for the DicomScp component
25 #=====
26 [ java_app/DicomScp ]
27 #debug_flags = 0x0000f
28 debug_flags = 0x00000
29
30 #
31 # if true, demonstrate the DataSetByteReader class for making
32 # a a decoded, and re-encoded network C-Store-Request look like
33 # a ReadableByteChannel or InputStream object.
34 #
35 use_byte_reader = YES
36
37 image_directory =
38 make_new_uids = FALSE
39 test_cfg_name = dcms.cfg
40 dicom_files_dir = dcms.cfg
41
42
43 [ java_lib ]
44
45 #=====
46 # per-instance information for the LOG_a component
47 #=====
48 [ java_lib/LOG_a ]
49 debug_flags = 0

```

After updating the DicomScpConfig file, as described above, it is necessary to restart the Apache Tomcat service. One way this can be performed is by executing the restart script (Restart\_VIX\_Services.ps1) as described in the [CVIX Installation Guide](#).

### 3.13. Configure ID Conversion

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

Perform this step to further configure the CVIX collection of DoD medical images to ECIA via the IdConversionConfiguration.config file which configures the destination of the ID conversion lookup.

**NOTE:** Before moving forward with the instructions for this step, it is expected that the site administrator is aware of all needed entries in the configuration, including the <protocol>, </host>, <port>, <username>, and <password> of the ID lookup.

**NOTE:** Some of the configuration including <host>, <username>, and <password> may be set based on the server type (i.e. test or production) during the end of the install via the PowerShell script utility. If these values are not the same as the values you have for these in the installation prerequisites, change them according to the values for these in the prerequisites; otherwise, leave them as they are.

Open the IdConversionConfiguration.config in C:\VixConfig. Run Notepad, Notepad++, or WordPad as an administrator, and then open the file.

To configure the ID lookup (refer Figure 17 to for line numbers):

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

8. Set the trustStorePassword (inside <trustStorePassword> </trustStorePassword> - line 10) (only if a change is needed).

Save the IdConversionConfiguration.config file after updating the entries. The IdConversionConfiguration.config should look like Figure 17.

**Figure 17: Sample IdConversionConfiguration.config file**

```
1 <gov.va.med.imaging.facade.configuration.IdConversionConfiguration>
2   <dirty>false</dirty>
3   <protocol>https</protocol>
4   <host>NEED.TO.CHANGE.HOST</host>
5   <port>443</port>
6   <urlResource>...</urlResource>
7   <username>**ADD USERNAME**</username>
8   <password>**ADD PASSWORD**</password>
9   <trustStoreFilePath>C:\VixCertStore\federation.truststore</trustStoreFilePath>
10  <trustStorePassword>**ADD PASSWORD**</trustStorePassword>
11 </gov.va.med.imaging.facade.configuration.IdConversionConfiguration>
```

## 4. VistA Site Service

This section covers:

- VistA Site Service Overview
- Checking the Site Service
- Updating Site Service Data

### 4.1. VistA Site Service Overview

The VistA Site Service is a central repository of connection information. Several Imaging components use the data stored in the site service to connect to Imaging components at other sites, remote VistA systems, and the CVIX.

Because the site service is centralized, Imaging components (such as a VIX or a Clinical Display workstation) at each VA site can use the site service's connection information without having to locally store and maintain any connection information.

When data is requested from the site service, the request goes to the CVIX's active load balancer. The load balancer passes the request to a node in the CVIX cluster, and that node retrieves the requested connection information from the site service primary configuration file (<C:\VixConfig\VhaSites.xml>). Then the connection information is passed back to the load balancer and ultimately back to the requestor.

The following sections explain how to check and maintain the site service.

### 4.2. Checking the Site Service

To access a listing of what is in the site service, use a browser to go to **REDACTED**. The page that displays list the connection information for all sites registered in the site service. Sites are grouped by VISN (Veterans Integrated Service Network) name.

Additional non-VISN sites are listed at the bottom of the page.

### 4.3. Updating Site Service Data

If the connection information in the site service needs to be changed, do the following.

1. Identify the specific information that needs to be changed. Typically, this will be received in an email directed to the **REDACTED** mail group.
2. Use ping or a similar command to verify that the information is correct.
3. Create an offline copy of the VhaSites.xml file. An instance of this file is stored in the <C:\VixConfig> folder on each CVIX node.
4. In the offline copy of VhaSites.xml, locate and update the applicable information.



5. On each CVIX server node, copy the modified VhaSites.xml file to the following folders (the CVIX can remain active during this activity):
  - [C:\VixConfig](#)
  - [C:\SiteService](#)
6. For each CVIX node, refresh its cached site service connection information by doing the following:
  - f. Use a browser to go to <http://xxx/Vix/secure/SiteService.jsp>, where <xxx> is the name of the CVIX node.
  - g. In the Site Service Utilities web, click the **Refresh Site Service** button.
7. Notify the originators of the request that the site service has been updated, and work with them to ensure the new connection information works as expected.

**NOTE:** A site VIX will not pick up the revised site information until it is restarted or until the VIX automatically updates its cached connection information at 11:00 P.M. daily.



## 5. CVIX Image Sharing

The CVIX is a key link in VA-DoD image exchange and is the primary source of information for the JLV. A functional description of the CVIX's image-sharing capabilities is covered in *CVIX Major Functions*. This section covers:

- Remote Metadata Retrieval
- Remote Image Retrieval
- Caching of Metadata and Images
- Image Sharing and CVIX Timeouts

### 5.1. Remote Metadata Retrieval

When an application requests images via a CVIX, the process usually takes two steps: metadata retrieval and then retrieval of the actual image.

**NOTE:** In the context of the CVIX, metadata is anything that describes an image or image-like object. Metadata includes patient names, IDs of various types, procedure names, the number of images in an exam, and so on.

In some cases, metadata retrieval is the only action needed to fulfill a clinician's data request. One example of this is the retrieval of an exam report. Also, in some cases (such as a request for a patient ID image by the JLV), an image request may not require a preliminary metadata request.

The CVIX handles metadata retrievals as follows:

1. An application issues a request for metadata based on a clinician's activities. The applications in Table 10 can request metadata from the CVIX.

**Table 10: Types and Sources of Metadata requested by Application**

Requesting Application	Type of metadata requested	CVIX interface used by requestor**	Ultimate source of requested metadata
VIX (on behalf of JLV, Clinical Display or VistARad, VIX Viewer)	DoD metadata for all DoD image/artifact types	Federation	ECIA for DICOM-related metadata or DES via DAS for artifact-related metadata (through DX)
DAS	VA metadata related to DICOM images and artifacts	MIX, AX	VIX at VA site if VIX is available. VistA at VA site if VIX is not available

**NOTE:** See *CVIX Interfaces* for more information about CVIX interfaces.

2. If the CVIX is processing a request from the DAS, the CVIX uses the VistA system at Station 200 to determine where in the VA the applicable patient was treated.
3. The CVIX retrieves metadata in the most expeditious manner possible:
  - If caching is allowed for the metadata in question, the CVIX checks its local cache for the metadata.
  - If caching is not allowed or the metadata is not in the CVIX cache, the CVIX contacts the remote system where the metadata is stored and retrieves the metadata (see the right column in Table 10).

The CVIX passes the data back to the requesting application.

## **5.2. Remote Image Retrieval**

When a CVIX gets a request for an image, the CVIX uses the following process to deliver the most desirable image in the shortest amount of time. Typically, an image request is preceded by a metadata request, as described in the previous section.

1. One of the following applications requests a remote image based on a clinician's activities:
  - DAS (from HAIMS) on behalf of a DoD clinician (VA DICOM images).
  - DAS (from DES) on behalf of a DoD clinician (VA non-DICOM images).
  - Clinical Display, VistARad, or VA JLV on behalf of a VA clinician (DoD images).
  - DoD users of JLV, requesting VA artifacts via DES and DAS
  - Image Viewer on behalf of a VA clinician (VA images).
2. The CVIX first checks its local cache for the image.
  - If the image is in the local CVIX cache and is of the desired quality and is in any of the acceptable formats, the CVIX stops the search and proceeds to step 5.
  - If the image is not stored in the local CVIX cache, the CVIX checks the SQLite database if the item is stored in the cluster of CVIX nodes and if an entry is found, the CVIX contacts the node fetches the data, and proceeds with step 5. Otherwise, the CVIX retrieves the image from its source.
3. Depending on the image quality specified by the requestor, the image may be compressed at this point.
  - If the image originates from the VA, a VIX may perform the compression if a VIX is present at the originating site. If no VIX is present, the CVIX performs the compression if compression is applicable.
  - If the image originates from the DoD, the CVIX does not perform any compression before sending the image to the requestor. (In the case of DICOM images requested by VistARad via a VIX, the images are already compressed and will be decompressed by the VIX).

- Possible image quality parameters are described in Table 11.

**Table 11: VIX Image Quality Parameters**

Parameter	Compression
DIAGNOSTIC UNCOMPRESSED	None. Used for objects that will be sent in their native formats such as TIF or PDFs. This parameter will be used by the CVIX when requesting full-fidelity non-radiology images from a VA site with a VIX.
DIAGNOSTIC	Lossless compression; typically used for DICOM (radiology) images. The highest-resolution available image is located and compressed. The typical compression ratio is about 2.5:1. Any image requestor can use this parameter.
REFERENCE	Lossy compression; typically used for DICOM (radiology) images. The highest-resolution available image is located and compressed. The compression ratio averages about 24:1 for CR images and 10:1 for CT and MR images. Any image requestor can use this parameter.

4. The CVIX caches the image in its local cache. If the CVIX compressed the image, the compressed version is cached, not the original version.
5. The CVIX sends the image to the requesting system.

## 5.3. Caching of Metadata and Images

The CVIX automatically stores all images and most of the metadata it handles in its local cache. The local CVIX cache is self-managing and is independent of other Imaging storage areas and caches.

The CVIX cache improves the CVIX's performance by storing data (especially images) retrieved from remote sites and/or processed by the CVIX. If the image is requested again, it can be pulled from the CVIX's cache or from another CVIX cluster node (when the Cache Cluster option is enabled) without having to retrieve it from the remote site or reprocess it.

**NOTE:** Metadata and images cached by the CVIX 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 CVIX.

### 5.3.1. Cache Retention Periods

The CVIX purges data from its cache when the retention period for the data is reached. Images are considered static data that allow longer cache retention while retaining data consistency. Metadata, which is less static, is retained for shorter periods.

Table 12 lists retention periods based on the source and type of data.

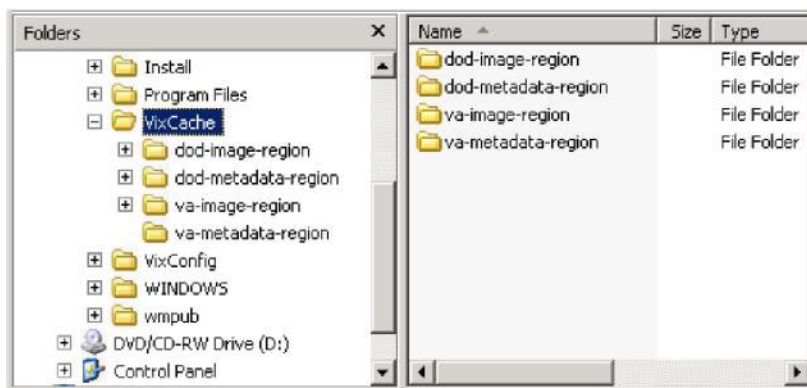
**Table 12: Image Data Retention Periods**

Data type	Retained for	Scan to delete old items is run
VA and DoD images	7 / 30 days	Once per day at 3 AM
VA metadata	1 hour	Once per minute
DoD metadata	1 day	Once per hour
DICOM SCP images and metadata	30 days	Once per minute

### 5.3.2. Cache Location and Structure

The CVIX cache is located in [x:\VixCache](#) on each node in the CVIX load-balanced cluster, where x is usually the E drive.

The CVIX cache is divided into regions based on the source and type of data being handled. These regions are reflected in the folder structure of the cache (Figure 18).

**Figure 18: CVIX Folder Structure**

Subfolders for each region are further broken down by STATION NUMBER (field (#99) of the INSTITUTION file (#4)) and then by internal ID numbers. Internal ID numbers do not trace back to live data such as SSNs or case IDs.

**NOTE:** Never manually change the contents of the VixCache folder and subfolders while the CVIX is running.

## 5.4. Image Sharing and CVIX Timeouts

When the CVIX retrieves metadata and images from remote sites, the system load at the remote site and Wide Access Network (WAN) network traffic will impact the time needed to complete the retrieval. If a request for data cannot be completed promptly, the CVIX will cancel its request. This prevents excessive delays in client applications that are the ultimate consumers of the metadata and images.

Table 13 summarizes CVIX connection timeout parameters based on the type of remote system and data involved.

**Table 13: CVIX Connection Timeout Parameters**

Remote System Type	CVIX Timeout Behavior
VA data via a remote VIX	<p>For metadata, 600 seconds for data transfer to begin (this is to handle very large datasets; usually, the data transfer begins in a few seconds).</p> <p>For images, wait up to 30 seconds for the initial connection and up to 120 seconds for data transfer to begin.</p>
VA data from a remote non-VIX VA site	<p>For metadata, no timeout.</p> <p>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.</p>
DoD data	<p>For metadata, the CVIX will wait up to 45 seconds to retrieve DoD metadata before sending a timeout message to the VIX that requested the data. 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 VIX that originally requested the data.</p>

## 6. VIX Log Collector Service

This section covers:

- VIX Log Collector Overview
- Log Collector Automatic Emails
- Archived Transaction Log Storage Area
- Excluding a VIX from Log Collection

### 6.1. VIX Log Collector Overview

The Log Collector automatically backs up transaction logs from remote VIXes and from the CVIX. This allows the information in VIX transaction logs to be retained after local logs are purged (the standard local retention period is 90 days).

Once a day, the Log Collector uses the VistA site service to retrieve connection information for all remote VIXes and the CVIX. The Log Collector then collects one full day's worth of transaction log entries from each VIX (and the CVIX). To ensure that all entries are captured for a given day, the Log Collector pulls entries that are at least 48 hours old. For example: on Monday, the Log Collector service will collect all VIX log entries from the previous Saturday. Logs are collected at 5:30 A.M.

In general, the Log Collection service does not need to be monitored.

- If the Log Collector cannot reach a VIX on a given day, it will queue its backup attempt and attempt to copy any backlogged items during the next backup period.
- If the CVIX failover cluster is rebooted, the Log Collector restarts automatically.

To manually verify that the Log Collector is gathering logs as expected, check the storage area **REDACTED** (E:\VIXLogs\) for collected logs for newly backed up files. For specifics, see the *Archived Transaction Log Storage Area*.

### 6.2. Log Collector Automatic Emails

If the Log Collector has any errors over a day, these errors are summarized into an email and sent to specified addressees each day at 7:30 A.M. The email subject line is always "Log Collection Errors."

Email addresses are initially specified when the Log Collector service is installed. To change the email recipient, use the following steps:

1. Login as an administrator to the active server.
2. Navigate to [C:\Program Files \(86\)\VistA\Imaging\VixLogCollectorService](#).
3. Open the file named VixLogCollector.WindowsService.exe.config in a text editor.
4. Locate the "emailAddress" key near the beginning of the file.

5. Edit the value for the emailAddress key as needed. Separate each email address with a comma.
6. Save and close the file.
7. Open the Services window (click **Start | All Programs | Administrative Tools | Services**).
8. On the right side of the window, locate the VIX Log Collector service.
9. Click the Restart the service link and wait until the service restarts.

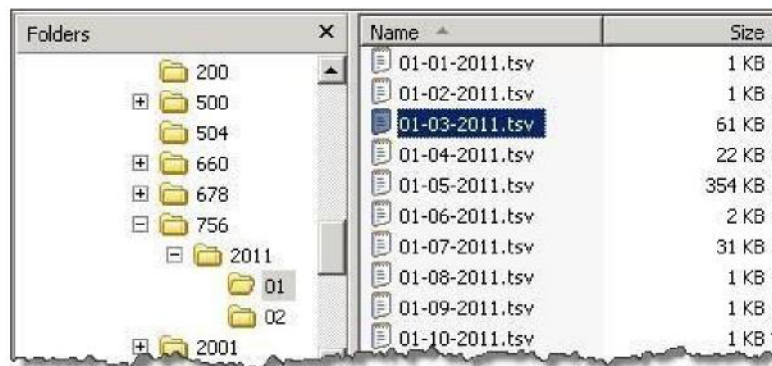
### 6.3. Archived Transaction Log Storage Area

The archived transaction log files gathered by the Log Collector are stored under [G:\VIXLogs](#) on the failover cluster (Figure 19). The folder structure is set up as follows:

[G:\VIXLogs\site\year\month](#)

...where *site* is the station number of the site where the log came from, and *year* and *month* indicate when the log was collected. In each *month* folder, each day's worth of transaction log entries for a specific VIX (or CVIX) is stored in a separate tab-separated file.

**Figure 19: Transaction Log File Display Example**



**NOTE:** Only logs more than 48 hours old are archived. A subfolder for the current month will not be created until the third day of the current month.

The month-specific folders in this structure are compressed using standard Windows compression.

### 6.4. Excluding a VIX from Log Collection

Use the following steps to disable the automatic collection of transaction logs from a specific VIX or CVIX:

1. Determine the ID number of the VIX or CVIX for which log collection is to be disabled.
  - For a site VIX, this is the STATION NUMBER (field (#99) of the INSTITUTION file (#4) of the site where the VIX resides.

- For the CVIX, this value will be 2001.
- 2. Login as an administrator to the active server.
- 3. Navigate to where the archive logs are stored ([E:\VixLogs](#) is the default location).
- 4. Open the folder of the VIX (or CVIX) to disable it.
- 5. Use a text editor to open the VixInfo.xml file.
- 6. Locate the IsActive element and change the element value from “true” to “false”.
- 7. Save and close the file.



## 7. CVIX Troubleshooting

This section covers:

- Routine Errors
- Significant Errors
- Unplanned Shutdowns
- CVIX Support Routine Errors

### 7.1. Routine Errors

The system may generate a small set of errors that may be considered routine in the sense that they have minimal impact on the user and do not compromise the operational state of the system. Most of the errors are transient and only require the user to retry an operation. The following subsections describe these errors, their causes, and what, if any, response an operator needs to take.

While the occasional occurrence of these errors may be routine, a large number of errors over a short period is an indication of a more serious problem. In that case, many errors need to be treated as an exceptional condition.

#### 7.1.1. Connectivity

Occasional data retrieval failures are expected given the nature of the WAN and the number of systems communicating with the VIX.

#### 7.1.2. Timeouts

The CVIX will cancel a data request if it does not get a response from the system in question. For specific timeout information, see *Image Sharing and CVIX Timeouts*.

#### 7.1.3. Security

Since the system is a component of a larger system that is responsible for user-level security, it is expected that all errors related to security are handled by the controlling application. All security failures (e.g., inability to access resources or stored objects) are generally caused by the controlling application either incorrectly passing security tokens or failing user authentication. Other security issues are under the jurisdiction of the site VistA Imaging security which has already established protocols and procedures.

If DoD clinicians cannot access any VA images and if Station 200 appears to be available, check the credentials for the CVIX USER service account on Station 200 to ensure that it has not expired. If VA clinicians cannot access DoD artifacts (scanned documents and non-radiology) images, the issue may be the authentication at DAS.

#### **7.1.4. Station 200 Issues**

If there is a temporary Station 200 VistA System outage, the CVIX will automatically refresh any previously cached connections within 30 seconds to 1 minute after Station 200 comes back online. DoD clinicians may have to repeat their most recent image requests, but any issues encountered should be transitory.

If there is an extended Station 200 outage, DoD clinicians will not be able to access VA images for VA/DoD shared patients. VA clinicians/ VBA connecting to CVIX will also be impacted.

If DoD clinicians cannot access any VA images and if Station 200 appears to be available, check the credentials for the CVIX USER service account on Station 200 to ensure that they have not expired.

### **7.2. Significant Errors**

Significant errors can be defined as errors or conditions that affect the system's stability, availability, performance, or otherwise make the system unavailable to its user base. The following subsections contain information to aid administrators, operators, and other support personnel in resolving significant errors, conditions, or other issues.

#### **7.2.1. Error Logs**

The CVIX transaction log is the first place to check for errors related to data retrieval. The CVIX transaction logs include unique transaction IDs that can be used to track related actions across other systems (such as other VIXes).

**NOTE:** Because the CVIX is set up as a load-balanced cluster without server affinity, check multiple CVIX nodes to see all log entries related to a given transaction (that is, receipt and fulfillment of a specific data request).

For detailed information about the transaction log, see *CVIX Transaction Log Fields*.  
For information about the CVIX's Java logs, see *CVIX Java Components*.

### **7.3. Unplanned Shutdowns**

#### **7.3.1. Recovering after unplanned restart of a single CVIX server**

If a single server in the CVIX cluster has an unscheduled restart, the request that it was actively processing at the time will fail. However, as soon as the server restarts, the CVIX service will also restart, and processing will continue as normal.

If the CVIX service on a single cluster node encounters a fatal error, the CVIX service will restart itself automatically after 60 seconds and continue restarting itself if it encounters additional errors.

If a specific cluster node needs to be taken offline, use the steps in *CVIX cluster: take the node offline*.

### 7.3.2. Recovering after unplanned reboot of a single load balancer

If a load balancer shuts down unexpectedly, the second load balancer will automatically begin handling CVIX operations. Let the second load balancer retain the active role if this occurs.

### 7.3.3. Recovering after an unscheduled power loss to all components

Startup the CVIX as described in *Planned Full CVIX Startup* and issue an ANR describing the nature of the outage and its resolution time.

Closely monitor CVIX operations until normal operations are verified.

## 7.4. System Recovery

The following subsections define the process and procedures necessary to back-out and rollback the system to a fully operational state after a service interruption. Each of the subsections starts at a specific system state and ends up with a fully operational system.

### 7.4.1. Back-out Procedures

If it is necessary to uninstall the MAG\*3.0\*348 Vista KIDS, you need to select the “Kernel Installation & Distribution System” menu option, “Backup a Transport Global” (see section 4.8.1, Step 4c of [MAG\\*3.0\\*348 Deployment, Installation, Back-Out, and Rollback Guide](#).), before you uninstall the patch.

Administrators will need to use the PackMan function INSTALL/CHECK MESSAGE. Check MailMan messages for the backup message sent by the “Backup a Transport Global” function executed before the patch install.

1. Select the **inbox** message shown below:

**Backup of MAG\*3.0\*348 install on *mmm dd, yyyy* *installer user name***

2. Select the Xtract PackMan option.
3. Select the Install/Check Message option.
4. Enter “Yes” at the prompt.
5. Enter “No” at the backup prompt. There is no need to back up the backup.

Enter message action (in IN basket): Ignore// Xtract PackMan

Select the PackMan function: ?

Answer with PackMan function NUMBER, or NAME

Choose from:

- 1      ROUTINE LOAD
- 2      GLOBAL LOAD
- 3      PACKAGE LOAD
- 4      SUMMARIZE MESSAGE
- 5      PRINT MESSAGE
- 6      INSTALL/CHECK MESSAGE
- 7      INSTALL SELECTED ROUTINE(S)
- 8      TEXT PRINT/DISPLAY
- 9      COMPARE MESSAGE

Select PackMan function: Select PackMan function: 6 INSTALL/CHECK MESSAGE

**Warning:** Installing this message will cause a permanent update of globals and routines.

Do you really want to do this? NO// YES<Enter>

Routines are the only parts that are backed up. NO other parts are backed up, not even globals. You may use the 'Summarize Message' option of PackMan to see what parts the message contains.

Those parts that are not routines should be backed up separately if they need to be preserved.

Shall I preserve the routines on disk in a separate backup message? YES// NO

No backup message built.

Line 2   Message #42925   Unloading Routine   MAGxxxx (PACKMAN\_BACKUP)

Select PackMan function: <Enter>

## 7.4.2. Rollback Procedures

If it is necessary to uninstall the MAG\*3.0\*348 CVIX, go to the Control Panel, choose Add/Remove Programs, and remove the MAG\*3.0\*348 CVIX Service Installation Wizard. To rollback the CVIX and replace it with the prior version which was included in MAG\*3.0\*329, please see the [MAG\\*3.0\\*348 CVIX Installation Guide](#) for more detail.

## 7.5. CVIX Support

Problems encountered with the CVIX that are not addressed in this document will require the entry of a Service Now Ticket for VistA Imaging/CVIX Support.

Contact the **VA IT DAS Technical** mail group at **REDACTED** for ongoing connectivity issues with DAS. If there is a CVIX outage, file an Automated Notification Report (ANR) at **REDACTED** or contact the National Help Desk at **REDACTED**.

## 8. CVIX Reference/Software Description

### 8.1. CVIX Java Components

The following sections summarize the CVIX's primary Java components.

#### 8.1.1. CVIX Servlet Container

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

#### 8.1.2. CVIX Security Realms

The CVIX implements security realms to verify that only properly authenticated applications (the site VIXes, and DoD systems) can use the CVIX Web applications' interfaces. Authentication is handled silently by the application and the CVIX and does not require an explicit login by clinicians requesting images. See *CVIX Connection Security* for more information.

#### 8.1.3. CVIX Interfaces

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

CVIX interfaces are used both for metadata and image retrieval. In general, each CVIX interface implements a Web service that handles metadata requests and an image servlet that handles image requests. Table 14 summarizes each CVIX interface.

**Table 14: CVIX Interfaces**

Interface Name	Description
DICOM SCU	Handles DICOM metadata and image requests from DoD providers via CVIX. Uses port REDACTED with the specified application entities (AEs).
Federation interface	Handles metadata and image requests from site VIXes; uses port REDACTED.
DX	Handles non-DICOM metadata and image requests from CVIX to HAIMS and DES via DAS. Uses port REDACTED.
VIX Viewer	Provides Viewing images and retrieving metadata for consuming applications (JLV and VIX)

When an interface receives a request, it issues the appropriate command to the CVIX core (described in the next section) for proper disposition. When the CVIX core ultimately responds (the requested data), the same interface responds to the requesting application.

### 8.1.4. CVIX Core

The CVIX core provides the central switching intelligence for the CVIX. It:

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

### 8.1.5. CVIX Data Sources

The CVIX has a dedicated data source for each outside entity that it retrieves data from. Data sources receive requests from and return responses to the CVIX core. Table 15 summarizes each CVIX data source. These data sources are identified in the Datasource Protocol field in the CVIX transaction log.

**Table 15: CVIX Data Sources**

Data Source Name	Description
vistaimaging	Retrieves data from a VistA Imaging System using RPCs.
vista	Retrieves data from a VistA system without Imaging using RPCs. The CVIX currently uses this data source for communicating with the Station 200 VistA system.
vftp	Retrieves data from other VIXes (or the CVIX) using their Federation interfaces.
FHIR	Retrieves non-DICOM metadata from DAS and non-DICOM images from DES via DAS servers.
ECIA	Retrieves metadata and DICOM images.

## 8.2. Java Installation Locations

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

### 8.2.1. CVIX folders on the System Drive

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

#### **\DCF\_RunTime\_x64**

Laurel Bridge DICOM Connectivity Framework (DCF) toolkit files.

#### **\Program Files\Apache Software Foundation\Tomcat 9.0**

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

**\bin** – servlet engine executables and Aware JPEG2000 toolkit files

**\conf** – servlet engine configuration files

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

**\logs** – Java and debugging logs

**\temp** – temporary files

**\webapps** – CVIX Web applications and associated parameter files

**\work** – servlet engine system files

### **\Program Files\Java\jre1.8.0\_371**

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

### **\VixCertStore**

Stores CVIX security certificates. For details about security certificates, see the *CVIX Security Certificates*.

### **\VixCache**

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

### **\VixConfig**

Configuration files are used by the CVIX Java components and the CVIX transaction log.

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

## **8.2.2. Java Logs**

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

**NOTE:** A symbolic link with the name ImagingArchivedLogsLink also resides in \Program Files\Apache Software Foundation\Tomcat 9.0\logs. This symbolic link points to the log archive



folder named ImagingArchivedLogs with the corresponding drive letter specified during installation.

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

**catalina.log:** Tomcat (CVIX servlet container) output.

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

**ImagingCache.log:** CVIX cache output.

**ImagingExchangeWebApp.log:** CVIX 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:** CVIX security realm output.

## 8.3. VistA/M Information

Table 16 describes the RPCs (Remote Procedure calls) that the CVIX uses when it retrieves data from remote VistA systems. The RPCs listed in these sections are only called when getting data from VA sites that do not have a VIX.

### 8.3.1. RPCs used by the CVIX

Table 16: MAG (VistA Imaging) RPCs Used by the CVIX

RPC Name	Description
<b>MAG BROKER SECURITY</b> Routine: BSE^MAGS2BSE	Returns a BSE token from BSE XUS SET VISITOR.
<b>MAG DOD GET STUDIES IEN</b> Routine: STUDY2^MAGDQR21	Returns study information based on the IMAGE file (#2005) Internal Entry Number (IEN) of the image group provided as a parameter.
<b>MAG DOD GET STUDIES UID</b> Routine: STUDY1^MAGDQR21	Returns study information based on the Study UID that is provided as a parameter.
<b>MAG GET NETLOC</b> Routine: SHARE^MAGGTU6	Returns a list of all entries in the NETWORK LOCATION file (#2005.2).

<b>RPC Name</b>	<b>Description</b>
<b>MAG IMAGE CURRENT INFO</b> Routine: INFO^MAGDQR04	Returns current values for the various DICOM tags that are to be included in the header of an image.
<b>MAG NEW SOP INSTANCE UID</b> 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.
<b>MAG3 CPRS TIU NOTE</b> Routine: IMAGES^MAGGNTI	Returns a list of all images for a Text Integration Utility (TIU) document.
<b>MAG4 GET IMAGE INFO</b> Routine: GETINFO^MAGGTU3	Returns specific fields of an image entry for display in the Clinical Display Image Information window.
<b>MAG4 PAT GET IMAGES</b> Routine: PGI^MAGSIXG1	Returns a list of image groups from the IMAGE file (#2005) based on filters provided.
<b>MAGG CPRS RAD EXAM</b> Routine: IMAGEC^MAGGTRAI	Returns a list of images for the radiology exam.
<b>MAGG GROUP IMAGES</b> Routine: GROUP^MAGGTIG	Returns array of images for a group entry in the IMAGE file (#2005). Included for backward compatibility only.
<b>MAGG INSTALL</b> Routine: GPACHX^MAGQBUT4	Returns a list of all Imaging package installs on the host system.
<b>MAGG LOGOFF</b> Routine: LOGOFF^MAGGTAU	Tracks the time of the Imaging session.
<b>MAGG OFFLINE IMAGE ACCESSED</b> Routine: MAIL^MAGGTU3	Sends a message when there is an attempt to access image from an offline jukebox platter.
<b>MAGG PAT FIND</b> Routine: FIND^MAGGTPT1	Used for patient lookups.
<b>MAGG PAT INFO</b> Routine: INFO^MAGGTPT1	Returns a string of '^' delimited pieces of patient information.
<b>MAGG PAT PHOTOS</b> Routine: PHOTOS^MAGGTIG	Returns a list of patient photo IDs.
<b>MAGG SYS GLOBAL NODE</b> Routine: MAG^MAGGTSY2	Returns the global node of an IMAGE file (#2005) entry.
<b>MAGG WRKS UPDATES</b> Routine: UPD^MAGGTAU	Starts a new session for image access logging.

RPC Name	Description
<b>MAGGACTION LOG</b> Routine: LOGACT^MAGGTU6	Call to log an action performed on the image. Actions are logged in the IMAGE ACCESS LOG file (#2006.95).
<b>MAGGRPT</b> Routine: BRK^MAGGTRPT	Returns associated report for Image IEN.
<b>MAGGUSER2</b> Routine: USERINF2^MAGGTU3	Returns information about a Clinical Display user.

### 8.3.2. Non-MAG RPCs used by the CVIX

Table 17 shows the RPCs the CVIX uses 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.

**Table 17: Non-MAG RPCs used by the CVIX**

RPC Name	Description
<b>DDR FILER</b> Routine: FILEC^DDR3	Generic call to file edits into a FileMan file.
<b>DG SENSITIVE RECORD ACCESS</b> Routine: PTSEC^DGSEC4	Verifies that a user is not accessing his/her own Patient file record if the RESTRICT PATIENT RECORD ACCESS field (#1201) in the MAS PARAMETERS file (#43) is set to yes and the user does not hold the DG RECORD ACCESS security key. If the parameter is set to yes and the user is not a key holder, a social security number must be defined in the NEW PERSON file (#200) for the user to access any Patient file (#2) record.
<b>DG SENSITIVE RECORD BULLETIN</b> Routine: NOTICE^DGSEC4	Adds an entry to the DG Security Log file (#38.1) and generates the sensitive record access bulletin depending on the value in the ACTION input parameter.
<b>VAFCTFU CONVERT ICN TO DFN</b> Routine: GETDFN^VAFCTFU1	Given a patient ICN, this will return the patient's IEN from the PATIENT file (#2).
<b>VAFCTFU GET TREATING LIST</b> Routine: TFL^VAFCTFU1	Given a patient DFN, this will return a list of treating facilities.
<b>XUS AV CODE</b> Routine: VALIDAV^XUSRB	Checks to see whether an ACCESS/VERIFY code pair is valid.
<b>XUS DIVISION GET</b> Routine: DIVGET^XUSRB2	Returns a list of divisions of a user.

RPC Name	Description
<b>XUS DIVISION SET</b> Routine: DIVSET^XUSRB2	Sets the user's selected division in Designated User (DUZ) (2) during sign-on.
<b>XUS ESSO VALIDATE</b> Routine: ESSO^XUESSO4	Verifies that a provided IAM STS authentication token is valid.
<b>XUS SIGNON SETUP</b> Routine: SETUP^XUSRB	Establishes the environment necessary for DHCP sign-on.
<b>XWB CREATE CONTEXT</b> Routine: CRCONXT^XWBSEC	Establishes context on the server that the Broker will check before executing any other remote procedure.
<b>XUS SET VISITOR</b> Routine: SETVISIT^XUSBSE1	Returns a Broker Security Enhancement token to the CVIX.
<b>XWB GET VARIABLE VALUE</b> Routine: VARVAL^XWBLIB	Accepts the name of a variable that will be evaluated, and its value returned to the server.

### 8.3.3. Database Information

The CVIX retrieves data from VistA databases using the RPCs described in the previous sections.

The CVIX only writes data directly to remote VistA systems if the VA site does not have a VIX. At such non-VIX sites, the CVIX can make the following updates to the site's VistA system:

- It can update the IMAGE ACCESS LOG file (#2006.95) to indicate remote image access. See *Logging on Remote VistA Systems* for details.
- It can update a site's IMAGE file (#2005) with SOP instance UIDs for images that do not have SOP instance UIDs already. The CVIX uses the MAG NEW SOP INSTANCE UID RPC used by other Imaging components for the same purpose.

There are no general CVIX parameters stored on VistA; all parameters are set during installation and are stored in the CVIX's local configuration files.

### 8.3.4. Exported Menu Options

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

### 8.3.5. Security Keys

There are VistA security keys associated with the CVIX, see Sections 8.3.2, 11, and 12 for further details.

## 8.4. Other VIX Components

The CVIX incorporates the following additional components:

- Security certificates
- .NET
- Sun JRE
- Laurel Bridge DCF toolkit
- SQLite
- Aware JPEG2000 toolkit
- LibreOffice

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

### **8.4.1. CVIX Security Certificates**

When a CVIX communicates with another VIX, with a DoD or other system (HAIMS, DES, DAS, ECIA, and so on), they exchange security certificates for authentication purposes. The CVIX's long-term security certificates are stored in the \VixCertStore directory on each server where the CVIX is installed.

The CVIX security certificates are used in the CVIX installation process and must be available to complete a CVIX installation. VistA Imaging certificates are administered by the VistA Imaging development group. The other certificates needed by the CVIX to communicate with the DAS and HAIMS systems were provided by the teams administering each production system. Please refer to the separate CVIX Certificate\_Maintenance.docx document for procedures to replace CVIX or partner system security certificates.

### **8.4.2. .NET**

The .NET 4.8 framework is needed to install and update the CVIX software.

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

### **8.4.3. JRE**

The CVIX's servlet container and the CVIX itself requires Java Runtime Environment (JRE) version 8.0\_371.

### **8.4.4. Laurel Bridge DCF Toolkit**

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

The license for this toolkit is tied to the servers where the CVIX 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.

#### **8.4.5. SQLite**

The CVIX uses SQLite, a public domain database engine, to support the database for the CVIX cache. SQLite is a Structured Query Language (SQL) database that is completely self-managed. There are no site interactions required to maintain this database. The purpose of the database is to manage cached objects. The complete loss of this database is not a failure as it gets repopulated with each caching operation. The amount of data stored in the database and the cache is managed by the application based on available storage. No specific database errors are identified.

#### **8.4.6. Aware JPEG2000 Toolkit**

The Aware JPEG2000 toolkit is a third-party software development toolkit that the CVIX uses for image compression and decompression.

Use of this toolkit presumes that a one-time permanent license has been purchased from Aware. This license does not have to be explicitly installed and is transferable from one system to another.

This toolkit is bundled with the CVIX installer and is installed automatically as part of the VIX setup process. Do not install newer versions of the Aware JPEG2000 toolkit not bundled with the CVIX installer unless explicitly directed to do so by the Imaging development team.

#### **8.4.7. LibreOffice**

The CVIX requires the installation of LibreOffice 7.3.5, a third-party open-source office productivity software suite, to support Rich Text Format (RTF) files. The CVIX Installation automatically installs LibreOffice.

## 9. Operations and Maintenance Responsibilities/RACI

The responsibility matrix in Table 18 defines the roles and responsibilities for supporting VistA patches as part of a deployed solution. This is a template of the standard support structure required for VistA patches; therefore, the Project Manager (PM) should note any deviations in responsibility from this standardized Field Operations responsibility matrix in the Operational Acceptance Plan (OAP).

VistA Patching is generally relegated to the sustainment of existing solutions but may also include emergency “hot fix” patches designed to remediate a noted deficiency within the solution. This Responsibility Matrix (Responsible, Accountable, Consulted, Informed, or RACI) is related to VistA patches released and supported at the national level (known as “Class I” patches), which are distributed to the entire Enterprise after testing and release management has been completed. VistA Patches are released via the FORUM, KERNEL, or via Secure File Transfer Protocol (SFTP) directly to the Field.

Entities involved with VistA Patching:

**NSD** = OI&T National Service Desk

**FCIO** = Facility Chief Information Officer

**SL-ASL** = OI&T Service Lines Application Service Line

**SL-Core** = Core Systems Service Line

**PS** = OI&T Product Support

**VHA** = Local Facility medical staff (customer)

**FO** = Field Operations

**PD** = OI&T Product Developer

**DSO** = VHA Decision Support Office

**HPS** = Health Product Support

**Table 18: Types of Support with Production Environment Location(s) as Appropriate**

Support	Production Environments
Tier 1: NSD	N/A
Tier 2: (local OI&T – FCIO/SL-ASL)	PD
Tier 3: HPS	HPS

<b>Support</b>	<b>Production Environments</b>
Tier 4: PD/Maintenance FO VistA Patching Responsibility Matrix	PD, FCIO/SL-ASL
Application development	NSD, FCIO, SL, HPS,
Release Management	Vendor
Rollback Plan	N/A
Application installation	N/A
Application support	N/A
Client/Server Update (where applicable)	SL-Core
OS Patching (where applicable)	SL-Core
Change Management	SL-ASL
Application Administration (Operations and Maintenance)	SL-ASL
Local Training for Front Line Staff	VHA
National Training (where applicable)	DSO



## 10. Appendix A: Image Sharing and DICOM Images

Images are delivered to VA sites by the CVIX and originate from DAS framework for HAIMS or from ECIA.

### 10.1. 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.

However, for certain DICOM object types, the associated objects are not images, and Clinical Display and VistARad cannot display them. For these DICOM studies, metadata (including reports) is provided but not the image counts and/or image locations. The following DICOM modality types (Table 19) are blocked if the data originates from the DoD.

**Table 19: DICOM Modality Types Blocked at the VA if Originating from the DoD**

DICOM Modality Description	DICOM Identifier
Audio	AU
Document <i>(Used for DICOM encapsulated secondary captures and scanned documents. Not equivalent to MS Word .doc files )</i>	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

VistARad does not support displaying certain DICOM modalities. The data returned from ECIA is already filtered out with all the studies with those modalities. For a list of unsupported modalities, please refer to the *Configurations for DoD images Provided to VA Clinicians*.

JLV, Clinical Display, and VistARad do not support certain SOP classes. Each display has its own unsupported list. For a list of unsupported SOP classes for each display, please refer to the *Configurations for DoD images Provided to VA Clinicians*.

## 11. Appendix B: CVIX Tools

There are numerous tools the system administrator executes to monitor and manage the CVIX server. Table 20 lists the VIX Tools available.

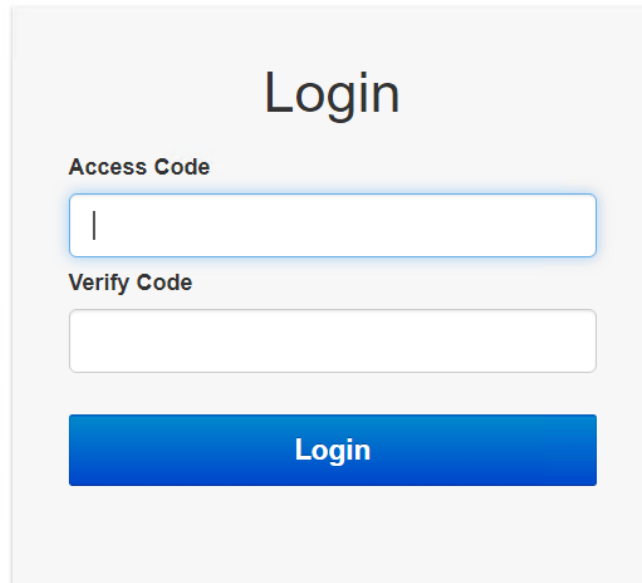
**NOTE:** In Table 20, please replace *FQDN* with your server's fully qualified domain name. For example: **REDACTED**/VixServerHealthWebApp/secure/MyVix.jsp

**Table 20: List of URLs**

URL	Description
<b>https://FQDN:REDACTED/Vix/ssl/JavaLogs.jsp</b>	Displays information for Java Logs: <ul style="list-style-type: none"><li>• Filename</li><li>• File Size</li><li>• Date Modified</li></ul>
<b>https://FQDN:REDACTED/VixCache</b>	To access the Cache Manager to manage metadata and images cached by the VIX.
<b>https://REDACTED/VIXDailyStatus/</b>	Shows statistics for all of the VIX sites.
<b>https://FQDN/VixServerHealthWebApp/secure/MyVix.jsp</b>	Displays information for the VIX: <ul style="list-style-type: none"><li>• Start Time</li><li>• Up Time</li><li>• Status</li><li>• Realm Configuration</li><li>• Tomcat Thread Details</li><li>• Transaction Log</li><li>• Site Service</li><li>• Release of Information (ROI)</li><li>• DICOM Services Transmit Failures</li></ul>
<b>https://FQDN&gt;:REDACTED/Vix/secure/VixLog.jsp</b>	To access the VIX transaction log while the VIX is running, which contains information about every image and metadata transfer handled by the VIX.
<b>https://FQDN:REDACTED/vix/viewer/dash</b>	To access a dashboard to access the VIX Image Viewer. The "Dash" is a tool for viewing medical artifacts (similar to the JLV) as well as providing more functionality, such as purging and viewing logs. For more information, see Appendix C: VIX Viewer Dashboard.

To access the tools, navigate to REDACTED/Vix/Viewer/Tools to be prompted to login (Figure 20) at the login page. To login you need a VistA account with the MAG ROI or MAG SYSTEM key. Once logged in, a tools page will appear.

**Figure 20: Login Page**

The image shows a login page with a light gray background. At the top center, the word "Login" is displayed in a large, black, sans-serif font. Below this, the text "Access Code" is positioned above a white input field with a blue border. The input field contains a single vertical line cursor. Below the "Access Code" field, the text "Verify Code" is positioned above another white input field with a gray border. At the bottom of the form, there is a solid blue rectangular button with the word "Login" written in white, centered text.

## 12. Appendix C: VIX Viewer Dashboard

MAG\*3.0\*177 introduced a dashboard to access the VIX Image Viewer without the need to run a consuming application. To utilize this functionality, the dashboard must be manually enabled through the VIX Viewer configuration. To enable the dashboard, 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.EnableDashboard" value="true" />
```

The resulting file looks 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="5" WorkerThreadPoolSize="5">
    <VixServices>
      <VixService ServiceType="Local" RootUrl="http://localhost:REDACTED" />
      <VixService ServiceType="SiteService" RootUrl="http://localhost:REDACTED" />
      <VixService ServiceType="Viewer" RootUrl="http://+:REDACTED" />
      <VixService ServiceType="Render" RootUrl="http://localhost:REDACTED" />
    </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.EnableDashboard" value="true" />
      <add name="Viewer.EnableESignatureVerification" value="true" />
    </Policies>
  </Vista>
</configuration>
```

Restart the VIX Viewer Service.

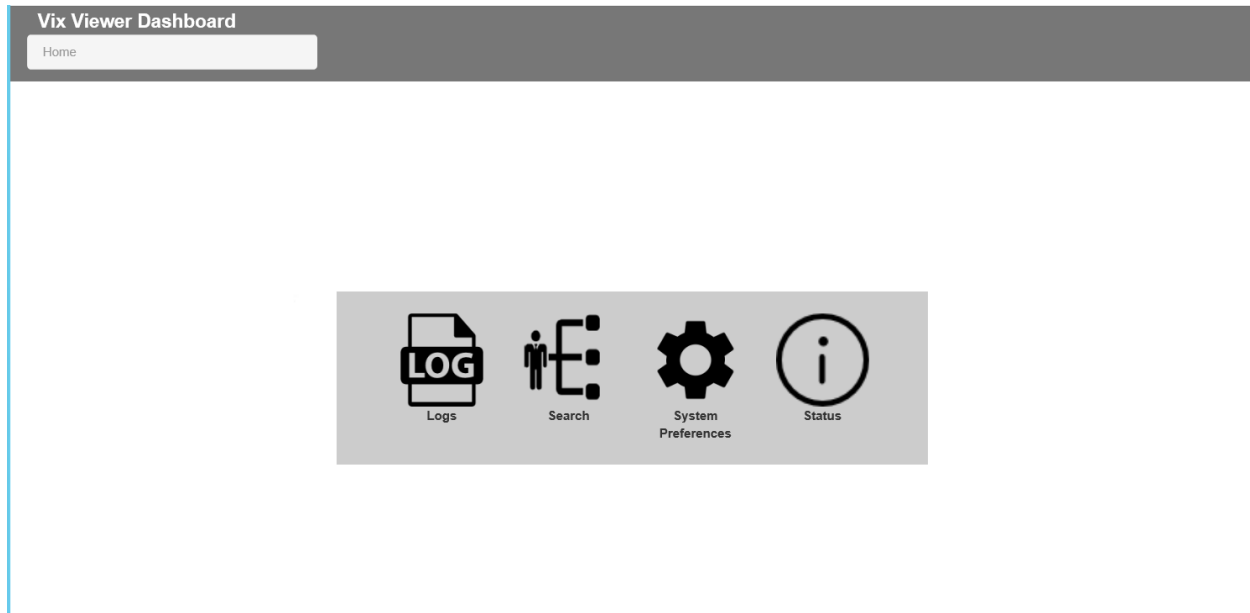
The default query information resides in the C:\Program Files\Vista\Imaging\Vix.Viewer.Service\TestData\Default.json file. It is not advised to change that file since the installer overwrites it.

To access the Dashboard, in a browser navigate to REDACTED/vix/viewer/tools to be prompted to login (Figure 20) at the login page. You need a Vista account with the MAG ROI or MAG SYSTEM key. Once logged in, the tools page appears, and click the VIX Viewer Dashboard's **Open** button to display REDACTED/vix/viewer/dash.

## 12.1. VIX Viewer Dashboard: Homepage

The VIX Viewer Dashboard homepage (Figure 21) contains the following four options: Logs, Search, System Preferences, and Status.

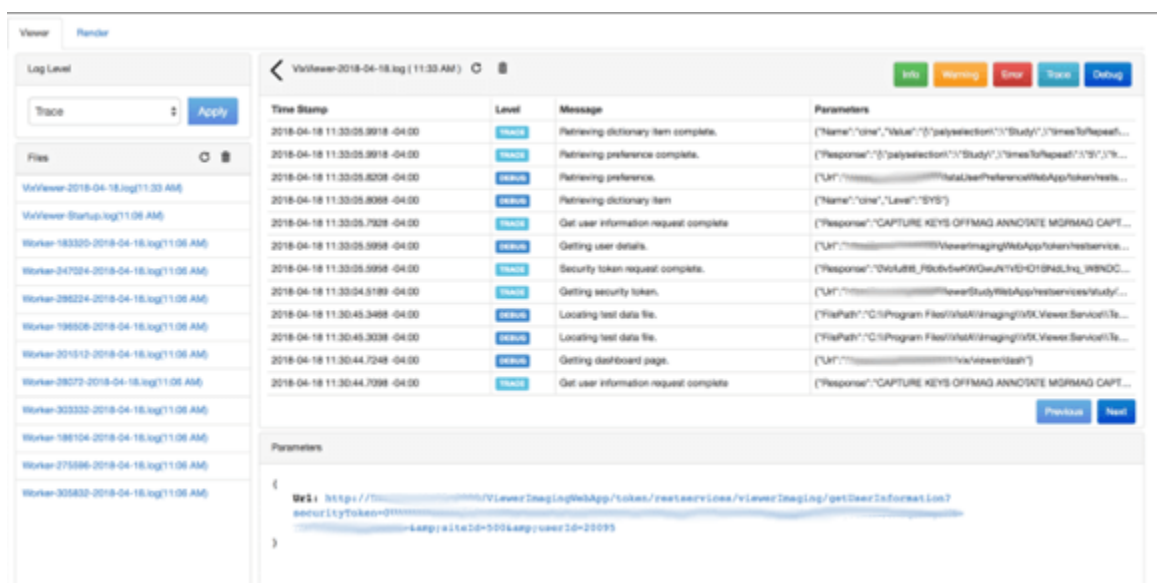
**Figure 21: VIX Viewer Dashboard: Homepage**



## 12.2. VIX Viewer Dashboard: Logs

The VIX Viewer Dashboard Logs option presents the logs (Figure 22).

**Figure 22: VIX Viewer Dashboard: Logs**



## 12.3. VIX Viewer Dashboard: Search

The VIX Viewer Dashboard search option (Figure 23) allows the user to edit the fields for both the body and the headers and submit them to query (search) for a patient's study list. The resulting page provides access to each study. The VIX Viewer Web API documentation describes the values for the body and headers. Access the API documentation by entering **REDACTED**/vix/viewer/VVSDoc in your browser's address bar.

Figure 23: VIX Viewer Dashboard: Search

The screenshot shows the 'VIX Viewer Dashboard' interface. At the top, there is a navigation bar with 'Home / Search' and icons for document, settings, and help. Below this is a 'Study Query' section with a text input field containing 'Patient 21 study query (JLV, excluding DAS/DES/HAIMS)'. To the right of the input field are 'Apply' and 'Send' buttons. Below the input field are two tabs: 'Body' (selected) and 'Headers'. The 'Body' tab displays a JSON object: 

```
{
  "imageFilter": "PAT,ENC",
  "patientICN": "REDACTED",
  "siteNumber": "500"
}
```

Selecting the View option opens the VIX Viewer. The Manage button opens the manage page, and the details show the study level return views. Report opens the text report.

## 12.4. VIX Viewer Dashboard: System Preferences

The VIX Viewer Dashboard System Preferences option allows for various preferences to be set.

## 12.4.1. Annotation Preferences

Click **Annotation** to display annotation preferences (Figure 24).

**Figure 24: Annotation Preferences: Annotation**

The screenshot shows a web browser window titled "HTML5 Viewer" with a URL bar showing "https://.../vix/viewer/dash#". The browser's address bar also shows "67%". The page content is titled "Vix Viewer Dashboard" and includes a navigation bar with "Home" and "System Preferences". The "System Preferences" section is active, and the "Annotation" tab is selected. The "Annotation Preferences" dialog box is open, showing the following settings:

- ANNOTATION** (header)
- Line Width**: 1 (dropdown)
- Color**: Cyan (color picker)
- Arrow** (header)
- Fill Color**: Cyan (color picker)
- Fill**: ☒ (checkbox)
- MEASUREMENT** (header)
- ELLIPSE & RECTANGLE** (header)
- LABEL** (header)
- TEXT** (header)
- MITRAL & AORTIC (uS)** (header)

At the bottom right of the dialog box, there are "Apply" and "Reset" buttons.

Click **Measurement** to display annotation measurement preferences (Figure 25).

**Figure 25: Annotation Preferences: Measurement**

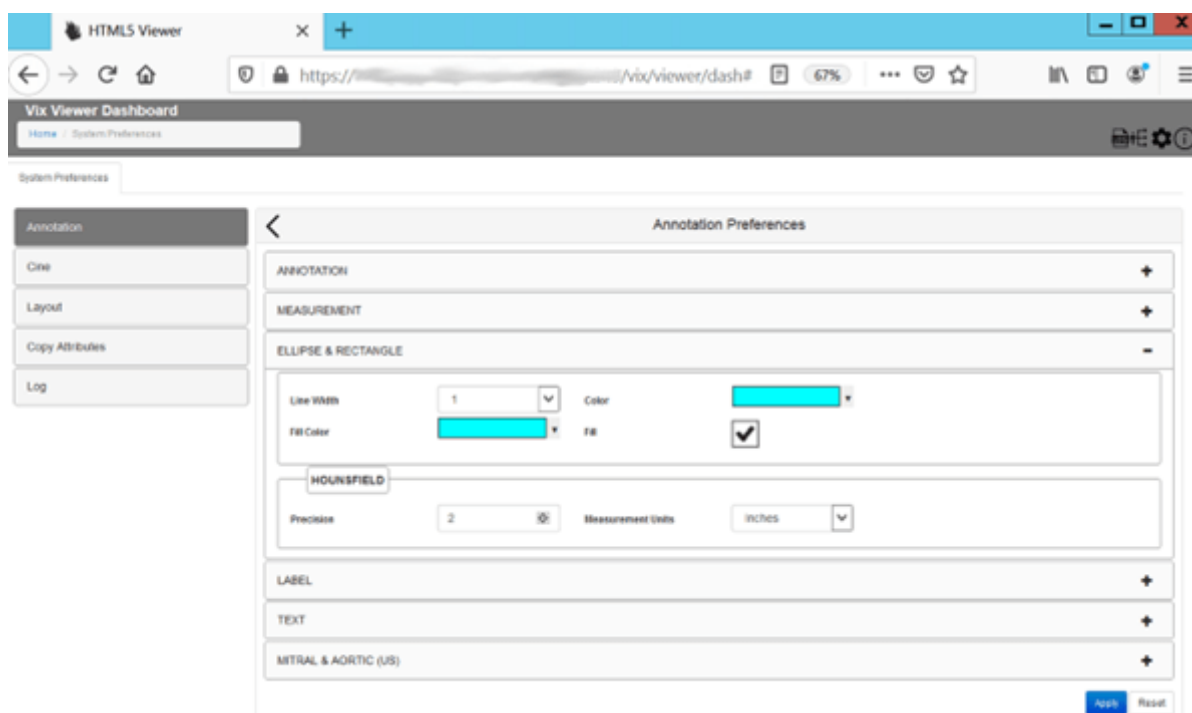
The screenshot shows a web browser window titled "HTML5 Viewer" displaying the "Vix Viewer Dashboard". The dashboard has a sidebar with "System Preferences" selected. The main content area is titled "Annotation Preferences" and contains several expandable sections. The "MEASUREMENT" section is expanded, showing settings for Line Width (1), Precision (2), Color (Cyan), Measurement Units (Centimeter), Gauge Style (Line), Gauge Length (7), and Angle (20). The "ELLIPSE & RECTANGLE", "LABEL", "TEXT", and "MITRAL & AORTIC (US)" sections are collapsed. At the bottom right of the "MEASUREMENT" section are "Apply" and "Reset" buttons.

ANNOTATION	
MEASUREMENT	
Line Width	1
Precision	2
Color	Cyan
Measurement Units	Centimeter
Length	
Gauge Style	Line
Gauge Length	7
Angle	
Arc Radius	20
ELLIPSE & RECTANGLE	
LABEL	
TEXT	
MITRAL & AORTIC (US)	



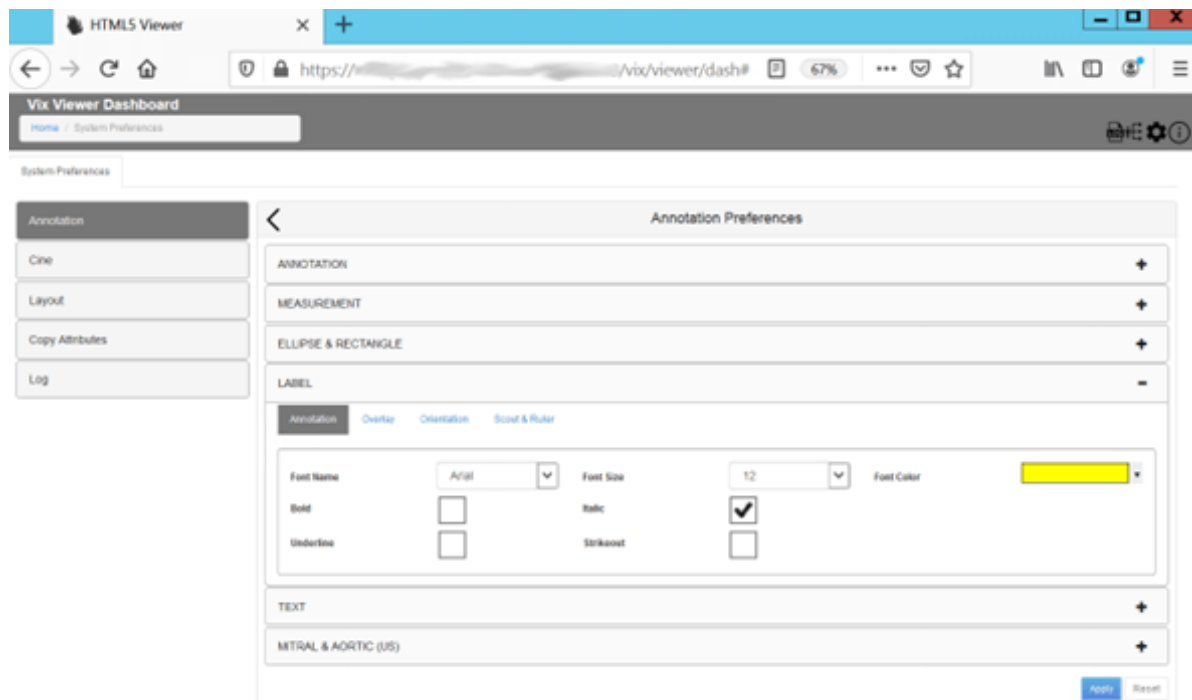
Click **Ellipse** and **Rectangle** to display annotation ellipse and rectangle preferences (Figure 26).

**Figure 26: Annotation Preferences: Eclipse and Rectangle**



Click **Label** to display label annotation preferences (Figure 27).

**Figure 27: Annotation Preferences: Label**



Under the **Label** preferences, toggle between **Annotation**, **Overlay**, **Orientation**, and **Scout & Ruler** to set all **Label** preferences. Click **Text** to display annotation text preferences (Figure 28).

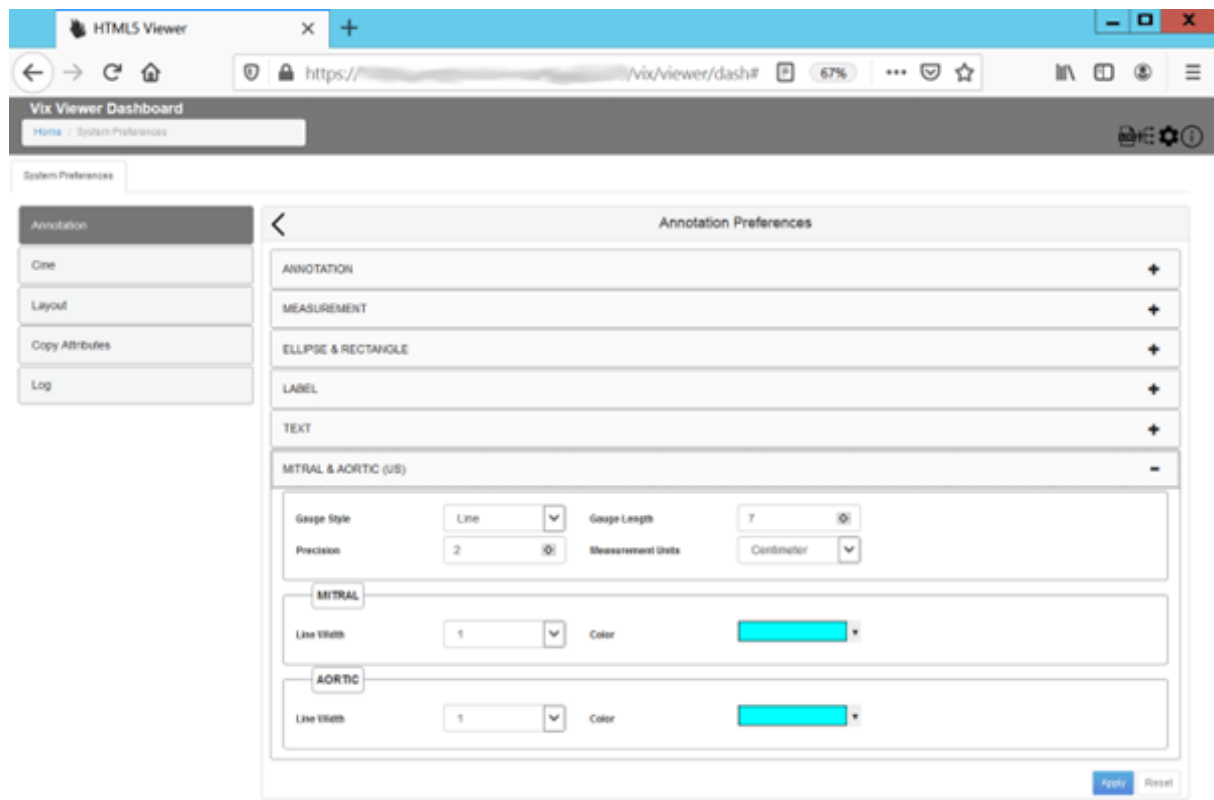
**Figure 28: Annotation Preferences: Text**

The screenshot shows a web browser window titled "HTML5 Viewer" displaying the "Vix Viewer Dashboard". The dashboard has a sidebar with "System Preferences" and a main content area. The "Annotation Preferences" dialog box is open, showing a list of categories: ANNOTATION, MEASUREMENT, ELLIPSE & RECTANGLE, LABEL, and TEXT. The "TEXT" category is selected, and its settings are displayed. The settings include Font Name (Arial), Font Size (12), Font Color (yellow), Fill (checkbox), Fill Color (cyan), Bold (checkbox), Italic (checkbox), Underline (checkbox), and Strikethrough (checkbox). At the bottom of the dialog, there is a "MITRAL & AORTIC (US)" category and "Apply" and "Reset" buttons.

Annotation Preferences			
ANNOTATION			
MEASUREMENT			
ELLIPSE & RECTANGLE			
LABEL			
TEXT			
Font Name	Arial	Font Size	12
Font Color	Yellow	Fill	<input type="checkbox"/>
Fill Color	Cyan	Bold	<input type="checkbox"/>
Italic	<input type="checkbox"/>	Underline	<input type="checkbox"/>
Strikethrough	<input type="checkbox"/>		
MITRAL & AORTIC (US)			

Click **Mitral** and **Aortic** to display annotation mitral and aortic preferences (Figure 29).

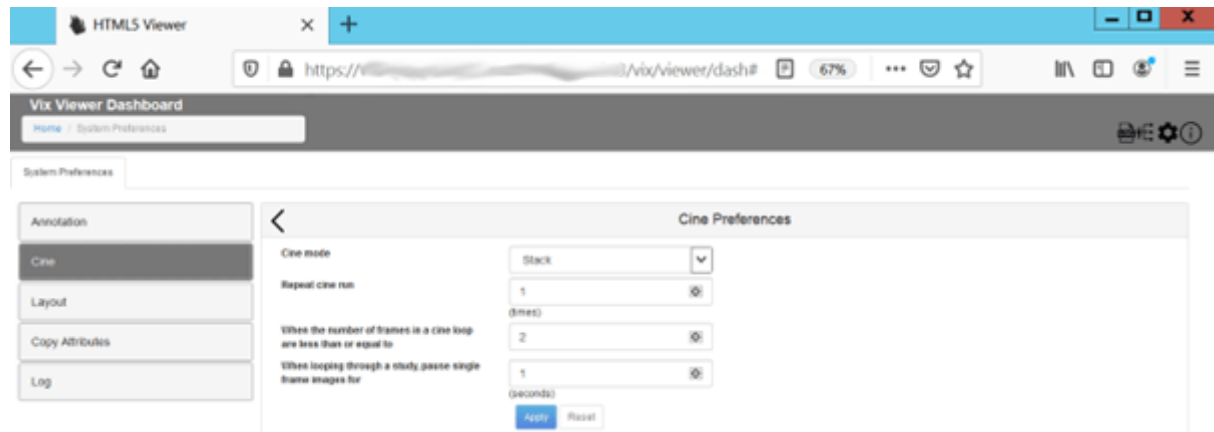
Figure 29: Annotation Preferences: Mitral and Aortic



### 12.4.2. Cine Preferences

To view or update **Cine** preferences, select the **Cine Preferences** (Figure 30).

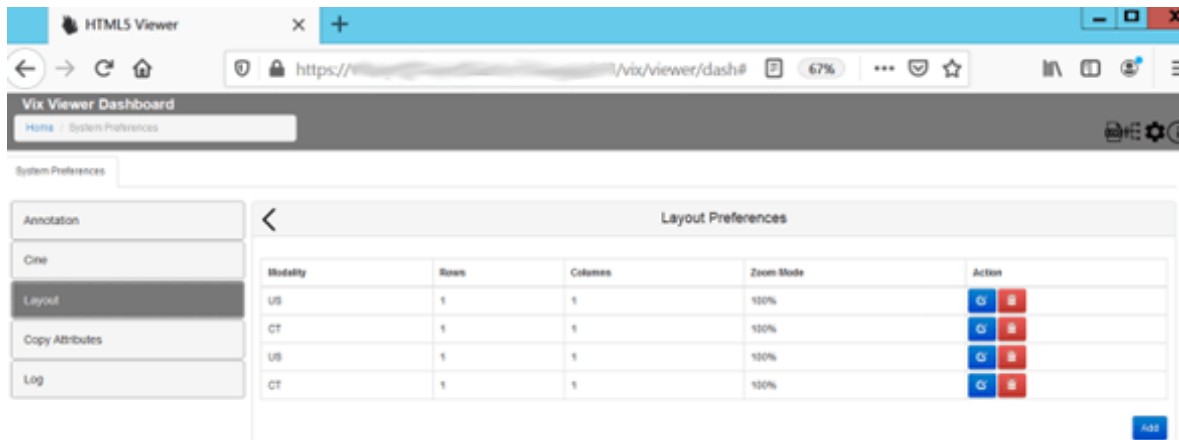
Figure 30: Cine Preferences



### 12.4.3. Layout Preferences

To view the **Layout** settings, select the **Layout Preference** (Figure 31).

Figure 31: Layout Preferences

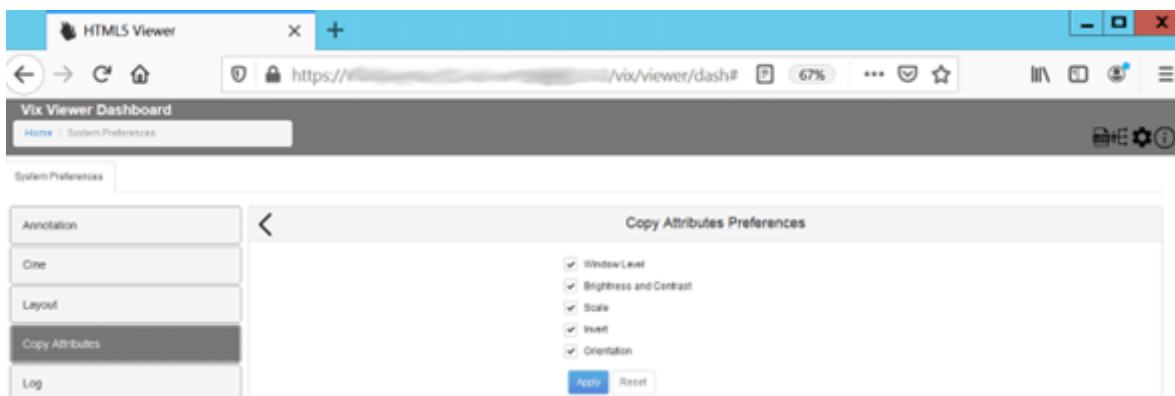


Click **Add** in the bottom right of the window to add a new layout preference.

### 12.4.4. Copy Attributes

To view the **Copy Attributes** settings, select the **Copy Attributes Preferences** (Figure 32).

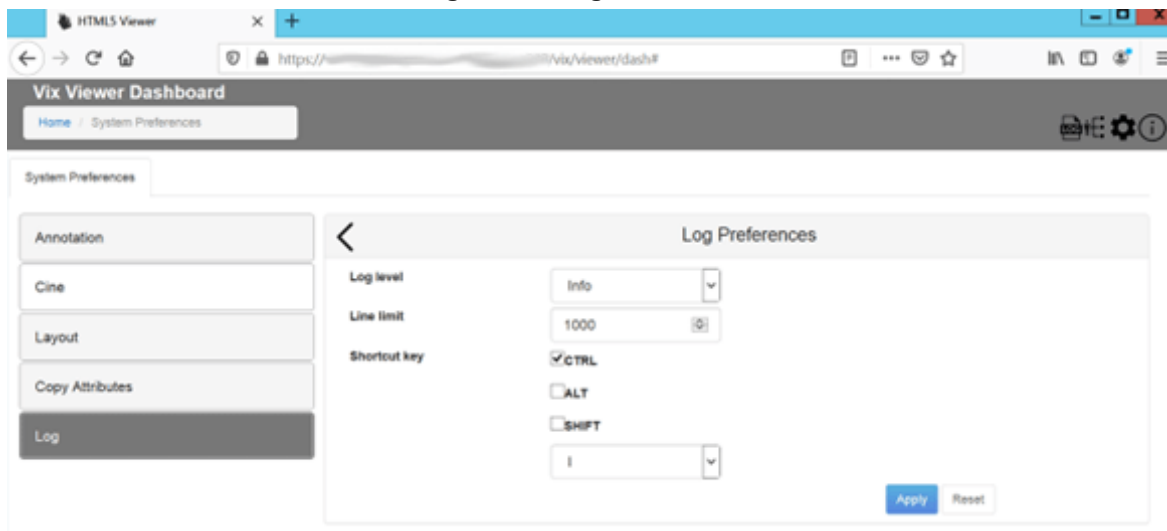
Figure 32: Copy Attributes Preferences



## 12.4.5. Log Preferences

Click **Log** to view the log preferences (Figure 33).

Figure 33: Log Preferences



Use the Log Level drop-down to set the log level for both Viewer and Render services. Setting the line limit for the log viewer sets the number of lines in the Line Limit field.

## 12.5. VIX Viewer Dashboard: Status

The VIX Viewer Dashboard Status option shows some configuration keys and values (Figure 34).

Figure 34: VIX Viewer Dashboard: Status

The screenshot shows the Vix Viewer Dashboard with the 'Status' option selected in the left sidebar. The 'Status' panel displays a table of configuration keys and values.

Key	Value
RootUrl	https://...
PublicHostName	...
TrustedClientRootUrl	https://...
LocalVixUrl	http://localhost...

## 13. Definitions, Acronyms, and Abbreviations

**Table 21: Definitions, Acronyms, and Abbreviations**

Term	Definition
AE	Application Entities
BSE	Broker Security Exchange
COOP	Continuity of Operations
CSV	Comma-Separated Values
CVIX	Centralized VistA Imaging Exchange
DAS	Data Access Service
DCF	DICOM Connectivity Framework
DES	Data Exchange Service
DMIX	Defense Medical Information Exchange
DoD	Department of Defense
DUZ	Designated User
ECIA	Enterprise Clinical Imaging Archive
EDIPI	Electronic Data Interchange Personal Identifier
FDA	Food and Drug Administration
GUID	Globally Unique Identifier
HAIMS	Health Artifact and Image Management Solution
ICN	Integration Control Number
ICR	Integration Control Registration
IEN	Internal Entry Number
JLV	Joint Legacy View
JRE	Java Runtime Environment
MVI	Master Veteran Index
OAP	Operational Acceptance Plan
PM	Program Manager
RACI	Responsible, Accountable, Consulted and Informed
ROI	Release of Information
RPC	Remote Procedure Call
RTF	Rich Text Format
SCP	Service Class Provider
SCU	Service Class User

<b>Term</b>	<b>Definition</b>
SFTP	Secure File Transfer Protocol
SOP	Service-Object Pair
SQL	Structure Query Language
TIU	Text Integration Utility
TSV	Tab-Separated Values
URN	Universal Resource Name
VAEC	Veteran Affairs Enterprise Cloud
VISN	Veterans Integrated Service Network
VIX	VistA Imaging Exchange
WAN	Wide Access Network