



## **VistA Imaging System**

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

August 2013 – Version 3  
MAG\*3.0\*34/116/118, MAG\*3.0\*119, MAG\*3.0\*127,  
MAG\*3.0\*129

Department of Veterans Affairs  
Product Development  
Health Provider Systems

**CVIX Administrator's Guide and Product Operations Manual**  
**VistA Imaging 3.0, MAG\*3.0\*34/116/118, 119, 127, 129**  
**August 2013**

**Property of the US Government**

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

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

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

VistA Imaging Product Development  
Department of Veterans Affairs

Internet: [REDACTED](#)  
VA intranet: [REDACTED](#)

**Revision History**

Date	Version	Notes
March 2013	1	Document created for Imaging patch MAG*3.0*124. C. Becky. Expanded CVIX Transition Log section with step-by-step instructions. <a href="#">REDACTED</a>
July 2013	2	Revised for MAG*3.0*124. Revised sections Using the Cache Browser and Cache Delete. <a href="#">REDACTED</a> .
August 2013	3	Revised for MAG*3.0*34/116/118, 119, 127, 129. Revised sections Using the Cache Browser and Cache Delete. <a href="#">REDACTED</a>

# Contents

---

<b>Introduction</b> .....	<b>1</b>
Intended Audience.....	1
Terms of Use .....	1
Document Conventions .....	1
Related Information .....	2
<b>CVIX Overview</b> .....	<b>3</b>
CVIX Major Functions.....	3
Provide DoD Images to VA Clinicians .....	3
Provide VA images to DoD requestors .....	5
Provide VA images to AWIV .....	6
Host the VistA Site Service.....	6
CVIX Physical and Logical Description .....	7
CVIX Operational Priority .....	8
CVIX Dependencies .....	9
The CVIX, VIXes, and Multidivisional VA Sites .....	10
CVIX Connection Security .....	11
<b>CVIX General Operations</b> .....	<b>13</b>
CVIX Monitoring .....	14
Using the CVIX Transaction Log .....	14
CVIX Transaction Log Fields .....	16
CVIX Transaction Log Fields (Export Only).....	19
Logging on Remote VistA Systems .....	20
Using the Cache Manager .....	20
Cache Organization .....	21
Cache Item Information .....	26
Cache Delete .....	26
User Notifications .....	27
Cluster-related Activities .....	27
CVIX cluster: take node offline .....	27
CVIX cluster: bring node online .....	28
Log Collector cluster: transfer cluster group and resources .....	29
Checking which load balancer is active .....	31
CVIX Planned Startup and Shutdown .....	31
Planned Full CVIX Shutdown .....	31
Planned Full CVIX Startup.....	33
CVIX Data Retention and Purges.....	35
CVIX and Backups .....	35
CVIX and User Management.....	35
<b>VistA Site Service</b> .....	<b>37</b>
VistA Site Service Overview .....	37
Checking the Site Service .....	37
Updating Site Service Data .....	37
<b>CVIX Image Sharing</b> .....	<b>39</b>
Remote Metadata Retrieval.....	39
Remote Image Retrieval.....	40

Caching of Metadata and Images .....	42
Cache Retention Periods .....	42
Cache Location and Structure .....	42
Image Sharing and CVIX Timeouts .....	43
<b>VIX Log Collector Service .....</b>	<b>45</b>
VIX Log Collector Overview.....	45
Log Collector Automatic Emails.....	45
Archived Transaction Log Storage Area .....	46
Excluding a VIX from Log Collection .....	47
<b>CVIX Troubleshooting .....</b>	<b>49</b>
Routine Errors.....	49
Connectivity .....	49
Timeouts .....	49
Security .....	49
Station 200 Issues .....	49
Significant Errors .....	50
Error Logs .....	50
Unplanned Shutdowns .....	50
Recovering after unplanned restart of a single CVIX server .....	50
Recovering after unplanned reboot of a single load balancer .....	50
Recovering after an unscheduled power loss to all components .....	50
CVIX Support.....	50
<b>CVIX Reference/Software Description.....</b>	<b>53</b>
CVIX Java Components .....	53
CVIX Servlet Container.....	53
CVIX Security Realms .....	53
CVIX Interfaces.....	53
CVIX Core.....	54
CVIX Data Sources.....	54
Java Installation Locations.....	54
Java Logs.....	56
VistA/M Information .....	56
RPCs used by the CVIX.....	56
Database Information .....	59
Exported Menu Options .....	59
Security Keys.....	59
Other VIX Components .....	59
CVIX Security Certificates .....	59
.NET .....	60
Sun JRE.....	60
Laurel Bridge DCF Toolkit .....	60
Aware JPEG2000 Toolkit.....	60
<b>Index.....</b>	<b>61</b>

# 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 Philadelphia SunGard Spring Garden data center. The CVIX facilitates data sharing and exchange across organizational and functional boundaries.

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

## Intended Audience

This document is intended for the VA data center personnel who are 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.

## 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 the installation of unapproved software, will adulterate the medical device. The use of an adulterated medical device violates US federal law (21CFR820).

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

## Document Conventions

This document uses the following 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**.

## 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\*124 AWIV Independent of VistA Web Patch Description* available at [REDACTED](#).
- *VIX Installation Guide*, available at [REDACTED](#)
- *VIX Administrator's Guide*, available at [REDACTED](#).

**Note:** This manual serves as both a Product Operations Manual (POM) and as a System Administrator's Guide. If it is determined that they are needed, Memorandum of Understanding (MOU), Service Level Agreement (SLA), Service Level Requirements (SLR), Operational Level Agreement (OLA), and Operations and Maintenance (O&M) documents may be developed at a future date.

# CVIX Overview

---

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

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

## CVIX Major Functions

The CVIX's major functions are:

- Provide Department of Defense (DoD) images to VA clinicians.
- Provide VA images to DoD clinicians.
- Provide VA images to users of VistAWeb and the Advanced Web Image Viewer (AWIV)
- Host the VistA Site Service, the repository of connection information used by various Imaging components.
- Host the VIX log collector.

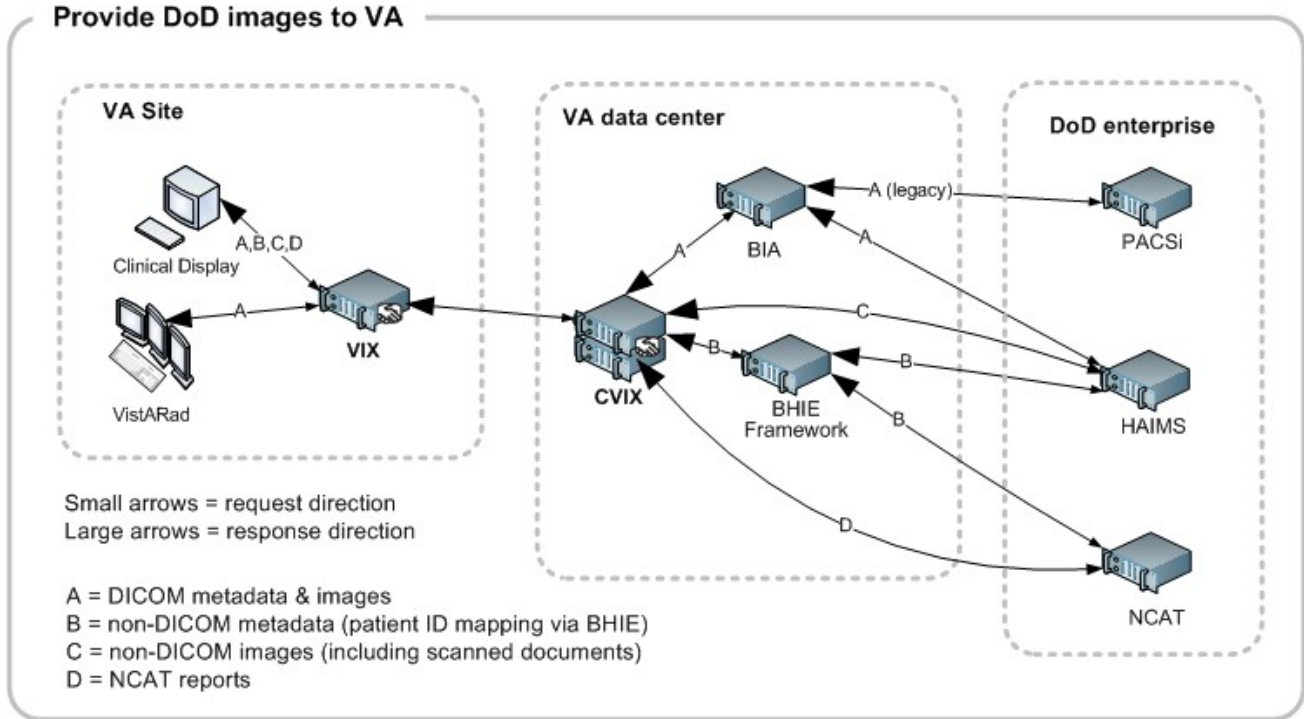
Each of these functions is described in the following sections.

**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 page 45.

### Provide DoD Images to VA Clinicians

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

The flow of DoD images through a CVIX is illustrated in the following diagram. Note that this complexity is not evident to the VA clinicians; they simply use Clinical Display or VistARad to select the desired images.



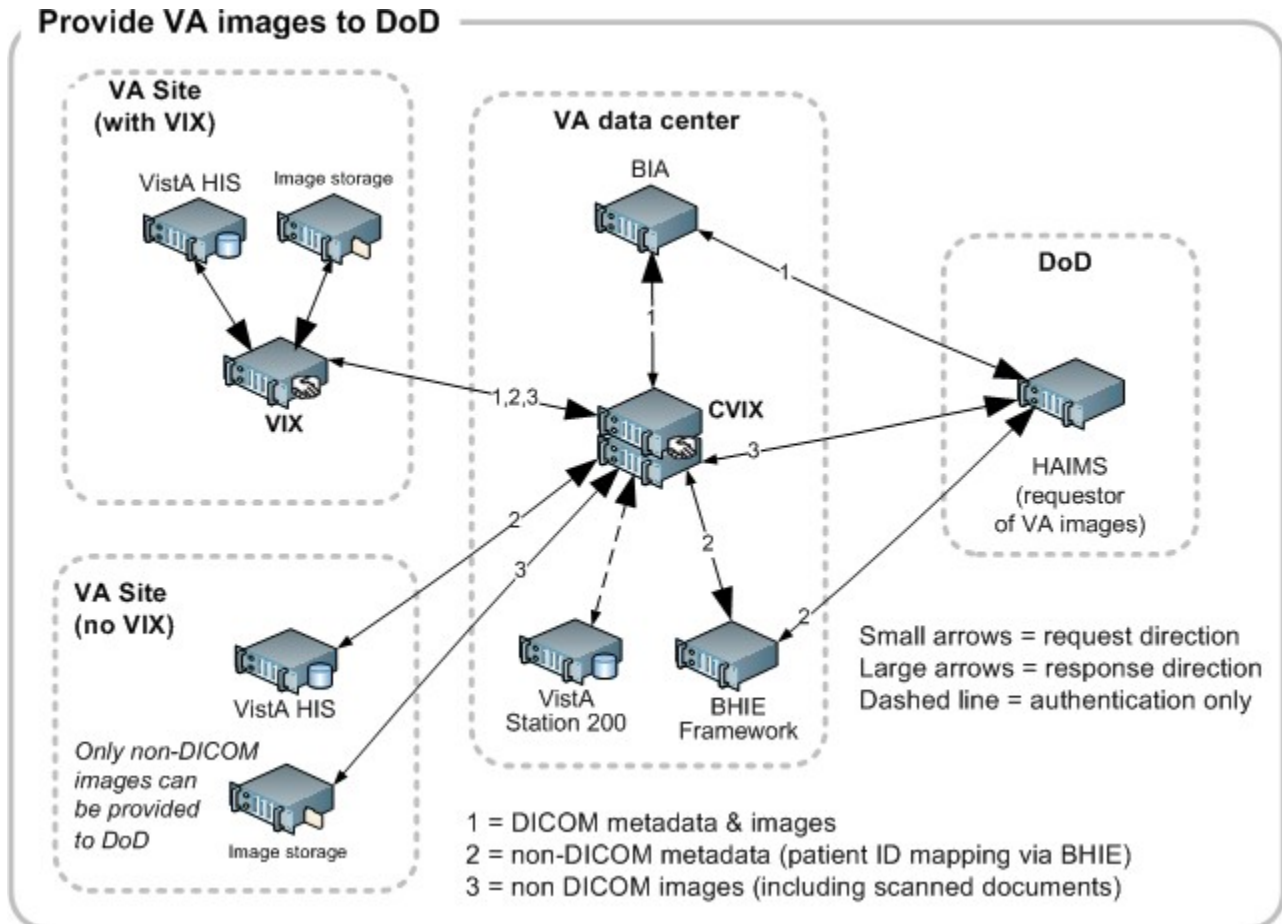
The following table details the types of DoD images that can be retrieved and where they originate from.

DoD Image category	DoD source	Viewable in VA VistA using
DoD DICOM (radiology) images	Available from participating DoD facilities via the BHIE Image Adapter (BIA). For a list of DoD participating facilities and information about the types of DICOM objects that can be retrieved, see the <i>VIX Administrator's Guide</i> .	Clinical Display and VistARad
DoD NCAT (Neurocognitive Assessment Tool) reports	Available if the NCAT server is online and if it is capable of communicating with the CVIX. Metadata for these images is provided by the Bi-directional Healthcare Information Exchange (BHIE) and the images come from the NCAT server.	Clinical Display
DoD artifacts (non-radiology medical images, scanned documents, etc.)	Available if HAIMS (Health Artifact and Image Management Solution) servers are online and if HAIMS servers are capable of communicating with the CVIX. Metadata for these images is provided by BHIE and the actual images come from the NCAT server (if the NCAT server is online).	Clinical Display



### 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 DoD images through a CVIX is illustrated in the following diagram.



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

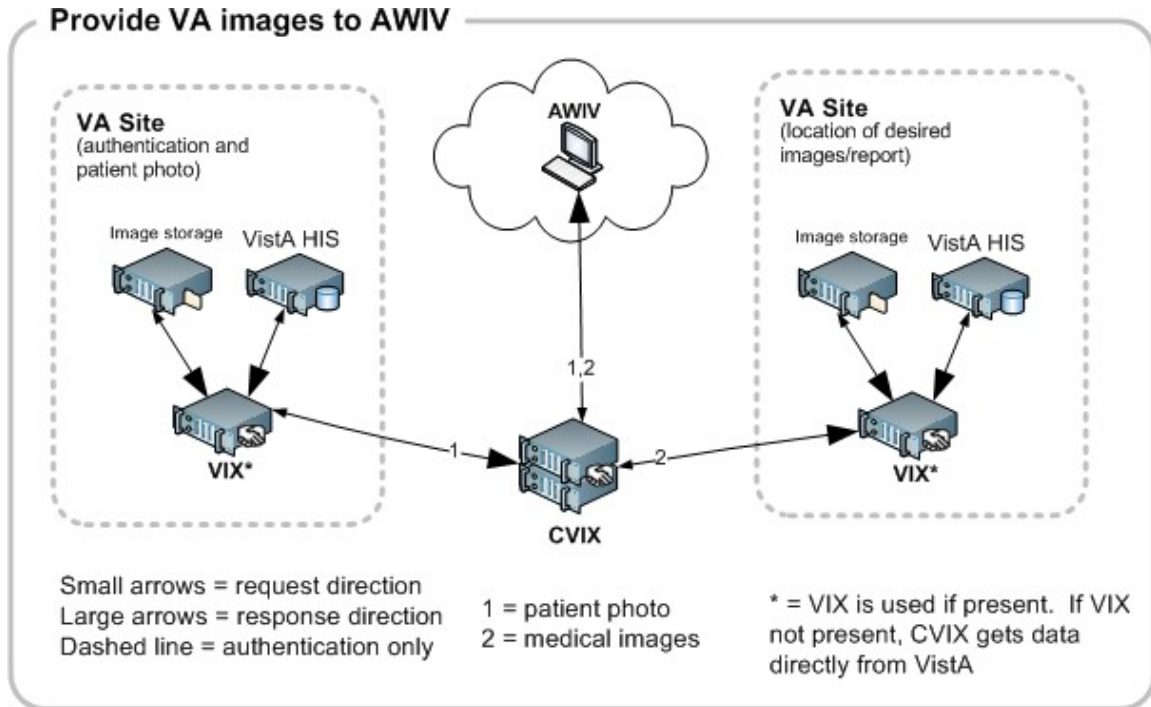
**Note:** MUSE EKG waveforms, commercial Picture Archive and Communication System (PACS) images, and other images not stored in VistA Imaging at a VA site cannot be accessed by DoD clinicians.

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:** 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*.

### Provide VA images to AWIV

The CVIX serves as the image access portal for the Advanced Web VistA Imaging Viewer (AWIV). The AWIV is a browser-based application used to access VA medical images, primarily for non-clinical purposes. The flow of data between the AWIV and the CVIX is illustrated below.



AWIV users can access any image or report associated with a VA Progress Note or a VA Radiology package report via the CVIX. The CVIX handles all connections with VA sites, insulating the AWIV from connection information changes.

**Note:** MUSE EKG waveforms, commercial PACS images, and other images not stored in VistA Imaging at a VA site cannot be accessed by AWIV users.

The AWIV itself is described in the *VistA Imaging AWIV User Guide*.

**Note:** The AWIV is hosted in a separate application (VistAWeb) that handles user authentication, patient selection, and progress note/report selection. VistAWeb does not communicate with the CVIX. For information about VistAWeb, see <http://www.va.gov/vdl/application.asp?appid=147>.

### 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. It is also used by the CVIX itself. The VistA Site Service is described in detail on page 37.

## CVIX Physical and Logical Description

The CVIX is located in the VA Annex of the Philadelphia SunGard Spring Garden data center. The CVIX is made up of:

- Two Unix-based Coyote Point E450GX load balancer appliances.

The primary (active) load balancer defines the Layer 4 load balanced CVIX cluster. Content removed: FOIA There is no server affinity associated with this cluster.

- Six DL360G6 servers, 8 GB RAM per server, each running Windows 2008 x64. These serve as the nodes in the CVIX virtual cluster.

These nodes host the CVIX service, CVIX metadata and image caches, local CVIX logs, and the VistA Site Service.

- Two DL360G6 servers, 4 GB RAM per server, each running Windows 2008 x64.

These serve as the CVIX failover cluster, and also host the Log Collector Service.

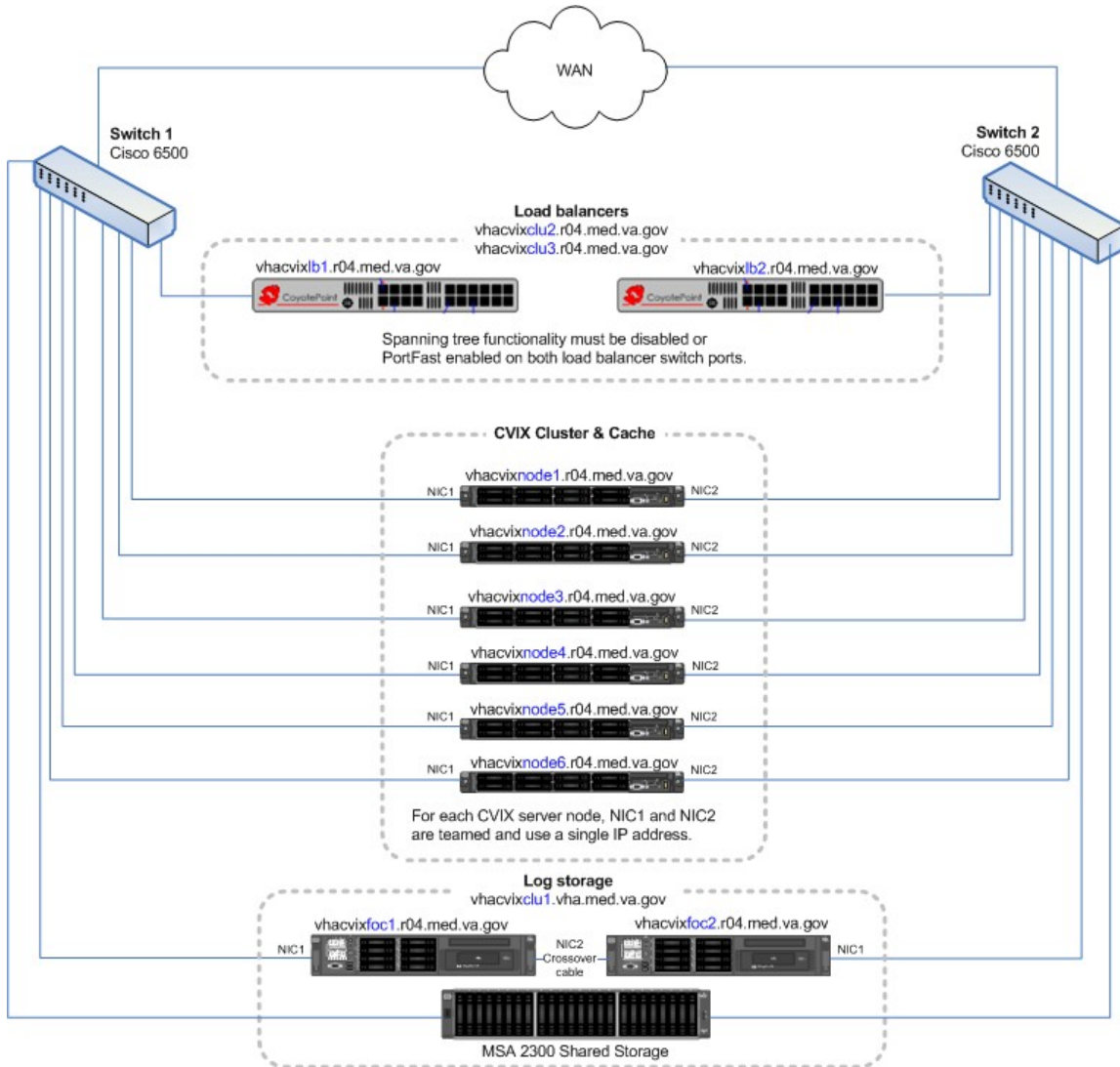
- One HP Modular Smart Array storage system with approximately one 1 TB capacity.

This is used to store copies of VIX transaction logs gathered by the Log Collector Service

- One 42U rack to provide housing for the components above.

The following diagram shows the physical components (except for the rack) and the connections between them. All connections indicated in the diagram below are gigabit Ethernet. Per VA policy regarding medical devices, the CVIX is in its own VLAN.

**Note:** The existing CVIX hardware is actively monitored to ensure that adequate capacity is available. More detailed capacity planning is on hold until after a usage history has been established.



## CVIX Operational Priority

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

CVIX Function	Priority	Notes
Host site service	medium-to-high	<p>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 specific site if they know which site the images are at.)</p> <p>The AWIV (see next row) and the TeleReader will not function properly until their access to the site service is restored.</p>

CVIX Function	Priority	Notes
Provide VA image access to AWIV users	medium	If the CVIX is not available to support the AWIV, images cannot be retrieved via the AWIV. The AWIV's hosting application (VistAWeb) can still be used to retrieve text-based data.
VA/DoD	See notes	Priority is dependent on specific clinical use. The CVIX provides access to remote data that may be relevant or highly valuable for patient care; however criticality is dependent on the specific use and data involved. As of the release of MAG*3.0*104, usage of VA/DoD image sharing is low. Usage is expected to increase as more DoD systems come online.

**Note:** A Continuity of Operations (COOP) site for the CVIX is in the planning stages. A disaster recovery plan will be put in place after the COOP site is established.

## CVIX Dependencies

The following systems 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.

System	Function	Interface method	CVIX behavior if "System" is not available
Local VistA (Station 200)	Provides CVIX with 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 will not be able to access VA images for VA/DoD shared patients. Other CVIX functions are unaffected.
Site VIXes	Provide metadata and images to the CVIX.	WAN/HTTP	AWIV users will be able to access all standard images, but performance may be reduced. DoD clinicians will not be able to access radiology images via CVIX, but non-radiology images will still be available.
Remote VistA	Source of remotely stored VA images for DoD clinician or AWIV access.	WAN/RPC	The CVIX cannot provide images from that site.
BIA	Source of DoD DICOM images for VA clinician access.	WAN/HTTP	The CVIX cannot provide DoD DICOM images to the VA.

System	Function	Interface method	CVIX behavior if “System” is not available
BHIE	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.
NCAT	Source of NCAT reports.	WAN/HTTP	The CVIX cannot provide NCAT reports to the VA.

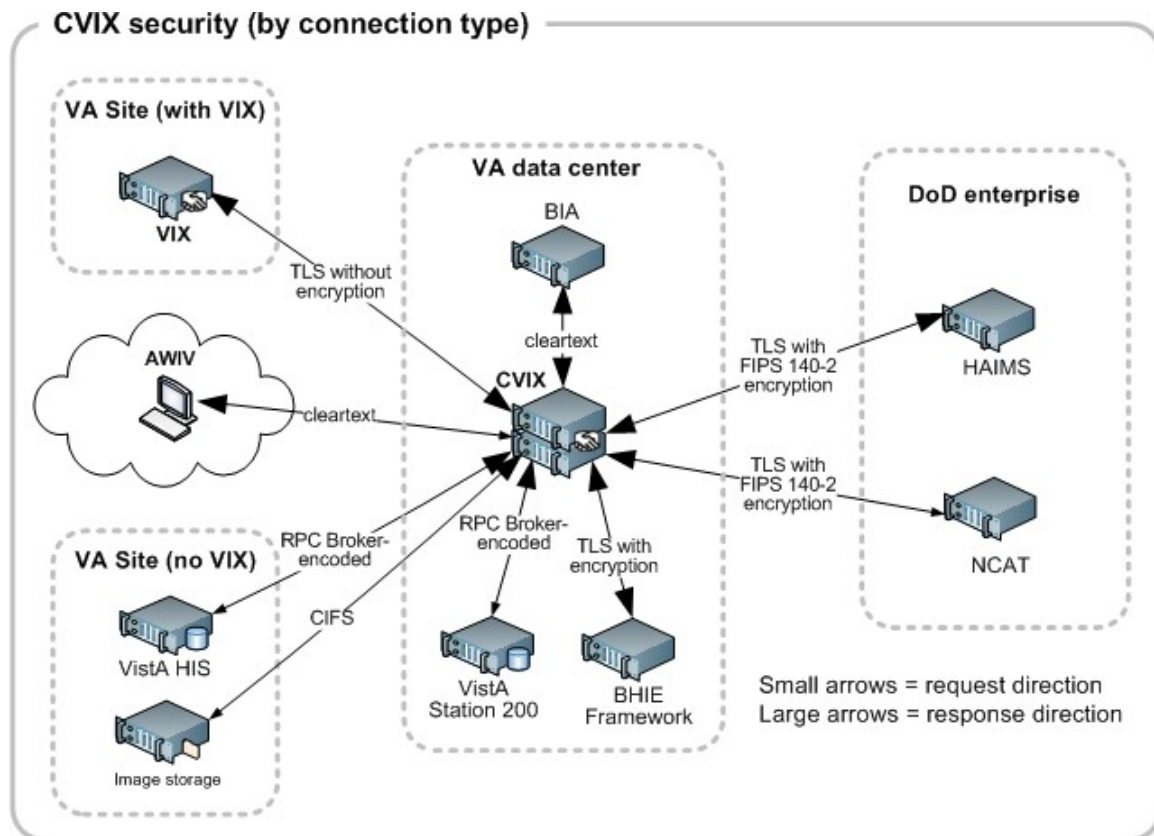
## The CVIX, VIXes, and Multidivisional VA Sites

When a CVIX requests images and metadata from a VA multidivisional site, the path the data takes depends how many VIXes are present at that site, as detailed below

# of VIXes	Data retrieval path
2 or more	<p>The CVIX gets metadata from the VIX at the primary division.</p> <p>If a subdivision has local image storage and a VIX, the CVIX requests the image from that VIX.</p> <p>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.</p>
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>

## CVIX Connection Security

The following diagram shows the security mechanisms used by the CVIX.



### Notes:

- 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 RPC brokers, the CVIX supports both Broker Security Enhancement (BSE) and pre-BSE-style remote logins. The CVIX will use BSE remote logins if BSE is enabled on the remote system.
- CVIX-to-VIX communications require a valid security certificate.

This page is intentionally left blank.



# CVIX General Operations

---

This chapter covers:

- CVIX Monitoring
- Using the CVIX Transaction Log

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. 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 obviously corrupt data, then the item should be located in all of the cache instances and deleted.

To delete a cache item, collect as much identification information as you can. 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, patient identifier (Integrated Control Number [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 you want the item deleted. The cache does not immediately delete the item since it has to synchronize operations from all clients. It may take a few seconds or up to a minute before the item is actually deleted. Usually, 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 the 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 of the “bad” ones. This is not an issue, since the CVIX will simply re-cache the/those items when they are requested again.

- User Notifications
- Cluster-related Activities

- CVIX Planned Startup and Shutdown
- CVIX Data Retention and Purges
- CVIX and Backups
- CVIX and User Management

## CVIX Monitoring

In typical usage scenarios, the CVIX service will need only minimal monitoring and maintenance.

- 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.
- For a given CVIX server, you can get a sense of 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 deleted.

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.

If the load balancer appliances encounter an issue they will email the [REDACTED](#) group automatically.

## 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 as described in the *VIX Log Collector Service* chapter on page 45.

An instance of the CVIX transaction log resides on each active server in on the CVIX cluster. The log itself is accessed using Internet Explorer 7 or later and Firefox 3 or later.

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




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* on page 16.

**Note:** Because the CVIX is set up as a load balanced cluster without server affinity, you will typically need to 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 `http://<FQDN>/Vix/secure/VixLog.jsp`.
2. Enter your VistA access and verify codes in the User Name and Password boxes and click **OK**.

**Note:** Transaction log credentials are authenticated against the local **VistA** system. Attempting to use Windows credentials 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 on page 16.
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 previous page of (newer) entries.
  - Click  to show the first page (newest) entries in the log.

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

1. To change the date range used to filter log entries, change the values in the Start Date and End Date boxes, and then click **Show in Browser**.
  - Dates are formatted as MM/DD/YYYY.
  - The most recent log entries are shown first.
2. To change the number of entries displayed on each page, select a different value from the Transactions per Page box, and then click **Show in Browser**.

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

1. On the Transaction Log page, use the date range boxes near the top of the page to specify the desired date range of entries to export.
  - 1,000 exported log entries will result in an approximately 0.5 megabyte file.
  - The Transactions per Page setting does not apply when log entries are supported.
2. Click **Save as CSV** for comma-separated values or **Save as TSV** for tab-separated values.
3. Use the browser Save dialog box to specify where the file will be stored.
4. Use a spreadsheet program or a text editor to open the resulting file.

**CVIX Transaction Log Fields**

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

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

<b>CVIX Transaction Log Fields</b>	
<b>Name</b>	<b>Description</b>
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, beginning when the CVIX receives a message and ending when the CVIX begins to send the response.
ICN	The Integration Control Number used to uniquely identify the patient across the VA and DoD systems.  (Note that the ICN is not equivalent to the VA patient ID, and is not considered Protected Health Information.)
Query Type	A multi-part field that indicates [ <i>handler method receiving site &lt;- sending site</i> ].  <i>handler</i> identifies the VIX Web application that handled the request. For details see the <i>CVIX Interfaces</i> section on page 53.  <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 date was transferred.

<b>CVIX Transaction Log Fields</b>	
<b>Name</b>	<b>Description</b>
Asynchronous	Indicates whether the transaction was performed asynchronously (true) or synchronously (false).
Items Returned	<p>The number of items returned to the requester.</p> <p>For study metadata, indicates the number of studies or images in the list being transmitted. For an image, this field will have a value of 1 if the requested image was transmitted or 0 if the requested image was not found.</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, 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.</p> <p><i>In the exported log, this field is labeled "Data Source Items Received."</i></p>
Bytes Returned	<p>If populated, the amount of data returned in the request.</p> <p><i>In the exported log, this field is labeled "Façade Bytes Returned."</i></p>
Bytes Received	<p>If populated, the amount of data received in the request.</p> <p><i>In the exported log, this field is labeled "Data Source Bytes Received."</i></p>
Throughput	The image transfer rate. Both the rate and the units of measurement (KB/sec, MB/sec are indicated). Not populated for metadata. This value is calculated at runtime and is not present in the exported log.
Quality	<p>Populated for images only. Can be one of the following:</p> <p style="text-align: center;">THUMBNAIL REFERENCE DIAGNOSTIC DIAGNOSTIC UNCOMPRESSED</p> <p>For more information about these parameters, see <i>Remote Image Retrieval</i> on page 40.</p>
Command Class Name	Internal CVIX command used for debugging and support.
Originating IP Address	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 BHIE framework.)
User	The name of the clinician that initiated the request.

<b>CVIX Transaction Log Fields</b>	
<b>Name</b>	<b>Description</b>
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 exchange – Radiology data from a source outside of VistA (typically the DoD) vftp – Data from another VIX xca – Non-radiology data from a source outside of VistA (typically the DoD)
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 PACS integrator and/or Imaging jukebox 412 – BSE token expired 415 – Image conversion exception 500 – Internal server error
Realm Site Number	The STATION NUMBER (field (#99) of the INSTITUTION file (#4) of the site that the requester's credentials are authenticated against.
URN	Only populated for image transactions. Universal Resource Name; the unique name of the image being requested.
Transaction Number	The Globally Unique Identifier (GUID) for an image or metadata transaction. For transactions that originate from Clinical Display or the BHIE framework, the same identifier will be reflected in the Image Access log at the site where the images are stored.
VIX Software Version	The software version of the CVIX.

CVIX Transaction Log Fields	
Name	Description
VistA Login Method	The log in method used to access a VistA system. This is only populated when connecting to VistA and only for the transaction that initiates the connection. Possible values are BSE, CAPRI, or LOCAL.
Client Version	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. 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.
DataSourceResponse 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. <b>Note:</b> This field cannot be populated if the requesting or responding sever is a MAG*3.0*83 VIX.
VIX Site Number	The site number of the local VIX (as defined in the local VIX's VixConfig.xml file). The site number should match the station number (field #99) defined in the INSTITUTION file (#4).
Requesting VIX Site Number	The site number of the requesting VIX (as defined in the remote VIX's VixConfig.xml file), Only populated for Federation (VIX-to-VIX) requests. The site number should match the station number (field #99) defined in the INSTITUTION file (#4).

### CVIX Transaction Log Fields (Export Only)

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

CVIX Transaction Log Fields (export only)	
Name	Description
Facade Bytes Retrieved	The number of bytes returned to the requestor, where the requestor could be Clinical Display, VistARad, another VIX, or the CVIX.
Data Source Bytes Returned	The number of bytes returned from the data source, where the data source could be a remote VistA system, a VIX, the CVIX, or a DoD data source such as the BIA or HAIMS.
Machine Name	Name of the CVIX server that performed the transaction.

<b>CVIX Transaction Log Fields (export only)</b>	
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 used for debugging and support.
Thread ID	The name of the thread that processed the transaction.

### 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*.

### Using the Cache Manager

A Cache Manager function allows users to browse the CVIX cache and delete data as required. The Cache Manager is accessed using Internet Explorer 7 or later and Firefox 3 or later.

To access the CVIX Cache Manager, go to <http://<FQDN>:8080/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.



## Cache Organization

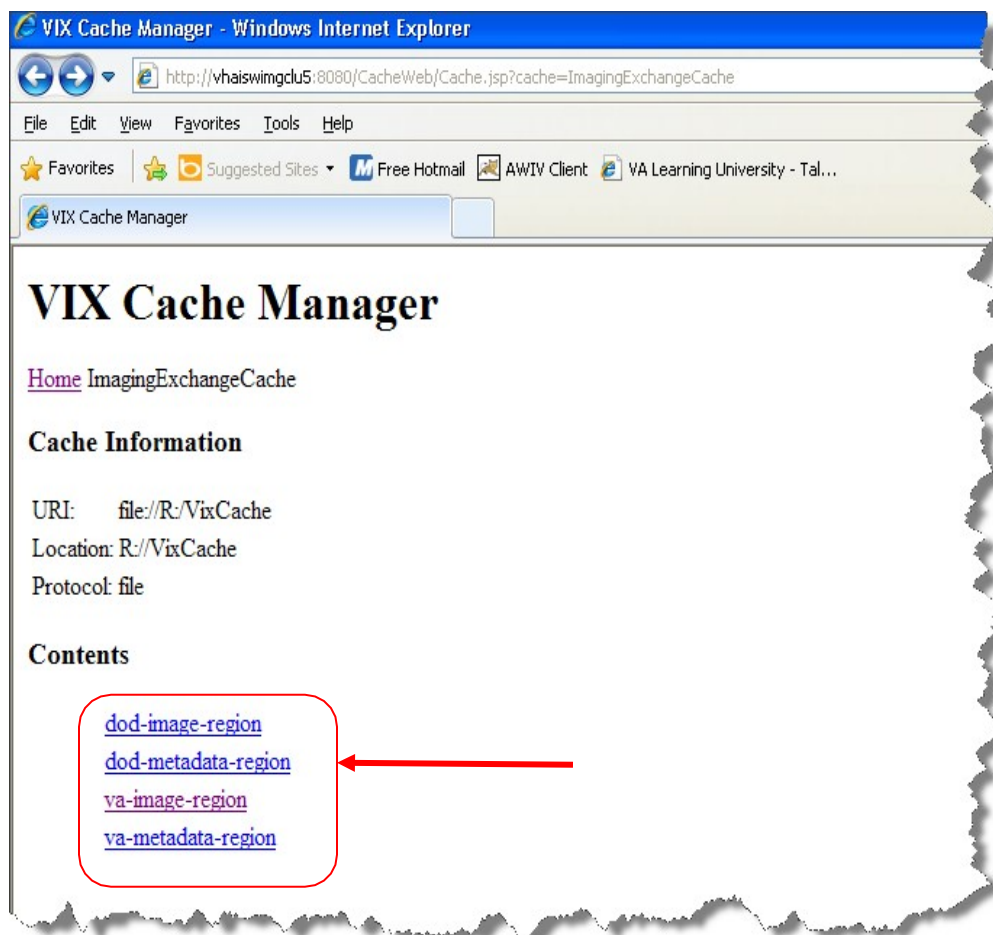
The data in the cache is arranged in a hierarchy with one or more of the following levels;

- data source (VA or DoD) and type (artifact, metadata, or image)
- repository (VA site or DoD facility)
- patient identifier (Integrated Control Number [ICN] for VA patients)

in some cases the

- study (group) identifier
- series and instance identifiers.

The source and type of the data are the most important factor in determining where an item is cached. When the CVIX Cache Manager is started, the following screen displays:



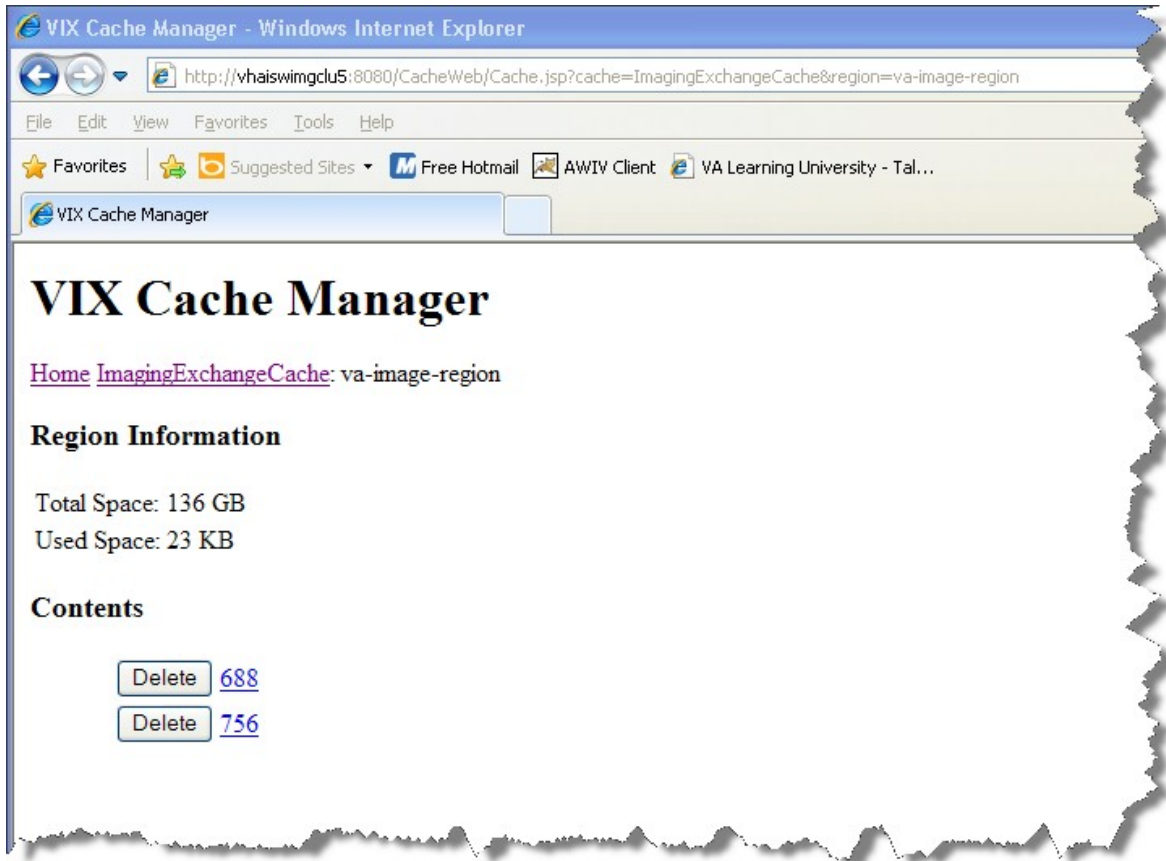
The items immediately under the cache name are called “regions” of the cache. Regions divide the items in the cache by the source of the item (VA versus anywhere else) and the type of the item (image versus anything else). A region defines the conditions under which a cache item is deleted from the cache.

Historically, it has been the case that anything that is not from the VA is from the 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”.

### **Technical Specifics**

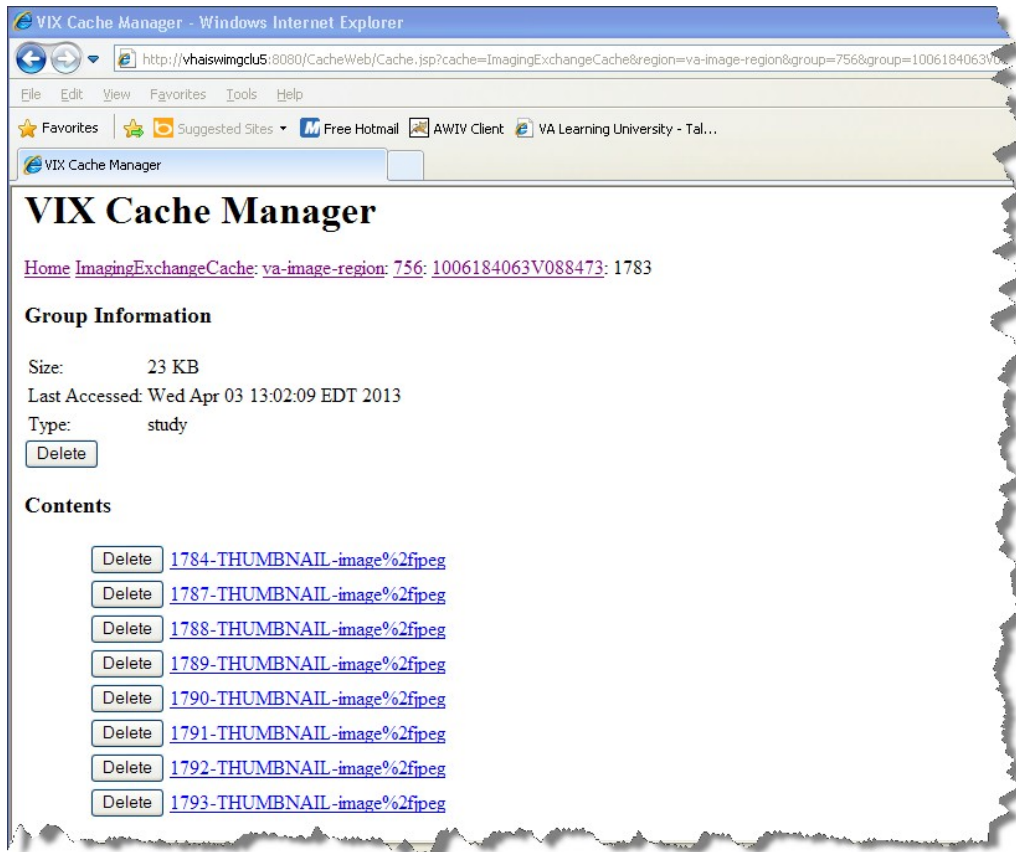
The cache does not understand anything about sites, patients, or studies but operates on the concept of regions, groups, and instances. Regions are collections of similar items that have the same lifespan in the cache (i.e., 30 days since last use). Groups are collections of groups and instances. Instances are the cache items proper. Groups are what is called a recursive data structure, a group can contain other groups, which in turn can contain still more groups, *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. If you think of the images in a study, then this makes more sense, if a study has not been accessed for 30 days, then the entire study is deleted from the cache. If none of the studies for a patient has been accessed within 30 days, then the whole patient is deleted from the cache.

Click the “va-image-region” region link and a list of cache groups will be displayed. You should see something like the next illustration, except that the cache contents will be different.



The CVIX Cache Manager displays the name of the region in the breadcrumb at the top of the page, and a list of the image repositories in this region. To drill down into an image repository, click on the image repository number. To delete an entire image repository, click on the **Delete** button to the left.

You can drill down through the 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 item in the cache at any level, click on the **Delete** button to the left.



### The DoD Regions

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

OID	Enterprise
<b>2.16.840.1.113883.3.42.10012.100001.207</b>	<b>DoD Radiology</b>
<b>2.16.840.1.113883.3.42.10012.100001.206</b>	<b>DoD Documents</b>
<b>2.16.840.1.113883.3.198</b>	<b>DoD NCAT Reports</b>
<b>2.16.840.1.113883.3.166</b>	<b>VA Documents</b>
<b>2.16.840.1.113883.6.233</b>	
<b>1.3.6.1.4.1.3768</b>	<b>VA Radiology</b>

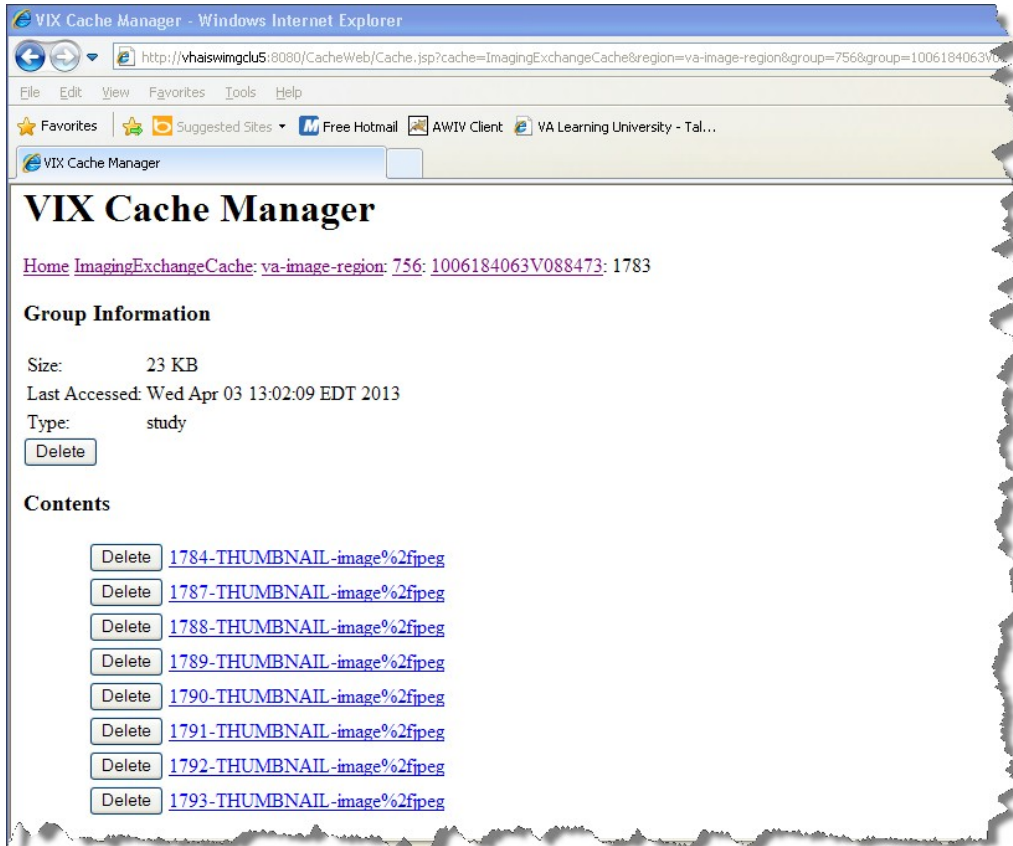
**Note:** The DoD NCAT server is no longer on line.

Below the enterprise OID is a repository (a site in VA parlance). At this time, DoD documents always come from the Central HAIMS server and are identified as “central”.

Likewise, DoD radiology always comes from the BIA, identified as “200”. DoD NCAT reports come from their own enterprise OID.

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.



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

### 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. 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 obviously corrupt data, then the item should be located in all of the cache instances and deleted.

To delete a cache item, collect as much identification information as you can. 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, patient identifier (Integrated Control Number [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 you want the item deleted. The cache does not immediately delete the item since it has to synchronize operations from all clients. It may take a few seconds or up to a minute before the item is actually deleted. Usually, 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 the 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 of the “bad” ones. This is not an issue, since the CVIX will simply re-cache the/those items when they are requested again.

## User Notifications

A CVIX outage (planned or unplanned) should be announced using the Automated Notification Report (ANR) system. You can do this by logging an ANR directly at [REDACTED](#), or by contacting the National Help Desk.

If you encounter ongoing connectivity issues with BHIE or BIA, you can also contact the **VA IT BHIE Technical** mail group.

## Cluster-related Activities

The following sections cover:

- CVIX cluster: take node offline
- CVIX cluster: bring node online
- Log Collector cluster: transfer cluster group and resources
- Checking which load balancer is active

### CVIX cluster: take node offline

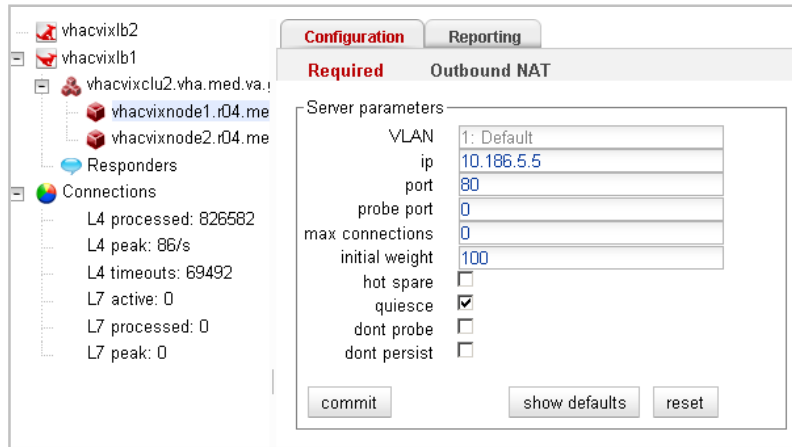
Use the following steps to take a single CVIX server node offline for maintenance.

1. Use a web browser to go to the active load balancer administrator page at [REDACTED](#).

**Note:** If you need to determine which load balancer is active, see the steps on page 31.

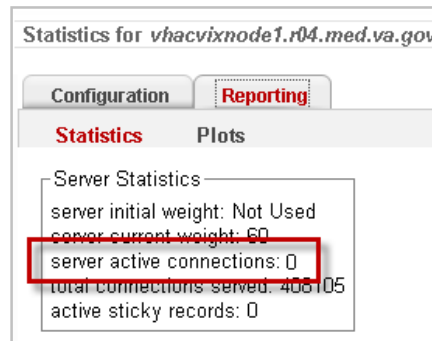
2. Log in using the username and password provided by the VistA Imaging team.
3. On the left side of the Welcome page, under the vhaevixclu2. [REDACTED](#) cluster, select the server that needs to be taken offline.

- In the Server parameters area, select the **quiesce** checkbox, and then click **commit**. This tells the load balancer not to route any additional requests to that server.



- Click the Reporting tab and check the contents of the Statistics box.
- When the **active connections** line displays 0 the server is offline.

**Note:** The load balancer web interface does not refresh automatically. To force a refresh, click back and forth between the Statistics and Plots sub-items on the Reporting tab.



- Perform the maintenance on the server.

**Tip:** The CVIX service will remain running on the server but will not be processing since it is not getting any data from the load balancer. The CVIX service can remain running while installing Microsoft patches. The CVIX service will restart automatically after a server reboot.

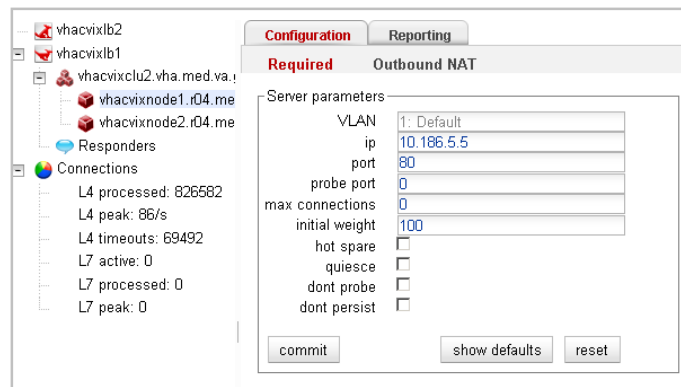
### CVIX cluster: bring node online

- Use a web browser to go to the active load balancer administrator page at [REDACTED](#).



**Note:** If you need to determine which load balancer is active, see the steps on page 31.

2. Log in using the username and password provided by the VistA Imaging team.
3. On the left side of the Welcome page, under the **Content removed: FOIA exemption b2/**, select the server that needs to be brought back online.
4. In the Server parameters area, clear the **quiesce** checkbox and then click **commit**. This tells the load balancer start routing requests to that server.



### Log Collector cluster: transfer cluster group and resources

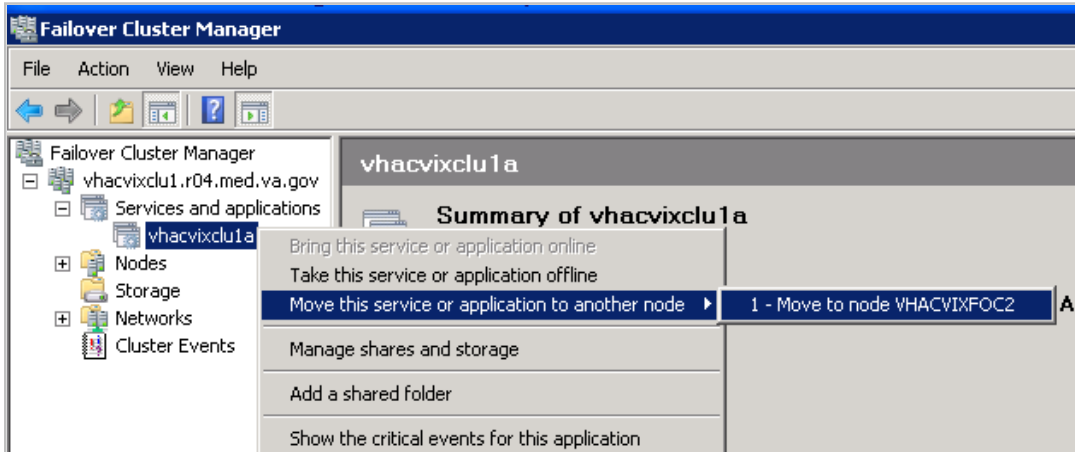
Use these steps to perform maintenance on the active server in the failover cluster (vhacvixclu1. **REDACTED**) that hosts the VIX Log Collector.

1. Log into the active server using a VA domain account with administrative privileges.

**Note:** These steps assume that the active server is **Content removed: FOIA**

2. Start the Failover Cluster Manager (**Start | All Programs | Administrative Tools | Failover Cluster Manager**).

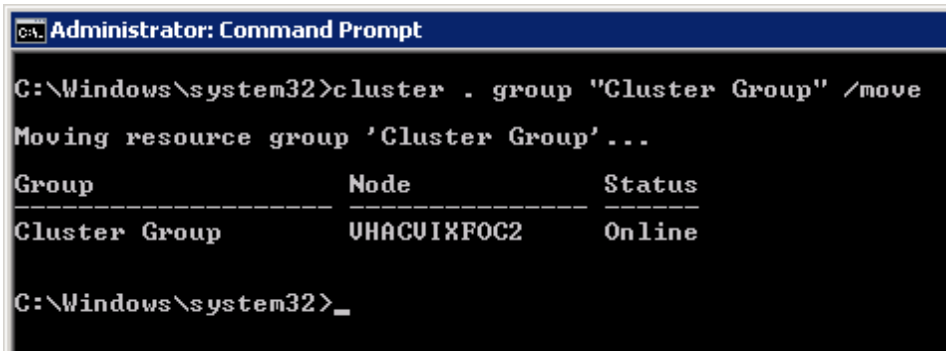
- In the left side of the window, expand the tree and select **vhacvixclu1a**. Then right-click and choose **Move this service or application to another node**→**1-Move to node VHACVIXFOC2**.



- Open an administrative command line window (click **Start**, then right-click **Command Prompt** and choose **Run as administrator**).

- Type this command in the command window:

```
cluster . group "Cluster Group" /move
```



- Perform the needed maintenance on the server.
- After maintenance is complete, use the Failover Cluster Manager to move the **vhacvixclu1a** resource back to the original server.
- Repeat steps 4 and 5 above to revert the cluster group back to the original server. (Node will be: VHAICVIXFOC1).

### Checking which load balancer is active

By default, the `vhacvixlb1` load balancer is the active load balancer. However, if there is any question as to which load balancer is active, do the following:

1. Use a web browser to go to either load balancer.

[REDACTED REDACTED](#)

2. Log in using the username and password provided by the VistA Imaging team.
3. When the Welcome page displays, hover the mouse pointer over the Equalizer System Information box. It will expand to show additional information.
4. In the expanded Equalizer System Information box, check the contents of the **failover mode** field.
  - If **primary** is shown, you are logged into the active load balancer.
  - If **backup** is shown, you are logged into the backup (inactive) load balancer.

### CVIX Planned Startup and Shutdown

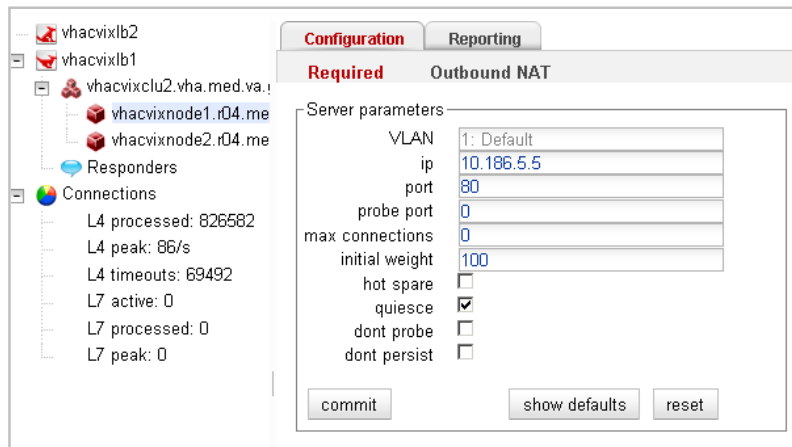
The CVIX is designed to be running at all times; for procedures about taking individual servers offline for maintenance, see the previous section.

If you must fully shut down and then restart all CVIX hardware, use the steps below.

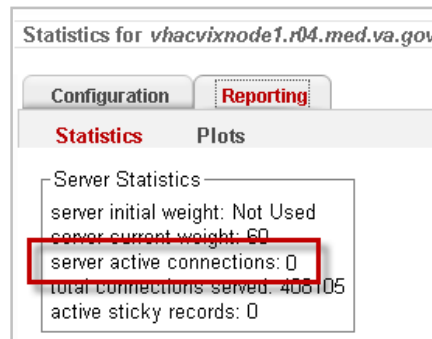
#### Planned Full CVIX Shutdown

1. Review the section *CVIX Dependencies* on page 9 to make sure that all the implications of a full CVIX shutdown can be planned for.
2. [REDACTED](#)
3. Quiesce all CVIX load-balanced server nodes as described in the following steps:
  - a. Use a web browser to go to the active load balancer administrator page at [REDACTED](#) and log in using the username and password provided by the VistA Imaging team.
  - b. On the left side of the Welcome page, select the first server under the `vhacvixclu2.vha`. [REDACTED](#) cluster.

- c. In the Server parameters area, select the quiesce **checkbox**, then click **commit**. This tells the load balancer not to route any additional requests to that server.



- d. Select and quiesce each remaining server in the cluster.
- e. For each server, check the Statistics box under the Reporting tab. When the **active connections** line displays 0, that server is quiescent.



**Note:** The load balancer web interface does not refresh automatically. A good way to force a refresh is to click through each cluster server in the tree, and recheck the active connections line until it shows as 0 for all servers in the cluster.

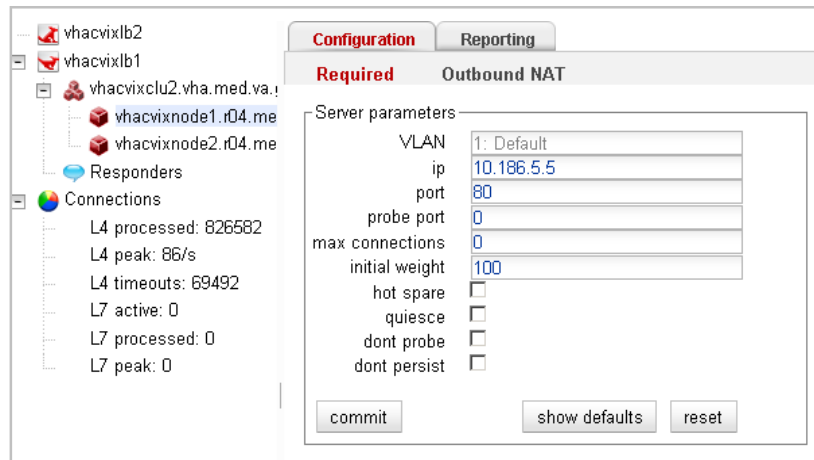
4. For each of the following servers, log in as an administrator and perform a Windows shutdown. When prompted, provide a meaningful reason for the shutdown.
- vhacvixnode1.r04.**REDACTED**
  - vhacvixnode2.r04.**REDACTED**
  - vhacvixnode3.r04.**REDACTED**
  - vhacvixnode4.r04.**REDACTED**
  - vhacvixnode5.r04.**REDACTED**

- `vhacvixnode6.r04`.REDACTED
5. Shut down both load balancers as follows:
    - a. Use a browser to go to <http://vhacvixlb2.r04.REDACTED> and log in. On the left side of the Welcome page, `vhacvixlb2`, select the Maintenance tab, and then click **shutdown**.
    - b. Use a browser to go to <http://vhacvixlb1.r04.REDACTED> and log in. On the left side of the Welcome page, `vhacvixlb1`, select the Maintenance tab, and then click **shutdown**.
    - c. Power down each load balancer by toggling the power switch.
  6. Shut down the CVIX failover cluster as follows:
    - a. Log into `vhacvixfoc2.r04`.REDACTED as an administrator and perform a Windows shutdown.
    - b. Log into `vhacvixfoc1.r04`.REDACTED as an administrator and perform a Windows shutdown.
    - c. Power down the MSA 2300 shared storage by toggling the power switch.
  7. Power down each of the four Power Distribution Units on the CVIX rack by toggling the power switches.

### Planned Full CVIX Startup

1. Turn on each of the four Power Distribution Units by toggling the power switches.
2. Turn on the CVIX failover cluster as follows:
  - a. Power up the MSA 2300 shared storage.
  - b. Power up `vhacvixfoc1.r04`.REDACTED.
  - c. Power up `vhacvixfoc2.r04`.REDACTED.
3. Start both load balancers as follows:
  - a. Turn on `vhacvixlb1` (the topmost load balancer in the rack) by toggling the power switch. Wait 60 seconds.
  - b. Turn on `vhacvixlb2`.

4. Power up each of the following servers.
  - vhacvixnode1.r04.**REDACTED**
  - vhacvixnode2.r04.**REDACTED**
  - vhacvixnode3.r04.**REDACTED**
  - vhacvixnode4.r04.**REDACTED**
  - vhacvixnode5.r04.**REDACTED**
  - vhacvixnode6.r04.**REDACTED**
  
5. Use the active load balancer to bring each of the CVIX server nodes online as described in the following steps:
  - a. Use a web browser to go to the active load balancer administrator page at [http://vhacvixlb1.r04.\*\*REDACTED\*\*](http://vhacvixlb1.r04.<b>REDACTED</b>) and log in using the username and password provided by the VistA Imaging team.
  - b. On the left side of the Welcome page, select the first server under the vhacvixclu2.vha.**REDACTED** cluster.
  - c. In the Server parameters area, clear the quiesce **checkbox**, then click **commit**.



- d. Repeat the step above for each server that needs to be brought online.
  
6. If there is an open ANR for the CVIX, update the ANR to indicate that the service interruption is over.

## CVIX Data Retention and Purges

The CVIX runs a daily purge process for locally stored data, as described in the following table:

Operation	When Performed
Purge Java logs	1 A.M. daily for Java log entries more than 30 days old.
Purge transaction log entries	2 A.M. daily for transaction log entries more than 90 days old.
Purge CVIX cache	3 A.M. daily for images more than 30 days old. Once per minute for old VA metadata, once per hour for old DoD metadata

## CVIX and Backups

The CVIX does not need to be explicitly backed up.

- CVIX transaction logs are automatically backed up by the VIX log collector service.
- The 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 Imaging Product Development Group for details.

## CVIX and User Management

CVIX administrators access and maintain the CVIX using the built-in administrator accounts on the Unix-based load balancers and on the Windows-based cluster and failover servers.

VA clinicians that request data via the CVIX use their local VistA site credentials. These are independent of the CVIX.

DoD clinicians that request data via the CVIX do so using a service account (named CVIX,USER) defined for them on the Station 200 VistA System.

This page is intentionally left blank.



# VistA Site Service

---

This chapter covers:

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

## 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, to remote VistA systems, and to 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\vhbsites.xml). Then the connection information is passed back to the load balancer and ultimately back to the requestor.

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

## 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 lists 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.

**Note:** If the CVIX becomes unavailable, the site service URL can be temporarily redirected from the CVIX (10.186.5.13) to the backup site service cluster in Albany (10.1.14.87). To make this change, enter a Remedy ticket with a Category/Type/Item of Applications-Enterprise/DNS/Issue and a priority and urgency of high.

## 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 \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 while you do this):
  - C:\VixConfig
  - C:\Site Service
6. For each CVIX node, refresh its cached site service connection information by doing the following:
  - a. Use a browser to go to [REDACTED](#), where <xxx> is the name of the CVIX node.
  - b. In the Site Service Utilities web page, click the **Refresh Site Service** button.
7. Enter a Remedy ticket to have the updated VhaSites.xml file sent to the site service backup server administrator at Albany.
  - For the ticket's category/type/item, use Applications-VistA/VistAWeb/Other.
  - For the tickets subject line, use "Changes to the COOP Site Service database (Albany)".
8. 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 pm daily.

# CVIX Image Sharing

---

- The CVIX is a key link in VA-DoD image exchange, and is the primary source of information for the VA AWIV. A functional description of the CVIX’s image sharing capabilities is covered in the *CVIX Major Functions* section on page 3. This chapter covers:
  - Remote Metadata Retrieval
  - Remote Image Retrieval
  - Caching of Metadata and Images
  - Image Sharing and CVIX Timeouts

## Remote Metadata Retrieval

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

**Tip:** 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, number of images in an exam and so on.

In some cases, metadata retrieval is the only action needed to completely 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 AWIV), 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 following applications can request metadata from the CVIX:

Requesting Application	Type of metadata requested	CVIX interface used by requestor**	Ultimate source of requested metadata
VIX (on behalf of Clinical Display or VistARad)	DoD metadata for all DoD image/artifact types	Federation	BIA for DICOM-related metadata BHIE for artifact-related metadata
AWIV	VA metadata associated with a specific progress note or radiology report	AWIV	VIX at VA site if VIX is available. VistA at VA site if VIX is not available.

Requesting Application	Type of metadata requested	CVIX interface used by requestor**	Ultimate source of requested metadata
BIA	VA metadata related to DICOM images	Exchange	
BHIE	VA metadata related to all other image types.	XCA	

\*\* See page 53 for more information about CVIX interfaces.

2. If the CVIX is processing a request from the BIA or BHIE, 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 if 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 the table in step 1).

The CVIX passes the data back to the requesting application.

## 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 metadata request as described in the previous section.

1. One of the following applications requests a remote image based on a clinician's activities:
  - BIA on behalf of a DoD clinician (VA DICOM images).
  - HAIMS on behalf of a DoD clinician (VA non-DICOM images).
  - Clinical Display or VistARad on behalf of a VA clinician (DoD images).
  - AWIV 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 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 CVIX cache, 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 the table below.

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 AWIV when clinicians request full-fidelity non-radiology images from other VA sites via the CVIX, or will be used by the CVIX when it is 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. Typical compression ratio is about 2.5:1.  This parameter can be used by any image requestor except for a DoD system that uses XCA.
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.  This parameter can be used by any image requestor except for a DoD system that uses XCA.
THUMBNAIL	N/A. This parameter refers to a thumbnail image stored on (or created by) the originating system.  This parameter can be used by any image requestor except for a DoD system that uses XCA.

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.

## Caching of Metadata and Images

The CVIX automatically stores all images and most of the metadata it handles in its own local cache. The CVIX cache is self-managing and is independent from 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 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.

### Cache Retention Periods

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

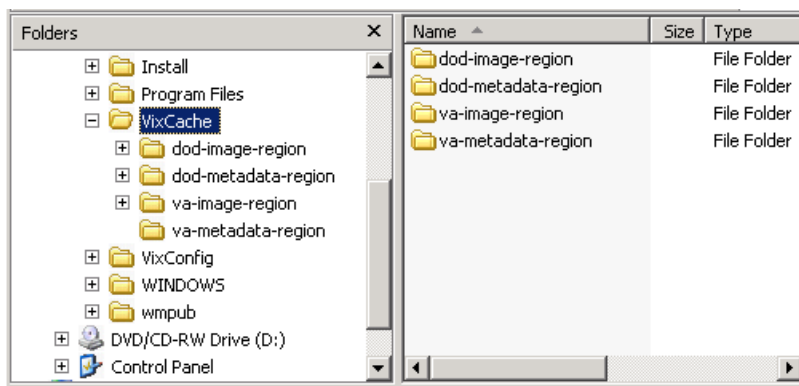
The following table lists retention periods based on the source and type of the data.

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

### Cache Location and Structure

The CVIX cache is located in C:\VixCache on each node in the CVIX load balanced cluster.

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.



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.

## Image Sharing and CVIX Timeouts

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

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

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 data transfer begins in a few seconds).</p> <p>For images, wait up to 30 seconds for 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.</p> <p>For images, the CVIX will wait up to 30 seconds for the initial connection with the DoD image source, and up to 120 seconds to 120 seconds for the image transfer to begin.</p> <p>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>

This page is intentionally left blank.



# 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

## VIX Log Collector Overview

The Log Collector automatically backs up transaction logs on remote VIXes and on the CVIX. This allows the information in VIX transaction logs to be retained after local instances of the 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 4:30 AM.

The VIX Log Collector service is installed on the CVIX failover cluster (vhacvixclu1.**REDACTED**).

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.

If you want to manually verify that the Log Collector is gathering logs as expected, check the storage area (G:\VIXLogs\) for collected logs for newly backed up files. For specifics, see the *Archived Transaction Log Storage Area* section on page 46.

## Log Collector Automatic Emails

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

Email addresses are initially specified when the Log Collector service is installed. If you need to change who gets this email, use the following steps.

1. Log in as an administrator to the active server in the failover cluster (usually vhacvixfoc1.r04.**REDACTED**).

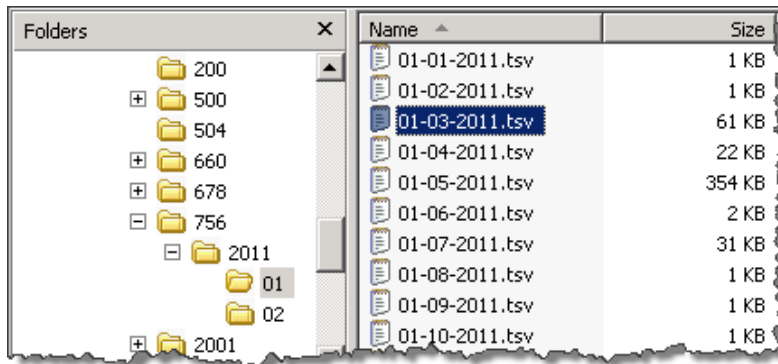
2. Navigate to C:\Program Files\Vista\Imaging\VixLogCollectorService.
3. Open the file named VixLogCollector.WindowsService.exe.config in a text editor.
4. Locate the “emailAddress” key near the beginning of the file.
5. Edit the value for the emailAddress key as needed. Separate each email address with 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.

## Archived Transaction Log Storage Area

The archived transaction log files gathered by the Log Collector are stored under G:\VIXLogs on the failover cluster. 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.




**Tip:** Because 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.

## Excluding a VIX from Log Collection

Use the following steps if you need 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 you want to disable log collection.
  - 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. Log in as an administrator to the active server in the failover cluster (usually )
3. Navigate to where the archive logs are stored (G:\VixLogs is the default location).
4. Open the folder of the VIX (or CVIX) to disable.
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.

This page intentionally blank.

# CVIX Troubleshooting

---

This section covers:

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

## Routine Errors

### Connectivity

Occasional data retrieval failures are to be expected given the nature of the WAN and the number of systems that communicate with the VIX.

### 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 page 43.

### Security

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

If VA clinicians cannot access DoD DICOM (radiology) images, the issue may be authentication at the BIA.

If VA clinicians cannot access DoD artifacts (scanned documents and non-radiology) images, the issue may be authentication at HAIMS.

### 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. Other CVIX functions are unaffected.

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

## Significant Errors

### 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, you will typically need to 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 page 14.

For information about the CVIX's Java logs, see page 56.

## Unplanned Shutdowns

### Recovering after unplanned restart of a single CVIX server

If a single server in the CVIX cluster is 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 on page 27.

### 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. You should let the second load balancer retain the active role if this occurs.

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

Start up the CVIX as described on page 33, and issue an ANR (see details in next section) describing the nature of the outage and the time of its resolution.

Closely monitor CVIX operations until normal operations are verified.

## CVIX Support

If you encounter any problems with the CVIX that are not addressed in this document, enter a Remedy ticket and ask that it be directed to Tier 3 support (specifically, the VistA Imaging Product Development group within the Office of Information & Technology (OIT)).

If you encounter ongoing connectivity issues with BHIE or BIA, you can also contact the **VA IT BHIE Technical** mail group.

[REDACTED](#)

This page is intentionally blank.



# CVIX Reference/Software Description

---

## CVIX Java Components

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

### 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.

### CVIX Security Realms

The CVIX implements security realms to verify that only properly authenticated applications (the AWIV, site VIXes, and DoD systems) can use the interfaces provided by the CVIX Web applications. 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* on page 11 for more information.

### 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. The following table summarizes each CVIX interface.

Interface Name	Description
AWIV interface	Handles metadata and image requests from the AWIV; <b>Content</b>
Exchange Interface	Handles DICOM metadata and image requests from DoD providers via the BHIE Imaging Adapter (BIA). <b>Content</b>
Federation interface	Handles metadata and image requests from site VIXes; <b>Content</b>
XCA	Handles non-DICOM metadata and image requests from BHIE and HAIMS servers. <b>Content</b>

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 provides a response (the requested data), the same interface responds to the requesting application.

## 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 one to retrieve the data requested and packages the request appropriately before passing the request to the data source.
- Implements and manages the CVIX cache.

## 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. The following table summarizes each CVIX data source. These data sources are identified in the Datasource Protocol field in the CVIX transaction log.

Data Source Name	Description
exchange	Retrieves DICOM data from the DoD via the BIA's exchange interface.
vistaimaging	Retrieves data from a VistA Imaging System using RPCs.
vista	Retrieves data from a VistA system without Imaging using RPCs. This data source is currently used by the CVIX for communicating with the Station 200 VistA system.
vftp	Retrieves data from other VIXes (or the CVIX) using their Federation interfaces.
xca	Retrieves metadata from the BHIE framework and non-DICOM images from HAIMS and NCAT servers.

## Java Installation Locations

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

### 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 6.0**

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\jre1.6.0\_30**

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

**\Program Files(x86)\Vista\Imaging\CvixInstaller**

CVIX installation files and resources.

**\VixCertStore**

Stores CVIX security certificates. For details about security certificates, see the *CVIX Security Certificate* section on page 59.

**\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* on page 42.

**\VixConfig**

Configuration files 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.

## Java Logs

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

**catalina.log:** Tomcat (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.

## VistA/M Information

The following sections describe 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.

### RPCs used by the CVIX

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 (Broker Security Enhancement) 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 that is 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>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>MAG (VistA Imaging) RPCs used by the CVIX</b>	
<b>RPC Name</b>	<b>Description</b>
<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.
<b>MAGG ACTION LOG</b> Routine: LOGACT^MAGGTU6	Call to log an action performed on the image. Actions are logged 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.

**Non-MAG RPCs used by the CVIX**

The CVIX uses the following RPCs from other VistA packages. The use of these RPCs is governed by Integration Control Registrations (ICRs) stored in FORUM. For information about viewing specific ICRs, see Chapter 12 in the *VistA Imaging Technical Manual*.

<b>Non-MAG RPCs used by the CVIX</b>	
<b>RPC Name</b>	<b>Description</b>
<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 parameter set to yes and user is not a key holder, a social security number must be defined in the NEW PERSON file (#200) for the user to access any Patient file (#2) record.
<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 ACTION input parameter.
<b>VAFACTFU CONVERT ICN TO DFN</b> Routine: GETDFN^VAFACTFU1	Given a patient Integration Control Number (ICN), this will return the patient Internal Entry Number (IEN) from the PATIENT file (#2).
<b>VAFACTFU GET TREATING LIST</b> Routine: TFL^VAFACTFU1	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.
<b>XUS DIVISION SET</b> Routine: DIVSET^XUSRB2	Sets the user's selected division in DUZ(2) during sign-on.
<b>XUS SIGNON SETUP</b> Routine: SETUP^XUSRB	Establishes 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.

## Database Information

The CVIX retrieves data 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* on page 26 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 does this using 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.

## Exported Menu Options

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

## Security Keys

There are no VistA security keys associated with the CVIX.

## Other VIX Components

The CVIX incorporates the following additional components:

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

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

## CVIX Security Certificates

When a CVIX communicates with another VIX or with a DoD system (HAIMS, NCAT, 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 by 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 BHIE, HAIMS, and NCAT systems were provided by the teams administering each production system.

### **.NET**

The .NET 2.0 framework is needed to install and update the CVIX software. This is installed as part of the Windows Server 2008 x64 operating system.

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.

### **Sun JRE**

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

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

### **Laurel Bridge DCF Toolkit**

The Laurel Bridge DICOM Connectivity Framework (DCF) toolkit, version 3.3.22c, 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.

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

### **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.

Version 3.18.7.2 of 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 unless explicitly directed to do so by the Imaging development team.



# Index

---

- #2005 file, 59
- #2006.95 file, 22
- .NET 2.0 framework, 60
- abstract (thumbnail) quality, 41
- accounts, user, 36
- Advanced Web Imaging Viewer (AWIV), 8, 39
- audience, 1
- Automated Notification Report (ANR), 51
- Automated Notification Report system, 28
- Aware JPEG2000 toolkit, 55, 59, 60
- Aware toolkit, 60
- AWIV, 11, 39, 53
- backups, CVIX, 36
- BHIE, 12, 28, 40
- BIA, 11, 28, 40
- cache. *See* CVIX cache
- cluster
  - bring nodes online, 29
  - specifications, 9
  - taking nodes offline, 28
- compression parameters, 41
- connection data, central registry of, 37
- connection timeouts, 43
- Continuity of Operations, 11
- CSV file, exporting transaction log as, 17
- CVIX
  - additional documentation for, 2
  - backups and, 36
  - connection security, 12
  - connection timeouts, 43
  - dependencies, 11
  - described, 1, 5
  - image retrieval and, 40
  - installation locations, 54
  - Java logs, 56
  - licensed subcomponents of, 60
  - Log Collector service and, 45
  - metadata retrieval and, 39
  - monitoring, 15
  - multidivisional sites and, 12
  - operational priority, 10
  - ports, 53
  - purge operations, 36
  - RPCs used by, 56, 58
  - security certificate, 59
  - shutdown and startup, 32
  - specifications, 9
  - terms of use, 1
  - transaction log, 15
  - VistA changes made by, 59
  - VistA logging and, 22
- CVIX cache
  - checking for images, 40
  - described, 42
  - monitoring, 15
  - retention periods, 42
  - structure of, 42
- CVIX core, 54
- data sources, CVIX, 54
- dependent systems
  - CVIX shutdown and, 32
  - summary of, 11
- DIAGNOSTIC parameter, 41
- DIAGNOSTIC UNCOMPRESSED param., 41
- DICOM toolkit, 60
- EKG waveforms, 7
- Exchange Interface, 53
- façades (interfaces), CVIX, 53
- FDA guidelines, 1
- Federation interface, 53
- help, getting, 50
- Image Access Log (#2006.95) file, 22
- Image File (#2005), 59
- image sharing
  - AWIV, 8
  - DoD to VA, 5
  - VA to DoD, 7
- images
  - caching of, 42
  - retention periods for, 42
  - retrieving via CVIX, 40
- interfaces, CVIX, 53
- Java Runtime Environment, 60
- JPEG2000 toolkit, 60
- Laurel Bridge DCF toolkit, 59, 60
- load balancer, 9, 50
- Log Collector service, 45
- Log Collector Service, 5, 9, 45

## Index

- logical description, 9
- logs
  - CVIX transaction log, 15
  - Image Access Log (#2006.95) file, 22
  - Java, 56
- maintenance and monitoring, 15
- metadata
  - caching of, 42
  - described, 39
  - retention periods for, 42
- multidivisional sites, 12
- NCAT, 6, 12
- physical description, 9
- ports, CVIX, 53
- Protected Health Information, 17
- purging, CVIX, 36
- REFERENCE parameter, 41
- Remedy, 50
- RPCs used by CVIX, 56, 58
- security certificate for CVIX, 59
- security keys, 59
- security realms, CVIX, 53
- security, connections and, 12
- servlet container, VIX, 53
- shutdown, CVIX, 32
- specifications, CVIX, 9
- startup CVIX, 32
- Station 200, 11, 49
- Sun JRE, 60
- support, customer, 50
- THUMBNAIL parameter, 41
- timeouts, connection, 43
- transaction log
  - accessing, 15
  - exporting, 17
  - fields in, 17, 21
  - monitoring, 15
- troubleshooting, 49
- TSV file, exporting transaction log as, 17
- user accounts, 36
- VistA site service
  - checking, 37
  - overview, 37
  - updating, 37
- VistA, changes made by CVIX, 59
- Visual J# runtime environment, 60
- VIX
  - at VA sites, 7, 11
  - excluding from log collection, 47
  - registry of connection data for, 37
- VIX Log Collector service
  - described, 45
  - excluding a VIX from, 47
  - status emails from, 45
  - storage area used by, 46
- Web services, CVIX, 53
- XCA, 53