VistA Imaging System

VistA Imaging Exchange (VIX) Service Installation Guide

June 2016 – Revision 5

VistA Imaging Exchange (VIX) Service Installation Guide
June 2016

Property of the US Government

Revision History

Date	Rev	Notes
Oct 14 2011	1	Created for MAG*3.0*104. WPR complete Aug 31; labeled for release Oct 14. A McFarren, K. Buck, R. Coney.
May 07, 2012	2	Updated for MAG*3.0*122. L.Scorza, K.Buck, J.Werfel. C. Gilbert.
July 25 2013	3	Updated for MAG*3.0*034/116/118, MAG*3.0*119, MAG*3.0*127, MAG*3.0*129. L.Scorza, C. Huth, K. Buck, P. Yeager
September 9, 2013	4	Updated for MAG*3.0*130, L.Scorza, C. Huth, K. Buck, P. Yeager
May 10, 2016	5	Updated for MAG*3.0*162, L. Shope, J. Lin, N. Nguyen, S. Marner

Contents

Introduction

This document explains how to install the VistA Imaging Exchange (VIX) service.

The VIX:

- Implements image sharing between Department of Veterans Affairs (VA) and participating Department of Defense (DoD) medical facilities.

- Supports and extends VA-to-VA remote image sharing for Clinical Display and VistARad.

Intended Audience

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

This document presumes a working knowledge of the VistA environment, VistA Imaging components and workflow, and Windows administration. If the VIX is implemented on the Imaging cluster, a working knowledge of Windows cluster administration is also assumed.

Terms of Use

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

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

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

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**.

- Critical information is indicated by:

Related Information

In addition to this manual, the following document contains information about the VIX:

- *VistA Image Exchange (VIX) Administrator's Guide*

Installing a New VIX

This section explains how to implement a new VIX. The installation checklist in Appendix A, VIX Update Checklist, summarizes the process.

Tip: If you are updating an existing VIX, see the *Updating an Existing VIX* section.

Preparing for a New VIX Installation

Preparing to install a new VIX involves:

Setting up VistA

- Selecting and validating the server where the VIX will be installed
- Getting VIX component licenses
- Getting a VIX security certificate
- Scheduling server downtime (cluster installs)

Specifics are covered in the following sections.

Setting up VistA

You must install the compatible KIDS package on the VistA system before installing the VIX server software. For information about how to install the KIDS package, see the patch description of the patch you are installing.

- If you are implementing a VIX for the first time, the MAG VIX ADMIN key, introduced in Patch MAG*3.0*83, must be assigned to the VistA accounts of administrators who need access to the VIX transaction log.
- While it is not required, it is recommended that sites run the MagDexter and MagKat utilities provided in patch MAG*3.0*98. Doing so populates DICOM series information for radiology exams acquired before the release of MAG*3.0*50. See the *VistA Imaging Storage Utilities Manual* for details.

Selecting and Validating the VIX Server

The VIX supports both single and clustered server configurations. It is highly recommended that the VIX be installed on the Imaging cluster. If the existing Imaging cluster server cannot accommodate the VIX, the VIX can also be installed on a dedicated standalone server.

The server or cluster where the VIX is installed must meet the FDA, hardware, and operating system/environmental requirements specified in the following sections.

FDA Requirements

The VIX is a component of VistA Imaging and is therefore regulated as a medical device by the Food and Drug Administration (FDA). Use of the VIX is subject to the terms of use listed in the introduction.

Hardware Requirements

Minimum VIX hardware requirements:

- 4 gigabytes of RAM (per server if installing on a cluster)

- A dedicated local drive for the VIX cache with at least 50 gigabytes of disk space. A larger drive may desirable based on usage.

- A 1 gigabit Ethernet connection will need to be available for use by the VIX.

Port Requirements

On the server where the VIX is installed, verify that ports 8080 and 8443 are accessible to VA wide area network IP addresses (10.x.x.x).

Operating System and Environment Requirements

The VIX can run on:

- Windows Server 2008 R2

- Windows Server 2012 R2

.NET Framework Requirement

You can download the Microsoft .NET Framework from the SFTP site with the patch distribution files or from the Microsoft site.

Note: After installing HDIG, use the Windows Update to install any security updates available for .NET 2.0 or later.

Note: You can install more recent .NET updates as long as .NET 2.0 is included in that update.

Getting VIX Component Licenses

Two toolkits used by the VIX require third-party licenses.

Laurel Bridge DCF Toolkit

The Laurel Bridge DICOM Connectivity Framework (DCF) toolkit is a third-party toolkit used by the VIX to convert images to and from DICOM format.

The VA has purchased an enterprise-wide license for this toolkit. To request site-specific serial numbers for this license, do the following:

1. From the server where the VIX is installed, attempt to access the Laurel Bridge activation code server at http://www.laurelbridge.com. Click on "Customer Access" in the top right corner. . (A login page will display if you can access the site.)

   > If you cannot this access this site, enter a Remedy ticket and indicate that your site ACL (access control list) needs to be modified to access http://www.laurelbridge.com.

2. Contact the VHAVILBLicenses@va.gov mail group. They will provide a request form and instructions for completing the form.

The serial number information provided will ultimately be used to generate an activation code (this is done during the VIX installation process). The activation code allows the Laurel Bridge DCF toolkit to be installed and used.

The Laurel Bridge activation code is linked to the hardware of the server where the toolkit is installed. If you have to replace the licensed server, email the contacts listed previously to arrange to get the serial number(s) transferred as well.

Aware JPEG2000 Toolkit License

The Aware JPEG2000 toolkit is a third-party toolkit used for DICOM-to-JPEG2000 image conversion by the VIX.

Sites that implement the VIX must purchase a one-time permanent license for the latest version of the Aware JPEG2000 toolkit from Aware for each server where the VIX is used (a VIX on a standalone server would need one license; a VIX on a cluster would need one license for each server in the cluster).

IMPORTANT: Do not install the Aware JPEG2000 toolkit before you run the VIX installer. The VIX installer installs the version of the Aware JPEG2000 toolkit with which the VIX has been tested. If you install the Aware JPEG2000 toolkit before running the VIX installer, this will interfere with the installation process.

Getting a VIX Security Certificate

Each server that hosts the VIX must be issued a security certificate. To get security certificates, send an e-mail to VHAVIVIXSETUP@VA.GOV and include the following information:

- Fully qualified VIX server name (for a cluster, include the names of each server in the cluster in addition to the fully qualified cluster name).

- Contact information for the primary and backup administrators of the VIX.

Requests will typically be processed within five business days. After the request has been processed, the security certificate (one per server) will be placed in the appropriate site folder on the Imaging FTP server and the originators of the request will be notified.

Each security certificate received will need to be copied to the local server where the VIX software is installed. The VIX installation wizard will prompt you for this certificate during the installation process.

Java Version

Validate the with the specific patch description document for the current version of Java. If the server has a different version of Java than the required version specified in patch description, please uninstall the application.

New VIX Installation – Cluster

Use the following steps to install a VIX on a clustered server for the first time.

Note The VIX cannot be installed on the same machine as the HDIG.

Installation should take 30-60 minutes assuming that all preparation steps are complete. Administrator-level access to the clustered server is presumed.

Note Only perform the steps in this section if you are installing the VIX on a clustered server. If you are installing the VIX on a standalone server, see the *New VIX Installation – Standalone Server* section.

Scheduling Downtime for Resource Group Moves

You will need to schedule downtime with appropriate personnel for the duration of the VIX installation.

WARNING: You will need to move the Imaging resources group from one server node to another as part of installing the VIX. To prevent issues with image acquisition, stop DICOM image processing on Image Gateways for the duration of the VIX install.

Preparing Passwords and Staging Files

Before starting the VIX installation process on a clustered server, do the following:

1. Prepare a password to be used for the Apache Tomcat administrator account that will be created as part of the VIX installation process.

   ▪ This account will be rarely used; it only needs to be secured properly.

   ▪ The password is case-sensitive and only alphanumeric characters are allowed.

2. Prepare a password for the Windows account that will be created as part of the VIX installation process.

- This Windows account, which will be named "apachetomcat" when it is created by the VIX installer, is used to run the VIX in the Tomcat environment. This account is limited to only the functions it needs to run the VIX.

- The password is case sensitive, must contain at least eight characters, and must contain at least one capital letter and one number.

3. Set up a service account in VistA for ROI periodic processing with the MAG DICOM VISA secondary menu option and the OR CPRS GUI CHART secondary menu option. The service account may be the same service account as the one the DICOM Gateway and the HDIG use. The credentials are required for the VIX to process ROI disclosure requests periodically, in the background and to purge completed requests.

4. Determine the email address or addresses for notification about invalid ROI periodic processing credentials. The VIX will send an email notification to the email address or addresses, if the ROI periodic processing credentials are invalid or have expired. You must specify this address when you install the VIX. You can set up a new email account for this purpose or use an existing one.

5. Copy the VIX security certificates to both primary hard drives (usually drive C) on each server where the VIX will be installed.

Clustered Server Installation

To install the VIX on the primary cluster node

1. Verify that DICOM image processing on all DICOM Gateways has been stopped.

2. Copy the latest VIX installer (`MAG3_0P<number>_VIX_Setup.msi`) to both nodes in the cluster.

3. Use an administrator-level account to log on to the active node of the cluster (that is, the server that currently owns the group used for Imaging resources).

4. Do the following to prepare the VIX Installation Wizard:

   a. Double-click the VIX installation file.

   b. When the Welcome page displays, click **Next**.

   c. When the Confirm Installation page displays, click **Next**.

   d. When the Installation Complete screen displays, click **Close**

5. Choose **Start | All Programs | VistA Imaging Programs | VIX Installation Service Wizard**.

6. In the Welcome page for the VIX installation wizard, click **Next**.

7. In the **Site Number** field of the Specify the VA site…page, enter the STATION NUMBER (field (#99) in the INSTITUTION file (#4)) of your site. Then, click **Lookup Server Addresses**.

8. Verify that the site-related information retrieved by the lookup is correct. Then, click **Next**.

   Note: The VIX server hostname will be blank and the port number will be 0; these values are populated automatically once the VIX is registered with the VistA site service.

9. When the Prerequisites page displays, verify that the icons for the first two items on the page are ✅.

   ▪ **<account> has Administrator role –** This check verifies that an administrative account is being used. If not, cancel the installation and restart it using a Windows administrator account.

   ▪ **Current operating system –** This check verifies that the proper operating system is present. If a non-supported operating system is identified, installation cannot continue.

10. On the same page, check the line that indicates the state of the Java Runtime environment. If ❌ is shown, do the following:

   a. Click **Install**.

   b. Wait until the status icon the Java Runtime Environment changes to ✅.

11. On the same page, check the line that indicates the state of the Apache Tomcat installation. If ❌ is shown, do the following:

   a. Click **Install**.

   b. In the dialog box that displays, enter the and confirm the Apache Tomcat password that you prepared as described in *Preparing Passwords and Staging Files* previously. Then, click **OK**.

   c. Wait until the status icon for Apache Tomcat changes to ✅.

12. On the same page, check the line that indicates the state of the Laurel Bridge toolkit. If ❌ is shown, do the following:

   a. Click the **Install** button next to the Laurel Bridge item. After a brief delay, the Activate DCF License window will open.

   Tip: The Network Activation tab will be selected automatically, and about half of the boxes in the window will be pre-populated.

   b. Enter all of the following information in the Network Activation tab:

> **Note:** The **Activate** button will be disabled if any of the following boxes are left blank.
>
> - **Product Serial Number** – the new Laurel Bridge DCF serial number (include dashes).
> - **Site** – the name of your site.
> - **CPUs** – the number of CPUs on the server hosting the VIX.
> - **Contact name and Contact email** – the administrator of your local VistA Imaging system.

   c. Near the bottom of the window, click **Activate**. After a brief delay, the Status box will display a green "Success" message.

   d. **Click Exit with success**. The Activate DCF License window will close and the updated Laurel Bridge toolkit will be installed (installation will only take a second or two).

13. On the same page, check the line that indicates the state of the service account. If is shown, do the following:

   a. Click **Create**.

   b. In the dialog box that displays, enter the Windows service account password that you prepared as described in in *Preparing Passwords and Staging Files* previously. Then, click **OK**.

   c. Wait until the status icon for the service account changes to .

14. On the same page, check the line that indicates the state of VIX security certificate. If is shown, do the following:

   a. Click **Install**.

   b. In the dialog box that displays, click **Select**.

   c. Specify the location of the security certificate setup file received from the national VistA Imaging team. Then, click **OK**.

15. In the Install the VIX Prerequisites page, confirm that all the icons are . Then, click **Next**.

16. In the Specify the location... page, select the drive where you want the VIX configuration files to reside. Then, click **Create**.

- In most cases, you should use the same drive for the VIX configuration files and for the cache.
- The drive must be accessible to all servers in the cluster.

17. In the same page, select the drive where the VIX cache will be located. Then, click **Create**.

18. Click **Next**.

19. In the Specify the Release of Information (ROI) Configuration, do the following:

   ▪ Specify the access and verify codes for the account with the ROI periodic processing credentials. The VIX uses this account for periodic processing of ROI disclosure requests. The account must be valid VistA credentials with the MAG DICOM VISA secondary menu option and the OR CPRS GUI CHART secondary menu option. The credentials can be the credentials of the same service account that the DICOM Gateway and the HDIG use.

   ▪ Specify the email address that gets notifications for invalid ROI periodic processing credentials. The VIX sends an email notification to the address or addresses specified in this field if the ROI periodic processing credentials are expired or invalid. You can enter several addresses, separated by a comma.

   For more information about the service account for ROI periodic processing and the email address for invalid or expired ROI periodic processing credentials, see *Preparing Passwords and Staging Files.*

20. Click **Validate**.

   The VIX installation program checks the information. If it detects an error, it displays a tooltip with information about the error. When it validates the configuration, **Next** becomes available.

21. Click **Next**.

22. In the Configure local DoD connection page, do one of the following:

   ▪ If your site does not have a local connection to a DoD facility, click **Next** (this will be the case at most VA sites).

   ▪ If your site has a local network connection to a DoD facility, you can enter connection information for the DoD's PACS integrator server. After entering the connection information, click **Validate** to test the connection. Then, click **Next**.

23. In the Install the VIX page, click **Install**. (The information in this page is saved in `C:\Program Filesx86\VistA\Imaging\ViX Installer` for future reference or troubleshooting.)

24. When the following message box displays, click **OK** to continue.

Clustered VIX - Additional action required

You have installed the VIX service on the first server in the cluster. Your next step is to use Cluster Administrator Move Group command to transfer the Imaging Resources group to the second server and repeat the VIX installation.

OK
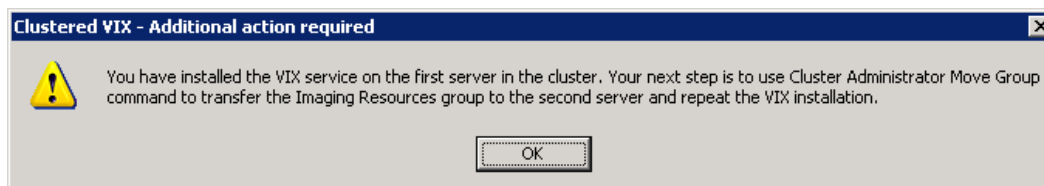
25. When installation is complete, click **Finish** to exit the wizard.

To install the VIX on the second cluster node

1. After installation on the first cluster node is complete, move the Imaging resources group to the second node. For operating system-specific steps, see page 43.

2. Log on to the second node as an administrator.

3. Execute the VIX installation wizard as described in steps 3 – 23 previously.

> **Note:** When you install the VIX on the second node, the pages in the wizard will be pre-populated based on what was specified for the primary node. Do not change the pre-populated values.

4. After installation is complete, move the Imaging resources group back to the first node.

5. At this point, normal Imaging operations (including DICOM Image Gateway processing) can resume; however, you need to perform additional cluster configuration steps for the VIX. See the next set of steps for details.

Creating the VIX Resource

After the VIX is installed on both nodes of the cluster, you will need to create a resource for the VIX and add that resource to the group used for other Imaging resources. This will allow the VIX to fail over onto the other node in the cluster the same way pre-existing Imaging resources will.

1. On the cluster server where the VIX was installed, start the Failover Cluster Manager (click **Start | All Programs | Administrative Tools | Failover Cluster Manage**r).

2. On the left side of the window, under Services and Applications, select the service used to manage Imaging resources. In most cases, the name of this service will be the cluster name followed by "a".
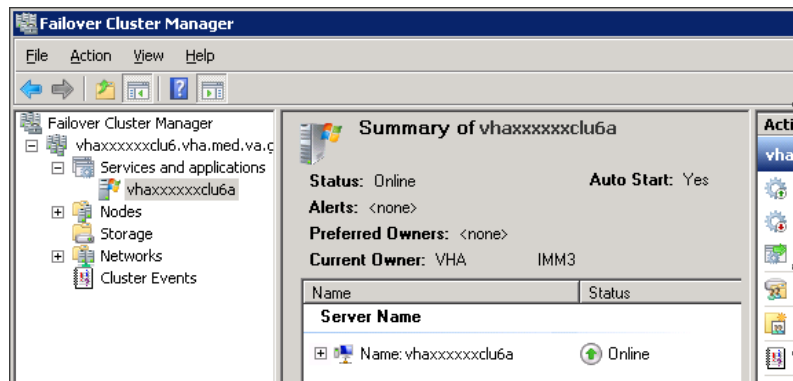
3. On the far right side of the window, click **Add** a resource. Then, click **4 – Generic Service**.

4. Wait until the first page in the New Resource Wizard populates. Then click the **Apache Tomcat** item at the top of the list.

5. Click **Next** twice. (There are no selectable items on the next two wizard pages.)

6. Click **Finish**. The wizard will close and the new Apache Tomcat resource will display under Other Resources in the Failover Cluster Manager window.

7. Right-click the Apache Tomcat resource and click **Properties**.

8. In the dialog box that opens, click the **General** tab. Then change the **Resource Name** to VIX.

9. Click the Dependencies tab and click the empty row in the Resource area. Then select the drive where the VIX configuration files were installed.

10. In the next (blank) row that appears, set the AND/OR column to AND. Then, set the Resource column to the name of the service that owns the resource (usually this will be the cluster name followed by "a").
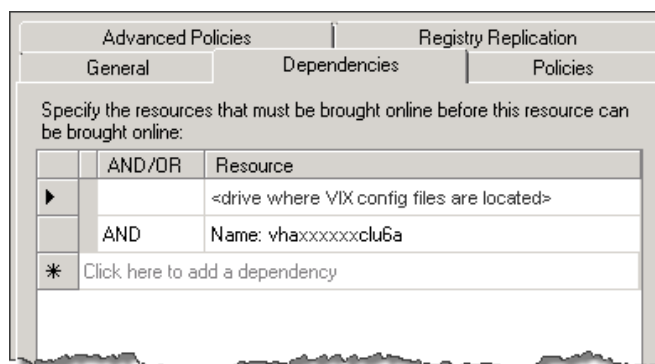
> **Note:** If the VIX cache is on a different drive than the VIX configuration files, add the VIX cache drive as an additional resource as well. Also set the AND/OR condition for the VIX cache drive to AND.

11. Click the **Policies** tab. Under the second option, set the Period for restarts to 15 minutes and set Maximum restarts to 10.

12. In the same tab, clear the checkbox for **If restart is unsuccessful, fail over all resources in this service or application**.
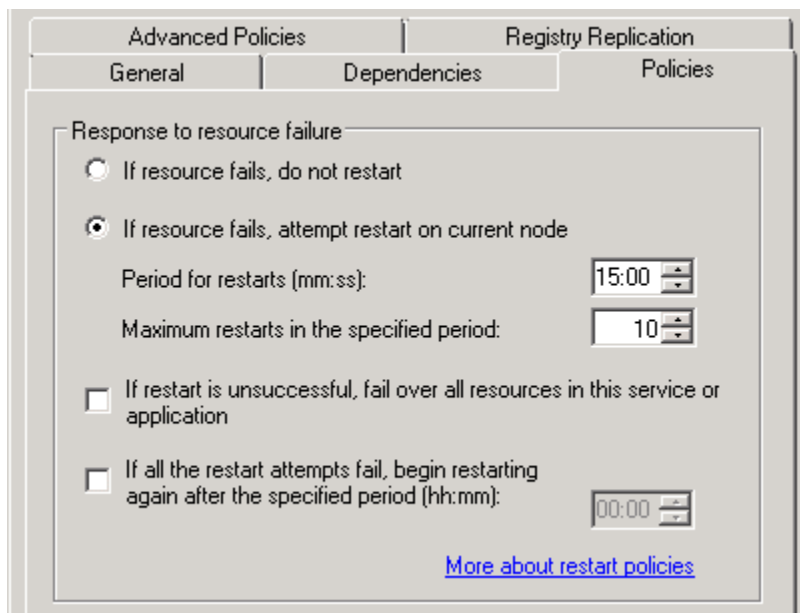
13. Click **OK** to accept the new settings and to close the Properties dialog box.

14. Near the middle of the Failover Cluster Manager window, under Other Resources, right-click the VIX resource and select **Bring this resource online**.

15. At this point, the VIX is fully installed. However, it cannot be used until it is activated and registered with the VistA Site Service. See *Preparing Passwords and Staging Files* in the following section.

New VIX Installation – Standalone Server

Use the following steps to install a VIX on a standalone server for the first time. Installation should take less than 30 minutes assuming that all preparation steps in previous sections are complete.

Note   Only perform the steps in this section if you are installing the VIX on a single server. If you are installing the VIX on a clustered server, see the *New VIX Installation – Cluster* section in this document.

Preparing Passwords and Staging Files

Before starting the VIX installation process on a standalone server, do the following:

1. Prepare a password to be used for the Apache Tomcat administrator account that will be created as part of the VIX installation process.

   ▪ This account will be rarely used; it only needs to be secured properly.

   ▪ The password is case-sensitive and only alphanumeric characters are allowed.

2. Prepare a password for the Windows account that will be created as part of the VIX installation process.

   ▪ This Windows account, which will be named "apachetomcat" when it is created by the VIX installer, is used to run the VIX in the Tomcat environment. This account is limited to only the functions it needs to run the VIX.

   ▪ The password is case sensitive, must contain at least eight characters, and must contain at least one capital letter and one number.

3. Set up a service account in VistA for ROI periodic processing with the MAG DICOM VISA secondary menu option and the OR CPRS GUI CHART secondary menu option. The service account may be the same service account as the one the DICOM Gateway and the HDIG use. The credentials are required for the VIX to process ROI disclosure requests periodically, in the background and to purge completed requests.

4. Determine the email address or addresses for notification about invalid ROI periodic processing credentials. The VIX will send an email notification to the email address or addresses, if the ROI periodic processing credentials are invalid or have expired. You must specify this address when you install the VIX. You can set up a new email account for this purpose or use an existing one.

5. Copy the VIX security certificates to both primary hard drives (usually drive C) on each server where the VIX will be installed.

6. Copy the VIX security certificate to the primary drive (usually the C drive) of the server where the VIX will be installed.

Standalone Server Installation

VIX installation involves running two processes back-to-back. The first short process installs the VIX Installation Wizard. The second, longer process involves using the VIX Installation Wizard to install the actual VIX.

Note: These steps presume that you have already obtained a serial number for the Laurel Bridge DCF toolkit. These steps also presume the VIX can access the Laurel Bridge license server via the internet.

To install the VIX on a standalone server

1. Use an administrator-level account to log on to the standalone server where the VIX will be installed.

2. Copy the VIX installation file (`MAG3_0P<number>_VIX_Setup.msi`) to a local folder on the server.

3. Do the following to prepare the VIX Installation Wizard:

   a. Double-click the VIX installation file.

   b. When the Welcome page displays, click **Next**.

   c. When the Confirm Installation page displays, click **Next**.

   d. When the Installation Complete screen displays, click **Close**.

4. Choose **Start | All Programs | VistA Imaging Programs | VIX Installation Service Wizard**.

5. When the Welcome page for the VIX installation wizard displays, click **Next**.

6. In the **Site Number** field of the Specify the VA site... page, enter the STATION NUMBER (field (#99) in the INSTITUTION file (#4)) of your site. Then, click **Lookup Server Addresses**.

7. Verify that the site-related information retrieved by the lookup is correct. Then, click **Next**.

   Note: The VIX server hostname will be blank and the port number will be 0; these values are populated automatically once the VIX is registered with the VistA site service.

8. When the Install the VIX Prerequisites page displays, verify that the icons for the first two items on the page are ✅.

   ▪ **<account> has Administrator role –** This line will indicate if an administrative account is being used. If not, cancel the installation and restart it using a Windows administrator account.

   ▪ **Current operating system –** This line will indicate if the proper operating system is present. If a non-supported operating system is identified, the installation cannot continue.

9. On the same page, check the line that indicates the state of the Java Runtime environment. If ❌ is shown, do the following:
   a. Click **Install**.

   b. Wait until the status icon the Java Runtime Environment changes to ✅.

10. On the same page, check the line that indicates the state of the Apache Tomcat installation. If ❌ is shown, do the following:

    a. Click **Install**.

    b. In the dialog box that displays, enter the and confirm the Apache Tomcat password that you prepared as described in *Preparing Passwords and Staging Files* previously. Then, click **OK**.

    c. Wait until the status icon for Apache Tomcat changes to ✅.

11. On the same page, check the line that indicates the state of the Laurel Bridge toolkit. If ❌ is shown, do the following:

    a. Click the **Install** button next to the Laurel Bridge item. After a brief delay, the Activate DCF License window will open.

       Tip: The Network Activation tab will be selected automatically, and about half of the boxes in the window will be pre-populated.

    b. Enter all of the following information in the Network Activation tab:

       Note: The Activate button will be disabled if any of the following boxes are left blank.

       - **Product Serial Number** – the new Laurel Bridge DCF serial number (include dashes).

       - **Site** – the name of your site.

       - **CPUs** – the number of CPUs on the server hosting the VIX.

       - **Contact name** and **Contact email** – the administrator of your local VistA Imaging system.

    c. Near the bottom of the window, click **Activate**. After a brief delay, the **Status** box will display a green "Success" message.

    d. Click **Exit with success**. The Activate DCF License window will close and the updated Laurel Bridge toolkit will be installed (installation will only take a second or two).

12. On the same page, check the line that indicates the state of the service account. If ❌ is shown, do the following:

    a. Click **Create**.

    b. In the dialog box that displays, enter the Windows service account password that you prepared as described in *Preparing Passwords and Staging Files* previously. Then, click **OK**.

   c. Wait until the status icon for the service account changes to ✅.

13. On the same page, check the line that indicates the state of VIX security certificate. If ❌ is shown, do the following:

   a. Click **Install**.

   b. In the dialog box that displays, click **Select**.

   c. Specify the location of the security certificate setup file received from the national VistA Imaging team. Then, click **OK.**

14. In the Install the VIX Prerequisites page, confirm that all the icons are ✅. Then, click **Next**.

15. In the Specify the location... page, select the drive where you want the VIX configuration files to reside. Then, click **Create**.

   ▪ In most cases, you should use the same drive for the VIX configuration files and for the VIX cache.

   ▪ If you have only one drive available, it will be pre-selected.

16. In the same page, select the drive where the VIX cache will be located. Then, click **Create**.

17. Click **Next**.

18. In the Specify the Release of Information (ROI) Configuration, do the following:

   ▪ Specify the access and verify codes for the account with the ROI periodic processing credentials. The VIX uses this account for periodic processing of ROI disclosure requests. The account must be valid VistA credentials with the MAG DICOM VISA secondary menu option and the OR CPRS GUI CHART secondary menu option. The credentials can be the credentials of the same service account that the DICOM Gateway and the HDIG use.

   ▪ Specify the email address that gets notifications for invalid ROI periodic processing credentials. The VIX sends an email notification to the address or addresses specified in this field if the ROI periodic processing credentials are expired or invalid. You can enter several addresses, separated by a comma.

   For more information about the service account for ROI periodic processing and the email address for invalid or expired ROI periodic processing credentials, see *Preparing Passwords and Staging Files.*

19. Click **Validate**.

   The VIX installation program checks the information. If it detects an error, it displays a tooltip with information about the error. When it validates the configuration, **Next** becomes available.

20. Click **Next**.

21. In the Configure Local DoD connection page, do one of the following:

    ▪ If your site has no local network connection to a DoD facility, click **Next** (this will be the case at most VA sites).

    ▪ If your site has a local network connection to a DoD facility, enter connection information for the DoD's PACS Integrator server. After entering the connection information, click **Validate** to test the connection. Then, click **Next**.

22. In the Install the VIX page, click **Install**. (The information in this page is saved in `C:\Program Filesx86\VistA\Imaging\ViX Installer` for future reference or troubleshooting.)

23. When installation is complete, click **Finish** to exit the wizard.

24. The VIX will start automatically, but cannot be used until it is activated and registered with the VistA Site Service. See the next section for details.

Verifying Installation Is Complete

After you have run the VIX Installation Wizard, verify that your installation is complete. Follow these steps:

1. Go to the VIX homepage: http://<fully qualified name of VIX server>:8080/

2. The current version is listed in the format XX.XXX.X.X. The first two digits represent Version 3.0 of the VistA Imaging system and do not change. The next three digits are the number of the latest patch that has affected the VIX. This patch number should match the number of the VIX component you have most recently installed.
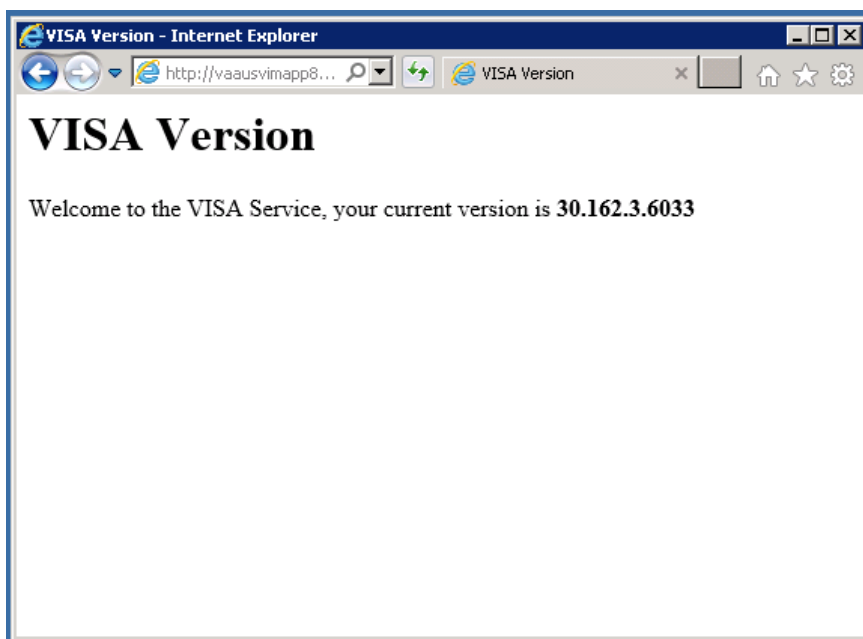
Activating a New VIX

After the VIX is installed, it will be inactive until it is registered with the VistA Site Service. Clinical Display workstations and VistARad workstations use the site service to determine if local and remote VIX servers are available.

After the VIX is registered in the site service, the VIX will begin to be actively used, both by clinicians at your site as well as by remote VA sites for access to locally stored images.

Note: Do not register the VIX with the site service until after it is installed. Registering the VIX before it is installed will cause errors and timeout issues for Clinical Display users.

To register the VIX

1. Gather the following information:

   Primary contact name, phone, and email:

   Backup contact name, phone, and email:

   Site name:

STATION NUMBER (field #99) from INSTITUTION file (#4):

Network Name defined for Imaging Resources group[*]**:**

For clustered servers only:

    Server node 1 name:

    Server node 2 name:

2. E-mail this information to VHAVIVIXSETUP@VA.GOV.

   ▪ Paste the lines in the preceding step into the email message.

   ▪ Use "Add VIX server to Site Service database" as the email title.

3. You will be notified, typically within five business days, when the site service registration is complete.

4. Verify that the VIX is running as described in *Verifying VIX Operations* on page 26.

---

[*] In Windows 2003 Cluster Administrator, the network name is shown on the right side of the window when the Imaging Resources group is selected. In Windows 2008 Failover Cluster Manager, the network name of the Imaging Resources group is shown by default on the left side of the window under Services and Applications.

Updating an Existing VIX

This chapter explains how to update an existing VIX server. An installation checklist that summarizes this process is on page 40.

Preparing for a VIX Update

Preparing for a VIX update involves:

- Making sure that the KIDS version installed on the VistA system matches the version the VIX requires.

- Scheduling downtime and notifying users of the impact of a VIX update.

  Tip: Aware licenses (used for DICOM-to-JPEG2000 conversion on the VIX) established for older VIXes will automatically carry over to new VIXes.

  Tip: VIX-specific account passwords and security key assignments established for older VIXes will automatically carry over to new VIXes.

VistA Software Dependencies

The VIX server software requires that a compatible Imaging KIDS package be installed on VistA. For details about the compatible KIDS package and installing it, see the patch description of the specific patch.

Scheduling Downtime and Impact of a VIX Update

You will need to schedule downtime with appropriate personnel for the duration of the VIX installation.

  WARNING: If the VIX is installed on the clustered server used to manage Imaging shares/RAID storage, the Imaging resource group will have to be transferred between server nodes as a part of the VIX installation. Because of this, DICOM image acquisition must be suspended for the duration of the VIX install (about 30 minutes).

  Note: If a VIX is installed on a standalone (dedicated) server, the DICOM image acquisition is not impacted and can continue.

  While the VIX server is being updated, VIX assisted functions will not be available. The following table summarizes how a VIX outage will affect clinicians:

Java Version

Validate the specific patch description document for the current version of Java. If the server has a different version of Java than the required version specified in patch description, please uninstall the application.

Clinical Group	Impact
Local Clinical Display users	DoD images will not be accessible for the duration of the VIX shutdown.
	Remote VA images may be temporarily inaccessible. Clinical Display will attempt to revert to pre-VIX remote image views, but users may have to disconnect from and reconnect to remote sites, or in some cases, restart Clinical Display.
	Clinicians may notice longer retrieval times for remote images for the duration of the VIX shutdown.
	After the VIX is restarted, restart Clinical Display to make sure that Clinical Display is no longer using pre-VIX remote image views for remote sites.
Local VistARad users	Remote exam data and monitored exam lists will not be available. For additional information, refer to the documentation for VistARad.
Remote VA or DoD clinicians requesting your site's images	Remote clinicians may experience transitory application errors if the VIX is shut down while it is in the middle of processing a request; the clinician may have to repeat the request.
	Remote VA clinicians issuing new requests may notice longer retrieval times for the duration of the VIX shutdown.
	Remote DoD clinicians will not be able to retrieve locally stored images for the duration of the VIX shutdown.

Performing a VIX Update – Cluster

Use the following steps to update a VIX on a clustered server. Typically, the update process will take less than 30 minutes assuming that all activities described in the *Preparing for a VIX Update* section of this document are complete.

1. Verify that DICOM Image processing on all DICOM Gateways has been stopped.

2. Go to the Control Panel, choose Add/Remove Programs, and remove the current version of the VIX instance.

3. Copy the latest VIX installer (`MAG3_0P<number>_VIX_Setup.msi`) to both nodes in the cluster.

4. Use an administrator-level account to log onto the cluster node where the VIX service is active (i.e., the server that owns the Imaging resources group).

5. Take the VIX service offline. For operating system-specific steps, see page **Error! Bookmark not defined.**.

6. Do the following to prepare the VIX Installation Wizard:

    a. Double-click the VIX installation file.

    b. When the Welcome page displays, click **Next**.

    c. When the Confirm Installation page displays, click **Next**.

    d. When the Installation Complete screen displays, click **Close**.

7. Choose **Start | All Programs | VistA Imaging Programs | VIX Installation Service Wizard**.

8. When the Welcome page displays, click **Next**. Then, when you are prompted to do so, uninstall the pre-existing VIX software.

9. When the Uninstall complete message displays near the top of the page, click **Next**.

10. In the **Site Number** field of the Specify the VA Site... page, verify that the **Site Number** box shows your STATION NUMBER (field (#99) in the INSTITUTION file (#4)).

11. Confirm the connection by clicking **Lookup Server Address**. Then click **Next**.

12. In the Install the VIX Prerequisites page, check the status of each item on the page. As this is a VIX update, most or all of the prerequisites will already be present.

13. In the VIX Prerequisites page, if all prerequisites are already installed, click **Next**. Then click **Next** three more times to accept defaults in the following three pages.

14. Click **Install** when the Install the VIX page displays.

15. After installation on the first cluster node is complete, move the Imaging resources group to the second node. For operating system-specific steps, see page 43.

16. Repeat steps 4 – 17 on the second cluster node.

17. After the VIX is updated on both nodes, move the Imaging resources group back to the first node in the cluster.

18. Bring the VIX resource back online. For operating system-specific steps, see page 43.

19. At this point, the VIX will be up and running, and normal Imaging operations can resume. Optionally, perform the steps on page 26 to verify VIX operations.

Performing a VIX Update – Standalone Server

Use the following steps to update a VIX on a standalone server. Typically, the update process will take 10 minutes or less assuming that all preparations described in the *Preparing for a VIX Update* section of this document are complete.

Note: These steps presume that you have already obtained a new Laurel Bridge DCF toolkit serial number. These steps also presume the VIX can access the Laurel Bridge license server via the internet.

1. Go to the Control Panel, choose Add/Remove Programs, and remove the current version of the VIX instance.

2. Use an administrator-level account to log on to the standalone server where the VIX will be installed.

3. Copy the VIX installation file (`MAG3_0P<number>_VIX_Setup.msi`) to a local folder on the server.

4. Do the following to prepare the VIX Installation Wizard:

   a. Double-click the VIX installation file.

   b. When the Welcome page displays, click **Next**.

   c. When the Confirm Installation page displays, click **Next**.

   d. When the Installation Complete screen displays, click **Close**.

5. Choose **Start | All Programs | VistA Imaging Programs | VIX Installation Service Wizard**.

6. When the Welcome page displays, click **Next**. Then, when you are prompted to do so, uninstall the pre-existing VIX software. (The wizard will gracefully stop the VIX service before performing the uninstall.)

7. When the Uninstall complete message displays near the top of the page, click **Next**.

8. In the **Site Number** field of the Specify the VA Site... page, verify that the **Site Number** box shows your STATION NUMBER (field (#99) in the INSTITUTION file (#4)).

9. Confirm the connection by clicking **Lookup Server Address**. Then click **Next**.

10. In the VIX Prerequisites page, if all prerequisites are already installed, click **Next**. Then click **Next** three more times to accept defaults in the following three pages.

11. In the VIX Prerequisites page, if all prerequisites are already installed, click **Next**. Then click **Next** twice more to accept defaults in the next two pages.

12. Click **Install** when the Install the VIX page displays. The VIX will start automatically when installation is complete.

13. Click **Finish**. The VIX Installation Wizard will close.

14. At this point, the VIX will be up and running. Optionally, perform the steps in the *Verifying VIX Operations* section to verify VIX operations.

Post-installation

Verifying VIX Operations

After a new VIX is installed and is registered with the Image Exchange Service, Clinical Display (MAG*3.0*93 or later) and VistARad (MAG*3.0*90 or later) workstations will automatically start using the VIX.

- Clinical Display will begin sending all of its requests for remote data to the VIX immediately. No configuration changes are required for Clinical Display to start using the VIX.

- VistARad will need some local configuration changes to enable some of its VIX-supported capabilities; refer to the VistARad documentation for details.

Verifying Access to the VIX Transaction Log

VIX administrators can use the VIX transaction log to monitor VIX activities. If the transaction log can be accessed, the VIX is running.

To access the transaction log you will need:

- A VistA account that has the MAG VIX ADMIN security key assigned to it (while the log is a Web page, the VIX uses a VistA account to secure the log).

- Access to http://<FQDN>:8080/Vix/secure/VixLog.jsp
  (Where <FQDN> is either the fully qualified domain name of the cluster the VIX is installed on, or in the case of single server installations, the server the VIX is installed on.)

If you cannot access the transaction log, verify that the VIX service is running as described in the *Bringing the VIX Online* section.

If the VIX is running but you cannot access the transaction log, ensure that port 8080 on the VIX server is not blocked. Possible culprits of a blocked port include antivirus firewalls and modifications to ACLs (Access Control Lists).

For detailed information about the contents of the transaction log, refer to the *VIX Administrator's Guide*.

You can also spot-check individual remote images to see if they were delivered via the VIX as described in this section.

Spot-checking VIX Image Delivery

1. On the Clinical Display workstation, select a patient with remote images.

2. If it is not visible already, display the Abstracts area to display an abstract for one of the remote images.

3. Right-click the abstract for the remote image and open the Image Information window.

4. In the Image Information window, check the IEN (Internal Entry Number) value. If the value starts with "urn", the remote image was retrieved by the VIX.

Using the VIX Installation Wizard to Reconfigure the VIX

You will need to re-execute the VIX Installation wizard if you need to:

- Change the drive where the VixCache or VixConfig folders are located. It is recommended that these folders reside on the same shared drive.

- Change the VIX configuration to use a different local VistA host name or port number.

Using the VIX Installation wizard is broadly similar to the steps for updating a VIX, except the process is much faster since no actual software is being installed.

Note: The following steps that new cache location is set up and/or that the local VistA database connection change has already been made.

Tip: Changing a VIX cache location or local connection information should take 10-15 minutes for a clustered VIX assuming no issues are encountered. For a VIX installed on a standalone server, this process should take about 5 minutes.

Reconfiguring a VIX – Cluster

1. Review the information in the *Scheduling Downtime and Impact of a VIX Update* section, and schedule downtime and notify appropriate groups of the downtime.

2. Take the VIX resource offline. For specific steps, see the *Taking a VIX Offline* section in this document.

3. If you are moving the location of the VixConfig folder, copy the folder from the old location to the new location. This will preserve the transaction log files that were previously created.

4. Use an administrator-level account to log into the cluster node that owns the VIX resource. Then choose **Start | All Programs | VistA Imaging Programs | VIX Installation Service Wizard**.

5. Click **Next** until the Specify the VA Site... page displays.

6. In this page, verify that the **Site Number** box shows your STATION NUMBER (field (#99) in the INSTITUTION file (#4)). Then click **Lookup Server Address**.

7. Verify that the correct hostname and port number for the local VistA system is displayed. Then click **Next**.

8. When the Install the VIX Prerequisites page displays, click **Next**. (All prerequisites are installed already).

9. In the Specify the location... page, do one of the following:

    ▪ If you are changing the location of the VIX cache and configuration files, select the new drive for each (the same drive should be used). Then, click **Create**. Then, click **Next**.

    ▪ If you are NOT changing the location of the VIX cache and configuration files, click **Next**.

10. In the Specify the Release of Information (ROI) Configuration, do the following:

    ▪ If you want to change any of the values, enter the new values. If you are changing the email address or addresses for invalid ROI periodic processing credentials notification, click **Validate**. If you do not want to change any of the values on this page, skip this step.

    ▪ Click **Next**.

11. In the Configure local DoD connection page, click **Next**.

12. In the Install the VIX page, click **Install**.

13. When the following message box displays, click **OK** to continue.
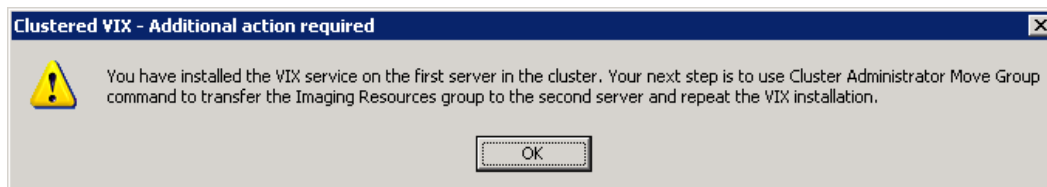
14. When installation on the first node is complete, click **Finish** to exit the wizard.

15. Move the Imaging resources group to the other node on the cluster. For operating system-specific steps, see the *Moving Imaging Resources to a Different Node* section of this document.

16. Log on to the second cluster node as an administrator.

17. Execute the VIX installation wizard as described in steps 2 – 11 previously.

Note: When you install the VIX on the second node, the pages in the wizard will be pre-populated based on what was specified for the primary node. Do not change the pre-populated values.

18. After installation is complete, move the Imaging resources group back to the first node.

19. At this point, normal Imaging operations (including DICOM Image Gateway processing) can resume.

Reconfiguring a VIX – Standalone Server

1. Review the information in the *Scheduling Downtime and Impact of a VIX Update* section, and schedule downtime and notify appropriate groups of the downtime.

2. Log in as an administrator on the server where the VIX is installed and choose **Start | All Programs | VistA Imaging Programs | VIX Installation Service Wizard**.

3. Click **Next** until the Specify the VA Site... page displays.

4. In this page, verify that the **Site Number** box shows your STATION NUMBER (field (#99) in the INSTITUTION file (#4)). Then, click **Lookup Server Address**.

5. Verify that the correct hostname and port number for the local VistA system is displayed. Then, click **Next**.

6. When the Install the VIX Prerequisites page displays, click **Next**. (All prerequisites are installed already).

7. In the Specify the location... page, do one of the following:

   ▪ If you are changing the location of the VIX cache and configuration files, select the new drive for each (the same drive should be used). Then, click **Create**. Then, click **Next**.

   ▪ If you are NOT changing the location of the VIX cache and configuration files, click **Next**.

8. In the Specify the Release of Information (ROI) Configuration, do the following:

   ▪ If you want to change any of the values, enter the new values. If you are changing the email address or addresses for invalid ROI periodic processing credentials notification, click **Validate**. If you do not want to change any of the values on this page, skip this step.

   ▪ Click **Next**.

9. In the Configure local DoD connection page, click **Next**.

10. In the Install the VIX page, click **Install**.

11. Wait until the installation is complete and click **Finish**. The VIX will restart automatically.

Troubleshooting

Resuming an Interrupted VIX Installation

If you have had to interrupt or cancel an in-progress VIX installation, you can resume the installation.

Note: If you re-run `MAG3_0P<number>_VIX_Setup.msi`, you are repeating the installation of the VIX Installation Wizard software, not the installation of the VIX itself. If you do this, click Cancel, choose **Yes** when prompted for confirmation, and then exit the installer. Then restart the VIX installation.

Resuming Installation (clustered VIX)

1. Use an administrator-level account to log into the cluster node that owns the VIX resource.

2. Then click **Start | All Programs | VistA Imaging Programs | VIX Installation Wizard**.

3. Follow the steps for a first-time clustered VIX installation or for updating a clustered VIX .

   > **Tip:** If it is necessary to take the VIX resource offline, the VIX installation wizard will take care of this automatically.

Resuming Installation (single server VIX)

1. Log onto the VIX server as an administrator.

2. Click **Start | All Programs | VistA Imaging Programs | VIX Installation Wizard**.

3. Follow the steps for a first-time standalone VIX installation or for updating a standalone VIX.

VIX Support

If you encounter problems installing the VIX log a trouble ticket or call the National Service Desk at 1-888-596-4357.

This page is intentionally blank.

Back Out/Uninstall

Back Out/Uninstall Scenarios

The information in this section addresses three possible cases that involve uninstalling a VIX:

- Troubleshooting

- Relocation onto a different server

- Decommission

Each of these scenarios is outlined in the following sections.

Uninstall/Restore as part of Troubleshooting

If you need to remove and then immediately reinstall the VIX on the same server for troubleshooting purposes, you will need to do the following:

1. Locate the product serial number for the Laurel Bridge software that is bundled with the VIX. This number is in the license paperwork that was provided by VHAVILBLICENSES@VA.GOV when the VIX was set up.

   Note: You will need to re-enter this serial number as a part of the VIX installation process.

1. Choose **Start | All Programs | VistA Imaging Programs | VIX Installation Service Wizard**.
2. When the Welcome page displays, verify that the screen dispalys "This wizard will guide you through the installation of the Vista Imaging Patch 162 VIX and click Next.
3. Then, when you are prompted to do so, Click **Uninstall version 30.162.xx.x**. (The wizard will gracefully stop the VIX service before performing the uninstall.)

4. Go to the Control Panel, choose Add/Remove Programs, and remove the MAG*3.0*162 VIX instance.

5. Re-execute the VIX installation as if for a new VIX.

   - For clustered server reinstallation, see the *Preparing Passwords and Staging Files* section.

   WARNING: on a clustered server, installation will require taking Imaging resources offline briefly.

   - For standalone server reinstallation, see the *New VIX Installation – Standalone Server* section.

Relocating a VIX onto a New Server

If you need to remove all traces of the VIX from the old server and set up the VIX on a new server, you will need to do the following:

1. Contact the VHAVILBLICENSES@VA.GOV mail group and arrange to have the existing Laurel Bridge DCF toolkit licenses transferred to a new server.

2. Validate the new server where the VIX will be installed as described in the *Selecting and Validating the VIX Server* section.

3. Manually remove the VIX as described in the *Uninstalling the VIX* section below.

4. Re-execute the VIX installation as if for a new VIX.

   ▪ For standalone server reinstallation, see the *New VIX Installation – Standalone Server* section.

   ▪ For clustered server reinstallation, see the *New VIX Installation – Cluster* section.

Decommissioning a VIX

If a VIX to be completely decommissioned and not replaced by another VIX, do the following:

1. Notify the VHAVILBLICENSES@VA.GOV mail group that the Laurel Bridge license seats used by your site are no longer being used.

2. Contact VHAVIVIXSETUP@VA.GOV mail group to have the VIX security certificates retired and the VIX removed from the site service.

3. Manually remove the VIX as described in the *Uninstalling the VIX* section below.

4. In VistA, remove the MAG VIX ADMIN security key from the accounts that have this key assigned.

Uninstalling the VIX

The following steps explain how to completely remove a VIX and all its supporting components (toolkits, runtime environments, etc.) from the server where the VIX is installed.

These steps will completely remove the VIX and permanently delete the VIX cache.

Depending on the VIX server configuration and operating system, the specifics of removing the VIX will vary, but the general process is as follows:

1) Stop the VIX service. For clustered servers, also delete the VIX service/resource

2) Remove VIX-related applications, accounts, directories, and variables

If the VIX is being used on a clustered server, the second part this process needs to be repeated for each node in the cluster.

These steps do not require a server reboot, and can be performed while the rest of the Imaging system is active.

Stopping the VIX service

The steps for stopping the VIX service vary based on operating system. On clustered servers, the VIX resource also needs to be deleted

Cluster server: stop VIX service and remove VIX resource

1. On the cluster server where the VIX is installed, log in as a local administrator.

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

3. On the left side of the window, under Services and Applications, select the service used to manage Imaging resources. In most cases this will be named the cluster name followed by "a".
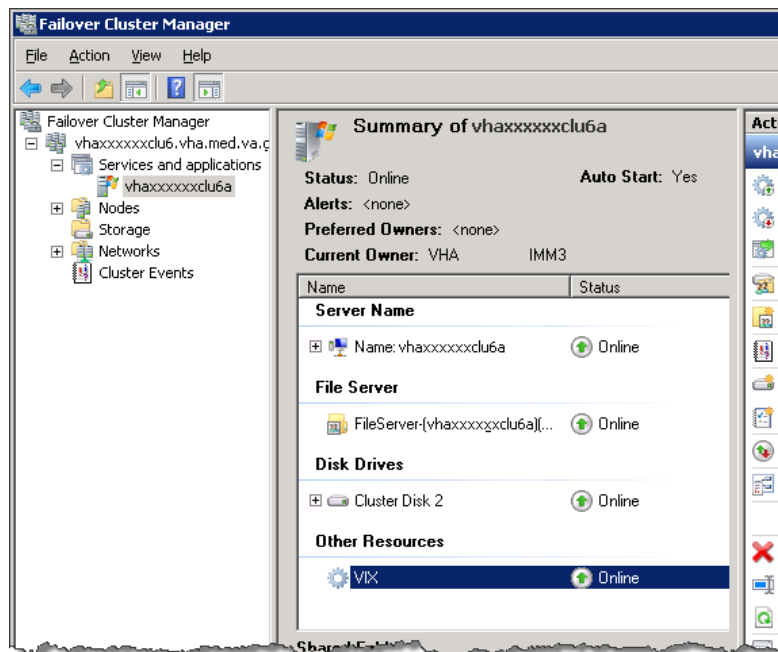
4. Near the middle of the window, under Other Resources, right-click the VIX resource and select **Take this resource offline**.

5. If you are asked for confirmation, click **Take VIX offline**.

6. Right-click the VIX resource again and click **Delete**. If you are asked for confirmation, click **Yes**.

7. Remove VIX-related applications, accounts, directories, and variables as described in the following sections.

Remove VIX-related applications, accounts, directories, and variables

After stopping (and/or removing) the VIX service as described in the previous sections, you will need to remove VIX software and settings.

These steps presume you are already logged in as an administrator on the server (or the active node, if the VIX is on a clustered server) where the VIX service used to reside.

These steps cover all supported VIX configurations.

1. Use Windows Explorer to navigate to the drive where the VIX Cache is located, and delete the following folders:

    <shared drive letter>\VixCache
    <shared drive letter>\VixConfig

2. Use Windows Explorer to delete the following directories:

    C:\ DCF_RunTime
    C:\Program Files\Java\jre1.6.0_xx

3. If you are removing the VIX permanently, also delete the following folders:

    SKIP THIS STEP if you are uninstalling and reinstalling the VIX on the same server for troubleshooting purposes. If you delete these folders, you will need to recreate the VIX configuration and request new VIX security certificates.

    <shared drive letter>\VixConfig
    C:\VixCertStore

4. Open the window used to remove programs.

    - On Windows click Start | Control Panel. Under the Programs item, click **Uninstall a program.**

    - Remove these three programs (no reboot required):

    Apache Tomcat 6.0
    Java (TM) 6 Update 45
    VIX Service Installation Wizard

5. In Windows Explorer, right-click the Local Disk (C:) folder, select **Properties**. Then, select the Security tab.

6. Select the `apachetomcat` user and click **Remove**.

7. Click **OK** to close the Properties dialog box, and click **Yes** when are asked if you want to continue.

   Note : If one or more "Error applying security" messages display, click **Continue** until they are all closed.

8. Open the Computer Management/Server Manager window.

   ▪ On Windows, right-click Computer on the desktop. Then, click **Manage**.

9. In the tree on the left side of the window, navigate to Users.

   ▪ On Windows , go to Server Manager/Configuration/ Local Users and Groups/Users.

10. In the right side of the window, right-click the `apachetomcat` user, click **Delete**, and click **Yes** when you are asked for confirmation.

11. Open the System Properties dialog box.

    ▪ On Windows, right-click Computer on the desktop. Then, click **Properties**. Then on the left side of the System window, click **Advanced system settings**.

12. In the Advanced tab, click **Environment Variables**.

13. In the System variables list near the bottom of the dialog, delete the following variables:

CATALINA_HOME	DCF_USER_CLASSES
DCF_BIN	DCF_USER_LIB
DCF_CFG	DCF_USER_ROOT
DCF_CLASSES	LD_LIBRARY_PATH
DCF_LIB	OMNI_BIN
DCF_LOG	OMNI_LIB
DCF_PLATFORM	OMNI_ROOT
DCF_ROOT	vixcache
DCF_TMP	vixconfig
DCF_USER_BIN	

14. In the System variables list, select the Path system variable. Then, click **Edit**.

15. In the Variable value box, delete the following substrings:

    C:\DCF (if present)
    C:\DCF_Runtime\bin

C:\DCF_Runtime\lib
C:\Program Files\Java\jre1.6.0_xx\bin

Note It is recommend that after deleting each substring you delete any extra semicolon characters.

16. After removing the substrings, click **OK**. Then click **OK** twice more to close the Environment Variables and System Properties dialog boxes.

17. If the VIX is installed on a clustered server, log into the non-active/secondary node on the cluster as an administrator. Then repeat all preceding steps except step 1.

18. If the VIX is installed on a standalone server, VIX removal is complete.

Appendix A: VIX Checklists

The checklist on this page summarizes the VIX update process. The checklist on the next page summarizes the process a new VIX install.

New VIX Install Checklist

VistA Setup

❑	Install the associated KIDS.
❑	Identify the users who need access to the VIX transaction log and assign the MAG VIX ADMIN key to their VistA accounts.

VIX Pre-Install

❑	Select and validate standalone or clustered server where the VIX will be installed (page 3).
❑	Get software licenses for Laurel Bridge DCF toolkit and Aware (page 4).
❑	Get security certificates (page 5).

VIX Install

❑	**Clustered servers only:** Schedule downtime to accommodate moving the Imaging resources group on the cluster (page 6).
❑	Prepare passwords needed by VIX installer and stage files needed for installation (page 6 for cluster, page 13 for standalone).
❑	Install the VIX (page 7 for cluster, page **Error! Bookmark not defined.** for standalone).
❑	**Clustered servers only:** Create the VIX resource (page 11).

VIX Post-Install

❑	Activate the VIX by registering it with the VistA Site Service (page 14).
❑	Verify proper operations (page 26).

VIX Update Checklist

VistA Setup

❑	Install the associated KIDS.

VIX Install

❑	**Clustered servers only:** Schedule downtime to accommodate moving the Imaging resources group on the cluster (page 22).
❑	Update the VIX (page 22 for cluster, page 24 for standalone).

VIX Post-Install

❑	Verify proper operations (page 26).
❑	Optional: Remove the VistA service account for DoD access.

Appendix B: VIX-related Cluster Operations

This information in this section explains how to do the following on a clustered server:

- Taking a VIX offline.
- Moving resources to a different cluster node (affects all Imaging resources as well as the VIX).
- Bringing the VIX online.

Note: The instructions in this section only apply to clustered VIX implementations. On standalone servers, the VIX service is turned on and off automatically as needed during the installation process.

Taking a VIX Offline

The following steps explain how to take the VIX offline on a clustered server in the context of a VIX installation.

When the VIX is offline:

- VistARad users will not be able to view remote images unless they log into the remote sites directly.
- Clinical Display users will not be able to view remote images from the DoD. Remote VA images can still be viewed, but performance will be reduced.
- DICOM Importer users will not be able to log into and use the client to import images or perform DICOM correction on HDIGs.

Taking a VIX Offline: Cluster

1. On the clustered server where the VIX is installed, log in as an administrator.

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

3. On the left side of the window, select the group used to manage VistA Imaging resources. (Usually the name of this group will be the cluster name followed by "a".)

4. Near the middle of the window, under Other Resources, right-click the VIX resource and select **Take this resource offline**.

5. If you are asked for confirmation, click **Take VIX offline**.

Moving Imaging Resources to a Different Node

The following steps explain how to move Imaging resources between nodes on a clustered server.

⚠️ Performing these steps affect all Imaging resources (i.e., the Imaging shares/RAID) as well as the VIX. These steps presume that applicable parties have been notified and that image acquisition on DICOM Image Gateways and Hybrid DICOM Image Gateways has been suspended.

These are to be performed only as part of a VIX installation. These steps assume that the cluster contains two nodes.

1. On the clustered server where the VIX is installed, log in as an administrator.

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

3. On the left side of the window, right-click the group used to manage VistA Imaging resources (usually the name of this group will be the cluster name followed by "a"). Then click **Move this service or application to another node | <secondary node name>**.

4. If you are asked for confirmation, choose the first option to confirm the operation.

5. After a brief delay, the Current Owner area near the middle of the window will update to show that the resources have been shifted to the other node in the cluster.
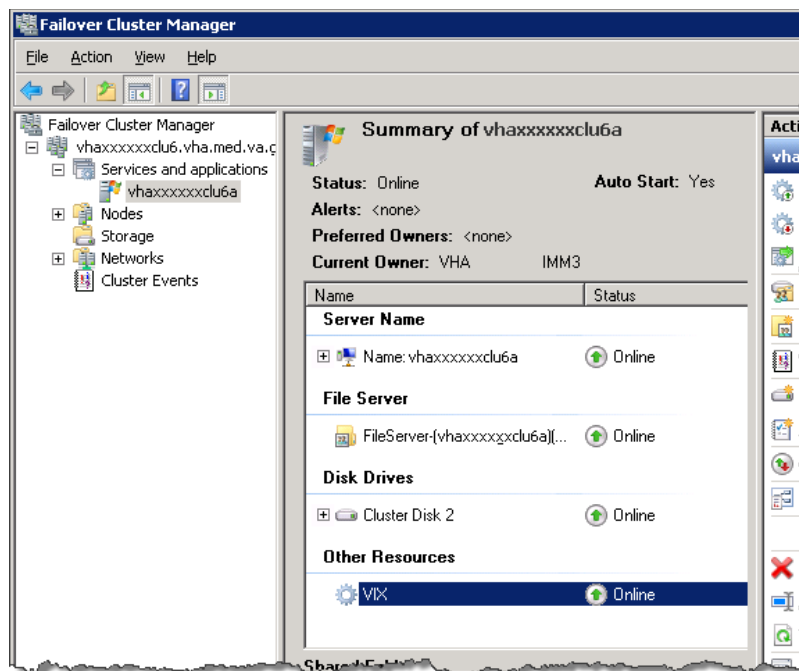
Bringing the VIX Online

The following steps explain how to bring the VIX back online in the context of a VIX installation.

▪ At sites where a pre-existing VIX is being updated, the VIX will automatically be used by Clinical Display and VistARad client applications as soon as the VIX goes back online.

▪ At sites where a new VIX is being implemented, the VIX will need to be activated before it is used. See the *New VIX Installation – Standalone Server* section of this document for details.

You can also use these steps to ensure that the VIX is running if there are any issues accessing the VIX transaction log.

1. On the clustered server where the VIX is installed, log in as an administrator.

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

3. On the left side of the window, select the group used to manage VistA Imaging resources. (Usually the name of this group will be the cluster name followed by "a".)

4. Near the middle of the window, under Other Resources, right-click the VIX resource and select **Bring this resource online**.

5. If you are asked for confirmation, click **Bring VIX online**.