VistA Imaging Exchange (VIX) Query Retrieve

MAG*3.0*269

VIX Installation Guide

June 2022

Version 43.4

Department of Veterans Affairs

Office of Information Technology (OIT)

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 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: https://www.va.gov/health/imaging/
VA intranet: REDACTED

Revision History

Date	Version	Description	Author
06/07/2022	43.4	Revisions to Service Account Settings Appendix.	VA IT VistA Imaging Technical team
06/03/2022	43.3	Updates for MAG*3.0*269 release date.	VA IT VistA Imaging Technical team
05/26/2022	43.2	Revisions to Installing a New VIX, Updating an Existing VIX, Post Installation Instructions, Troubleshooting, and Service Account Settings Appendix.	VA IT VistA Imaging Technical team
05/12/2022	43.1	Revisions to Installing a New VIX, Updating an Existing VIX, Post Installation Instructions, and Troubleshooting.	VA IT VistA Imaging Technical team
05/11/2022	43.0	Revisions to Service Account Settings Appendix.	VA IT VistA Imaging Technical team
05/10/2022	42.9	Revisions to Installing a New VIX, Updating an Existing VIX, and Post Installation Instructions.	VA IT VistA Imaging Technical team
04/20/2022	42.8	Revisions to Installing a New VIX and Updating an Existing VIX.	VA IT VistA Imaging Technical team
03/18/2022	42.7	Revisions to Updating an Existing VIX, and Post Installation Instructions.	VA IT VistA Imaging Technical team
02/22/2022	42.6	Revisions to Updating an Existing VIX, and Post Installation Instructions.	VA IT VistA Imaging Technical team

02/10/2022	42.5	Revisions to Updating an Existing VIX, and Post Installation Instructions.	VA IT VistA Imaging Technical team
02/04/2022	42.4	Revisions to Installing a New VIX and Updating an Existing VIX, and Back Out/Uninstall Scenarios.	VA IT VistA Imaging Technical team
01/03/2022	42.3	Revisions to Installing a New VIX and Updating an Existing VIX.	VA IT VistA Imaging Technical team
12/10/2021	42.2	Revisions to Installing a New VIX and Updating an Existing VIX.	VA IT VistA Imaging Technical team
11/16/2021	42.1	Incorporated comments from reviewers for MAG*3.0*269, Revisions to Installing a New VIX, Updating an Existing VIX, Back Out/Uninstall Scenarios, & Appendices. Reduced image file sizes.	VA IT VistA Imaging Technical team
09/03/2021	42.0	Update for MAG*3.0*269, Revisions to Installing a New VIX and Updating an Existing VIX.	VA IT VistA Imaging Technical team
09/02/2021	41.0	Updates for MAG*3.0*284	REDACTED
04/06/2021	40.4	Additional Updates for MAG*3.0*254, Revisions to Installing a New VIX, Updating an Existing VIX, Post-Installation for New VIX Installations and Updating Existing VIX Installations.	VA IT Vista Imaging Technical team
03/17/2021	40.3	Additional Updates for MAG*3.0*254, Post-Installation for New VIX Installations and Updating Existing VIX Installations.	VA IT VistA Imaging Technical team
03/11/2021	40.2	Additional Updates for MAG*3.0*254, Back Out/Uninstall Scenarios.	VA IT VistA Imaging Technical team
02/24/2021	40.1	Additional Updates for MAG*3.0*254, Post-Installation for New VIX Installations and Updating Existing VIX Installations, & Appendices.	VA IT VistA Imaging Technical team
01/28/2021	40.0	Additional Updates for MAG*3.0*254, Revisions to Installing a New VIX, Updating an Existing VIX, Post-Installation for New VIX Installations and Updating Existing VIX Installations, & Appendices.	VA IT VistA Imaging Technical team

01/20/2021	39.0	Update for MAG*3.0*254, Revisions to Installing a New VIX, Updating an Existing VIX, Post-Installation for New VIX Installations and Updating Existing VIX Installations, & Appendix A.	VA IT VistA Imaging Technical team
05/29/2020	38.0	Update for MAG *3.0*249, Addition of PowerShell Verification section, Revisions to Pre-Installation Configuration - Backup Copies and Tomcat User Permissions section.	REDACTED
05/26/2020	37.0	Revisions for Zip/Unzip, Manual restart sections, Figure headings, Post-Installation for New VIX Installations and Updating Existing VIX Installations & Appendix A.	REDACTED
03/16/2020	36.0	Update for MAG*3.0*249, 508 compliant.	REDACTED
08/16/2019	35.5	Update for T3 Build.	REDACTED
08/02/2019	35.0	Update for MAG*3.0*230.	REDACTED
05/20/2019	34.0	Update to save VIX configuration settings.	REDACTED
04/29/2019	33.0	Update to save VIX configuration settings.	REDACTED
04/05/2019	32.0	Updated for MAG*3.0 221 T5 Updates.	REDACTED
03/22/2019	31.0	Updated for MAG*3.0 221 T4.	REDACTED
03/01/2019	30.0	Updated for MAG*3.0 221 T4.	REDACTED
02/22/2019	29.0	Updated for MAG*3.0 221.	REDACTED
02/01/2019	28.0	Updated for MAG*3.0 201 T9.	REDACTED
11/19/2018	27.0	Updated for MAG*3.0*201.	REDACTED
09/27/2018	26.0	Additional MAG*3.0*197 Updates.	REDACTED
08/21/2018	25.0	Additional MAG*3.0*197 Updates.	REDACTED
08/14/2018	24.0	Additional MAG*3.0*197 Updates.	REDACTED
07/26/2018	23.0	Additional MAG*3.0*197 Updates.	REDACTED
07/06/2018	22.0	Updated for MAG*3.0*197.	REDACTED
06/21/2018	21.0	Additional MAG*3.0*197 Updates.	REDACTED
05/25/2018	20.0	Additional MAG*3.0*197 Updates.	REDACTED
03/13/2018	19.0	Additional MAG*3.0*197 Updates.	REDACTED
01/26/2018	18.0	Updated for MAG*3.0*197.	REDACTED
01/25/2018	17.0	Additional MAG*3.0*185 Updates.	REDACTED
01/11/2018	16.0	Additional MAG*3.0*185 updates.	REDACTED
12/05/2017	15.0	Updated MAG*3.0*185 build numbers.	REDACTED
11/14/2017	14.0	Incorporated comments from reviewers regarding MAG*3.0*185.	REDACTED

10/25/2017	13.0	MAG*3.0*185 Updates.	REDACTED
10/03/2017	12.0	MAG*3.0*177 Updates.	REDACTED
08/01/2017	11.0	MAG*3.0*177 Updates.	REDACTED
07/26/2017	10.0	MAG*3.0*170 Updates.	REDACTED
07/05/2017	9.0	MAG*3.0*170 Installer Updates.	REDACTED
04/27/2017	8.0	Updated port information.	REDACTED
03/24/2017	7.0	Date updates.	REDACTED
02/14/2017	6.0	Updated for MAG 3.0*170.	REDACTED
05/10/2016	5.0	Updated for MAG*3.0*162.	REDACTED
09/09/2013	4.0	Updated for MAG*3.0*130.	REDACTED
07/25/2013	3.0	Updated for MAG*3.0*034/116/118, MAG*3.0*119, MAG*3.0*127, MAG*3.0*129.	REDACTED
05/07/2012	2.0	Updated for MAG*3.0*122.	REDACTED
10/14/2011	1.0	Created for MAG*3.0*104. WPR complete Aug 31; labeled for release Oct 14.	REDACTED

Table of Contents

1. Introduction 1
   - 1.1. Intended Audience 1
   - 1.2. Document Conventions 1
   - 1.3. Terms of Use 1
   - 1.4. Related Information 1
2. Installing a New VIX 2
   - 2.1. Preparing for a New VIX Installation 2
     - 2.1.1. Setting up VistA 2
     - 2.1.2. Selecting and Validating the VIX Server 2
       - 2.1.2.1. FDA Requirements 3
       - 2.1.2.2. Hardware Requirements 3
       - 2.1.2.3. Port Requirements 4
       - 2.1.2.4. Operating System and Environment Requirements 4
     - 2.1.3. Getting VIX Component Licenses 7
       - 2.1.3.1. Laurel Bridge DCF Toolkit 7
       - 2.1.3.2. Aware JPEG2000 Toolkit License 8
     - 2.1.4. Getting a VIX Security Certificate 8
     - 2.1.5. PowerShell Version Verification 8
     - 2.1.6. SQL Version Verification 11
     - 2.1.7. Java Version Verification 12
     - 2.1.8. LibreOffice Verification 12
   - 2.2. New VIX Server Installation 12
   - 2.3. Preparing Passwords, Activating Components, and Staging Files 13
     - 2.3.1. VIX Server Installation 13
       - 2.3.1.1. To install the VIX Server 13
   - 2.4. Activating a New VIX 32
     - 2.4.1. To Register the VIX 32
3. Updating an Existing VIX 34
   - 3.1. Preparing for a VIX Update 34
     - 3.1.1. VistA Software Dependencies 34
     - 3.1.2. Scheduling Downtown and Impact of a VIX Update 34
   - 3.2. Preparing Service Account and Passwords 36
   - 3.3. Pre-Installation Configuration 36
   - 3.4. Performing a VIX Server Update 37
4. Post-Installation for New VIX Installations and Updating Existing VIX Installations 58
   - 4.1. Post-Installation Configuration 58
   - 4.2. MUSE Configuration 59
   - 4.3. McAfee Exclusions 59

4.4. Verifying Installation/Upgrade is Complete 60
4.5. Verifying VIX Operations 63
4.5.1. Verifying Access to the VIX Tools and VIX Transaction Log 64
4.5.2. Spot-Checking VIX Image Delivery 65
4.6. DICOM SCP Configuration 66
4.7. Using the VIX Service Installation Wizard to Reconfigure the VIX 66
4.7.1. Reconfiguring a VIX Server 66
5. Troubleshooting 69
5.1. Resuming an Interrupted VIX Installation 69
5.1.1. Resuming Installation (single server VIX) 69
5.2. Tomcat Permissions 70
5.3. VIX Support 70
6. Back Out/Uninstall 71
6.1. Stopping the VIX Services 71
6.2. Back Out/Uninstall Scenarios 71
6.2.1. Uninstall/Restore as part of Troubleshooting 72
6.2.2. Relocating a VIX onto a New Server 72
6.2.3. Decommissioning a VIX 73
6.3. Uninstalling the VIX 73
6.3.1. Remove VIX related applications, accounts, directories, and variables 73
6.4. Rollback and Back Out of MAG*3.0*269 75
6.4.1. Rollback Verification Procedure 77
7. Appendix A: Enable MUSE Functionality 78
8. Appendix B: DICOM SCP Configuration 83
8.1. AE Titles Configuration 83
8.1.1. Laurel Bridge AE Titles Configuration on VIX/CVIX 83
8.1.2. AE Titles Configuration on DICOM SCU 85
8.2. Tomcat/ Laurel Bridge DICOM SCP Configuration 85
9. Appendix C: Restart Script 88
10. Appendix D: Tomcat Permissions 90
11. Appendix E: Service Account Settings 93
12. Appendix F: VIX Install Checklist 104
12.1. VIX Install Checklist 104

Table of Figures

Figure 1: MINIMUM VIX Settings 3
Figure 2: STRONGLY RECOMMENDED VIX Settings 4
Figure 3: Add Roles and Features Wizard 5
Figure 4: .NET Framework Missing 5
Figure 5: Registry Editor .NET Framework Key 6
Figure 6: NET Framework Setup Dialogs 7
Figure 7: Execute Windows PowerShell 9
Figure 8: PowerShell Version 4.0 Check 9
Figure 9: PowerShell Setup Dialogs 10
Figure 10: PowerShell Version 5.1 Check 11
Figure 11: PowerShell Script Error 11
Figure 12: Microsoft SQL Removal 12
Figure 13: Java and LibreOffice Version Check 12
Figure 14: User Account Control - VIX Service Installation Wizard 14
Figure 15: Run the VIX Service Installation Wizard 15
Figure 16: User Account Control - VIX Installer 15
Figure 17: VIX Service Installation Wizard 30.269.5.7925 16
Figure 18: VIX Prerequisites - Tomcat Not Installed 17
Figure 19: VIX Prerequisites - Laurel Bridge Not Installed 18
Figure 20: VIX Prerequisites - Service Account not Created 19
Figure 21: VIX Prerequisites - VIX Security Certificate not Installed 20
Figure 22: VIX Prerequisites - LibreOffice not Installed 21
Figure 23: VIX Prerequisites - VIX Viewer/Render Services not Installed 22
Figure 24: VIX Viewer/Render Info Dialog 22
Figure 25: Select the SQLEXPRESS_X64-14_0_1000_169.ZIP dialog 23
Figure 26: SQL Server Setup 24
Figure 27: VIX Service Installation Wizard Prerequisites Complete 24
Figure 28: VIX Cache and Configuration Folder Creation 25
Figure 29: VistA and Email Configuration - Validate 26
Figure 30: VistA and Email Configuration - Next 26
Figure 31: Local DoD Connection for Images Configuration 27

Figure 32: VIX Install Start 28
Figure 33: PowerShell Pop-up Script Top Portion 29
Figure 34: PowerShell Pop-up Script Middle Portion 30
Figure 35: PowerShell Pop-up Script Bottom Portion 31
Figure 36: VIX Install Complete 32
Figure 37: Execute Windows PowerShell 37
Figure 38: User Account Control - Vix Service Installation Wizard 38
Figure 39: Run the VIX Service Installation Wizard 39
Figure 40: User Account Control - VixInstaller 39
Figure 41: Update VIX Components 40
Figure 42: Update VIX Components PowerShell Pop-up Script 41
Figure 43: VIX Service Installation Wizard 42
Figure 44: VIX Prerequisites - Java Not Installed 43
Figure 45: VIX Prerequisites - Tomcat Not Installed 44
Figure 46: Apache Tomcat Service Account Password 45
Figure 47: VIX Prerequisites - LibreOffice Not Installed 46
Figure 48: All Services Except VIX Viewer/Render Installed or Configure 47
Figure 49: VIX Viewer/Render Info Dialog Screenshot 47
Figure 50: Save/Configuration Button 48
Figure 51: All VIX Prerequisites Installed or Configured 49
Figure 52: VIX Cache and Configuration Folder Creation 50
Figure 53: Specify the VistA and Email Configuration - Before Validate 51
Figure 54: Specify the VistA and Email Configuration - After Validate 51
Figure 55: Configure Local DoD connection 52
Figure 56: Begin the VIX Install 53
Figure 57: PowerShell Pop-up Script Top Portion 54
Figure 58: PowerShell Pop-up Script Middle Portion 55
Figure 59: PowerShell Pop-up Script Bottom Portion 56
Figure 60: VIX Installation Complete 57
Figure 61: VIX.Viewer.Config File Policies 58
Figure 62: Set Exclusions Dialog 60
Figure 63: VISA Version Verification 61
Figure 64: VIX Viewer and Render Services Running 61

Figure 65: Listener Running 62
Figure 66: 10 Hydra IX Processor and 5 Hydra VistA Worker Processes Running 63
Figure 67: Login Page 64
Figure 68: VIX Tools Page 65
Figure 69: Run the VIX Service Installation Wizard 67
Figure 70: Run the VIX Service Installation Wizard 70
Figure 71: Stopping VIX Viewer Service 71
Figure 72: Sample MuseDataSource-1.0.Config File for One Server (MUSE ENABLED FOR JLV VIX Image Viewer) 79
Figure 73: Background Processor Queue Processor 80
Figure 74: EKG Tab in Network Location Manager in Background Processor Queue Processor 81
Figure 75: Network Location Properties in Background Processor Queue Processor 82
Figure 76: Sample AE Titles Configuration File 84
Figure 77: Example AE Titles Configuration File 84
Figure 78: Sample AE Titles configuration File with Multiple DICOM SCP Clients 85
Figure 79: Sample DICOM SCP Configuration File 86
Figure 80: Example ScpConfiguration Configuration File 87
Figure 81: Execute Windows PowerShell 88
Figure 82: Windows PowerShell Restart Script 89
Figure 83: Execute Windows PowerShell 90
Figure 84: FileMan File Entry 200 102

Table of Tables

Table 1: Functions Affected by VIX Updates 35

Table 2: VIX Site's User Profile SSN, Service Account on Local VistA, and Suggested Service Account on Local VistA 95

Table 3: VIX Install Checklist 104

1. Introduction

This document explains how to install the VistA Imaging Exchange (VIX) service. Please follow the install checklist in *Appendix F: VIX Install Checklist* at the same time as you follow the main sections of this document. To do that, most people open two copies of this document at once.

1.1. Intended Audience

This document is intended for VA staff responsible for managing a local VIX, called *the VIX server* for the remainder of this document.

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

1.2. Document Conventions

This document uses the following conventions:

Controls, options, and button names are displayed 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 displayed in bold and in brackets.

Sample output is displayed in `monospace`.

Helpful information is denoted by a **TIP**.

Important or required information is displayed in a **NOTE**.

Critical information is indicated by:

1.3. 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:

The FDA classifies VistA Imaging, and the VIX (as VistA Imaging component) as a medical device. **Unauthorized modifications to VistA Imaging, including the VIX, such as installing unapproved software, adulterates the medical device.** The use of an adulterated medical device violates US federal law (21CFR820).

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

1.4. Related Information

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

VistA Image Exchange (VIX) Administrator's Guide

2. Installing a New VIX

This section explains how to implement a new VIX. The installation checklist in *Appendix F: VIX Install Checklist* summarizes the process.

TIP: If you are updating an existing VIX, do not use this section; instead, use the *Updating an Existing VIX* section.

2.1. Preparing for a New VIX Installation

Preparing to install a new VIX involves:

- Configuring the MUSE interface. This requires the MUSE username and MUSE password for the site's online MUSE server. If the MUSE username and password are not documented in existing site VistA Imaging documentation, please contact the local BioMed team or MUSE administrator for the information.
- Acquiring Installation Files. Copy MAG3_0P269_VIX_SETUP.msi and SQLEXPRESS_X64-14_0_1000_169.ZIP (SQL 2017) to C:\temp. (Download if required. See the patch description of the patch for the download location.)
- Setting up VistA: Install the VistA KIDs package, see *Setting up VistA*.
- Selecting and validating the server where the VIX gets installed, see *Selecting and Validating the VIX Server*.
- Getting VIX component licenses, see *Getting VIX Component Licenses*.
- Getting a VIX security certificate, see *Getting a VIX Security Certificate*.
- PowerShell Version Verification, see *PowerShell Version Verification*.
- SQL Version Verification, see *SQL Version Verification*.
- Java Version Verification, see *Java Version Verification*.
- LibreOffice Verification, see *LibreOffice Verification*.

NOTE: Please ensure you have scheduled a downtime of VIX services. It may take 1-2 hours to complete.

NOTE: It is strongly suggested to restart the VIX Server prior to installing a new VIX.

Specifics are covered in the following sections.

2.1.1. Setting up VistA

You must install the compatible KIDS package on the VistA system before installing the VIX server software. For information about installing 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 must be assigned to the VistA accounts of administrators who need access to the VIX transaction log.

2.1.2. Selecting and Validating the VIX Server

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

2.1.2.1. 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.

2.1.2.2. Hardware Requirements

VIX hardware requirements:

- Installation must be done on a 64bit OS machine.
- The VIX servers run on a minimum configuration of 2 CPUs, 4 gigabytes of RAM, and 200 gigabytes of disk space. However, during previous field testing, VIX performance was found to be less than optimal, with image retrieval taking several minutes. Because of the slow performance with the minimum configuration, the following specifications are strongly recommended. (If using minimum configurations, refer to Figure 1.)
    - Strongly Recommended: 4 CPUs and 8 gigabytes or more of RAM.
- A dedicated local drive for the VIX cache.
    - Strongly Recommended: 500 gigabytes of disk space (Figure 2).
- The VIX requires a 1 gigabit Ethernet connection.

Figure 1: MINIMUM VIX Settings

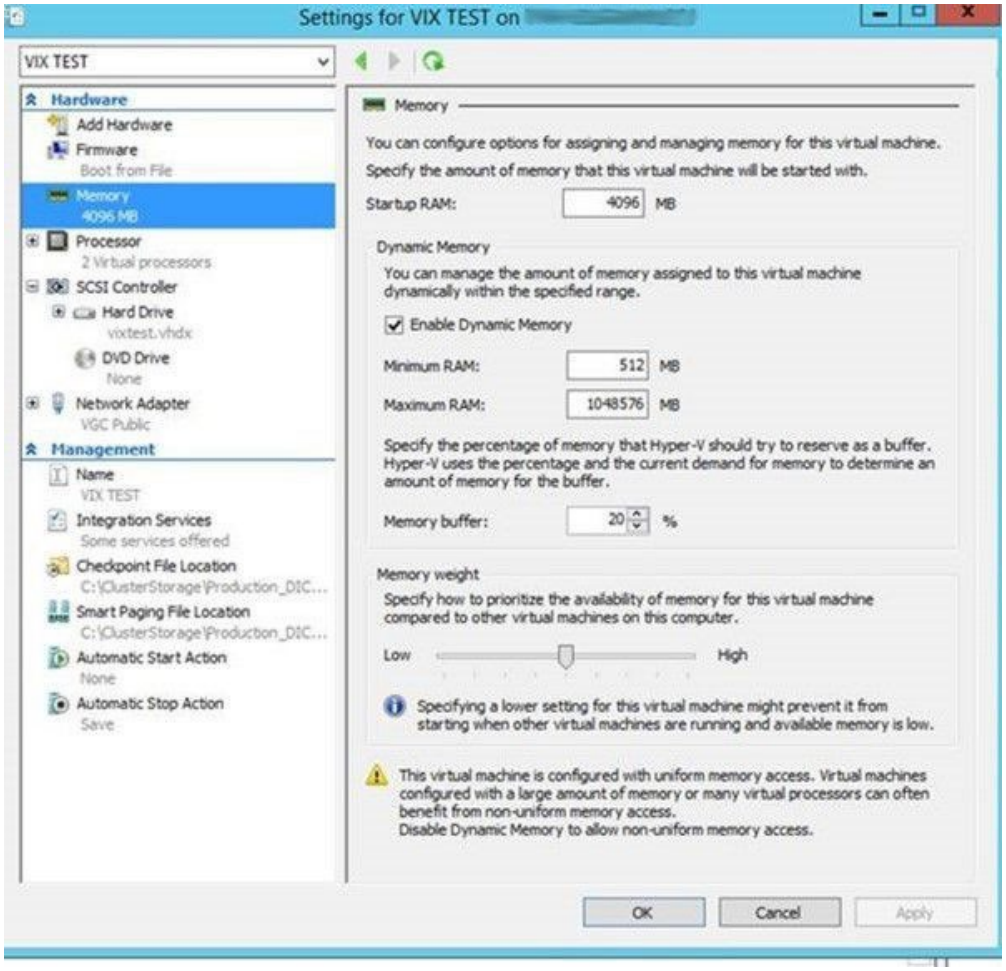
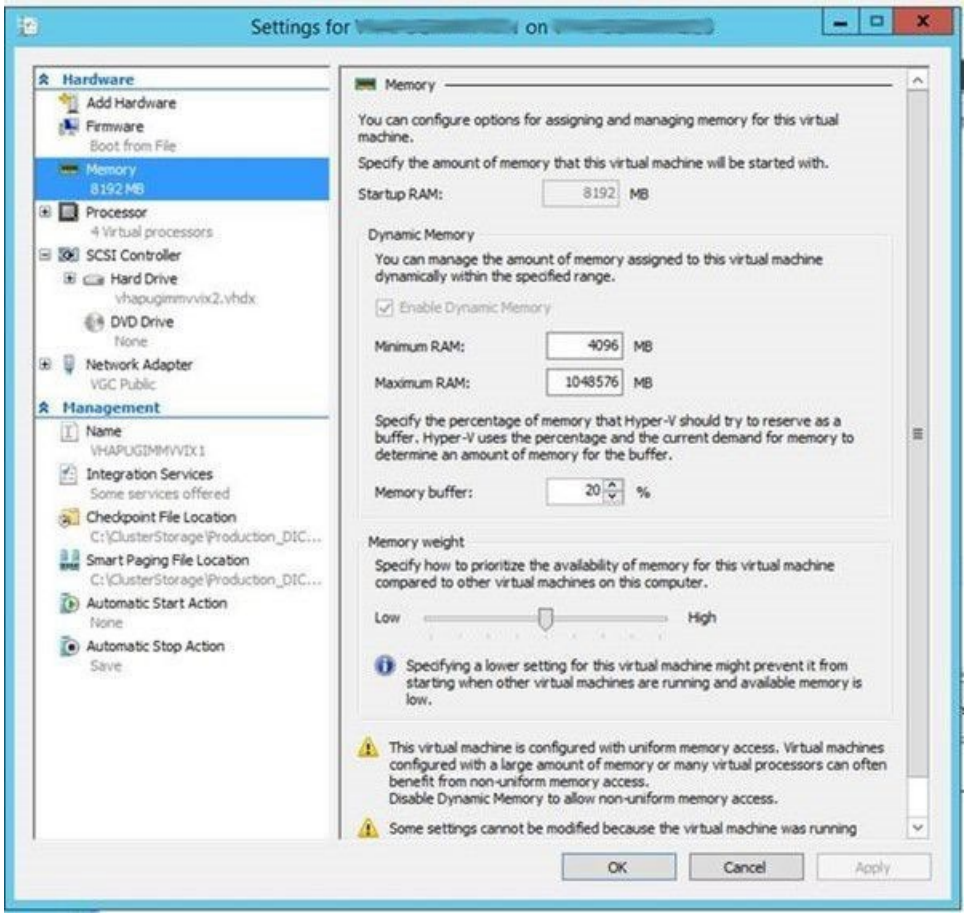


Figure 2: STRONGLY RECOMMENDED VIX Settings



2.1.2.3. Port Requirements

On the VIX server, verify that ports REDACTED, REDACTED, REDACTED, REDACTED, REDACTED, REDACTED, REDACTED, and REDACTED are accessible to VA wide area network IP addresses (10.x.x.x).

NOTE: Port REDACTED was new with MAG*3.0*249 and required for communication with the site's MUSE server.

2.1.2.4. Operating System and Environment Requirements

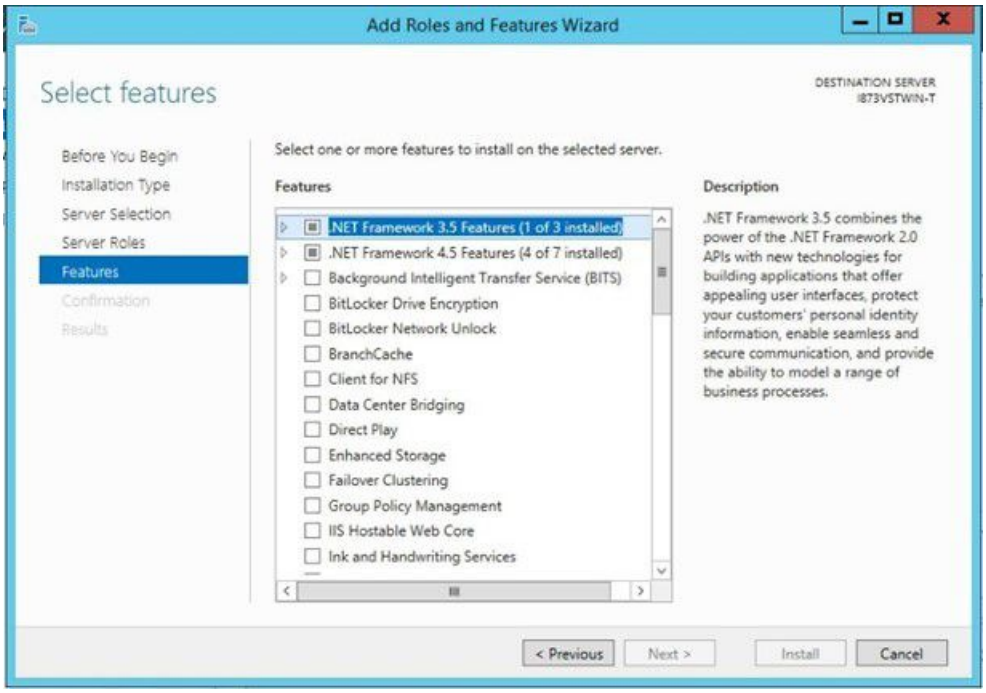
The VIX can run on:

- Minimum: Windows Server 2012 R2. Maximum: Windows Server 2016.
- Verify Visual C++ 2010 Redistributable Package (x64) is installed by viewing Programs and Features in the Control Panel. If Visual C++ 2010 Redistributable Package (x64) is not installed, download it, and install it.
  - **NOTE**: Microsoft Visual C++ 2010 Redistributable Package (x64) can be directly downloaded from https://www.microsoft.com/en-us/download/details.aspx?id=14632
- Verify .NET 3.5 features are enabled from Add Roles and Features (Figure 3) from the Server Manager option, with the Features Wizard (required for VIX install).

Alternatively, to discover if .NET 3.5 framework is installed, find .NET Framework versions in the registry by doing the following:

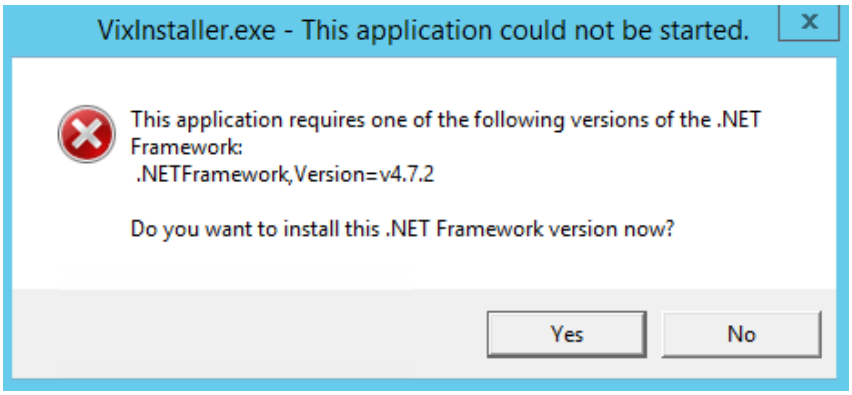
1. On the Start menu, select **Run.**
2. In the Open box, enter regedit.exe. You must have administrative credentials to run regedit.exe.
3. In the Registry Editor, open the following subkey: Software\Microsoft\NET Framework Setup\NDP\v3.5.
4. Ensure the Install REG_DWORD equals 1.

Figure 3: Add Roles and Features Wizard



- If running Windows Server 2012 R2, verify .NET 4.7.2 or .NET 4.8 framework. If running Windows Server 2016, verify .NET 4.8 framework is installed. If one of these frameworks is not installed, the installer displays an error message and asks to install the .NET Framework (Figure 4).

Figure 4: .NET Framework Missing



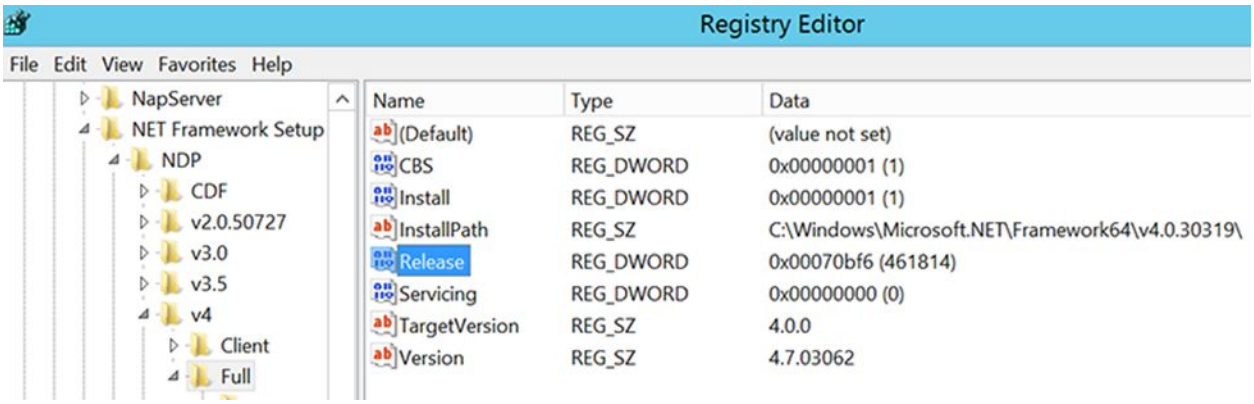
To discover if you have .NET 4.7.2 or .NET 4.8 framework installed, find .NET Framework versions in the registry, do the following:

1. On the Start menu, select **Run.**
2. In the Open box, enter regedit.exe. You must have administrative credentials to run regedit.exe.
3. In the Registry Editor, open the following subkey: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full (Figure 5).
4. Ensure the Release REG_DWORD is greater than or equal to 461808 (for .NET 4.7.2) or greater than or equal to 528040 (for .NET 4.8).

   NOTE: Release REG_DWORD is equal to 461814 (for .NET 4.7.2) or 528049 (for .NET 4.8) at the time this install documentation was last updated.

   NOTE: Additional details on determining .NET Framework versions installed is available at https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/how-to-determine-which-versions-are-installed.

Figure 5: Registry Editor .NET Framework Key

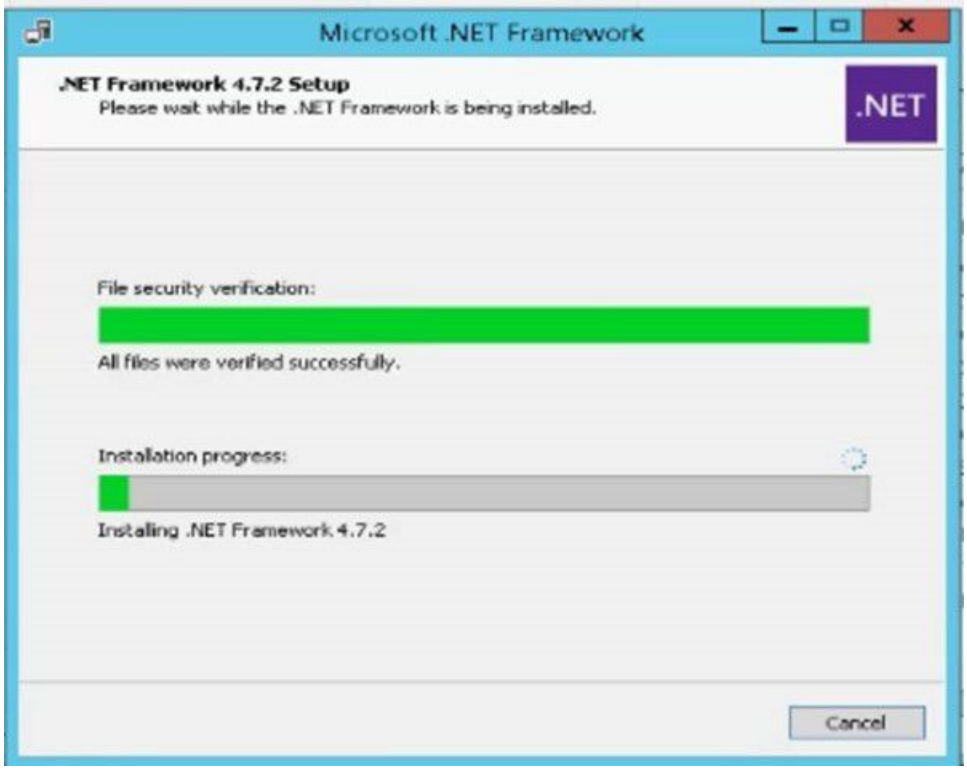


If either .NET 4.7.2 or .NET 4.8 framework is not installed, download it, install it, and then restart the server (Figure 6).

NOTE: .NET 4.7.2 software can be found on the download site, i.e.: NDP472-KB4054530-x86-x64-AllOS-ENU.exe, or directly download from the URL - https://support.microsoft.com/en-us/help/4054530/microsoft-net-framework-4-7-2-offline-installer-for-windows.

NOTE: .NET 4.8 software can be found on the download site, i.e. ndp48-x86-x64-allos-enu.exe, or directly downloaded from the URL for Windows Server 2012 R2 - https://support.microsoft.com/en-us/help/4486081/microsoft-net-framework-4-8-for-windows-server-2012 or for Windows Server 2016 https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0.

Figure 6: NET Framework Setup Dialogs



2.1.3. Getting VIX Component Licenses

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

2.1.3.1. 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 VIX server, attempt to access the Laurel Bridge activation code server at REDACTED. (A login page displays if you can access the site.)

If you cannot access this site, enter a ticket and indicate that your site ACL (access control list) needs to be modified to access REDACTED.

2. Contact the REDACTED mail group to obtain a request form and instructions for completing the form.

The VIX installation process generates an activation code using the serial number information provided. The activation code allows the Laurel Bridge DCF toolkit to be installed and used.

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

2.1.3.2. 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.

NOTE: 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 interferes with the installation process.

2.1.4. Getting a VIX Security Certificate

Each server that hosts the VIX must be issued a security certificate. To get security certificates, send an email to REDACTED and include the following information.

- Fully Qualified Domain Name (FQDN) of the VIX server name.
- Contact information for the primary and backup administrators of the VIX.

Requests typically process within five business days, after which the setup team securely transmits the security certificate (one per server) to the requesting site POC for install on the site VIX.

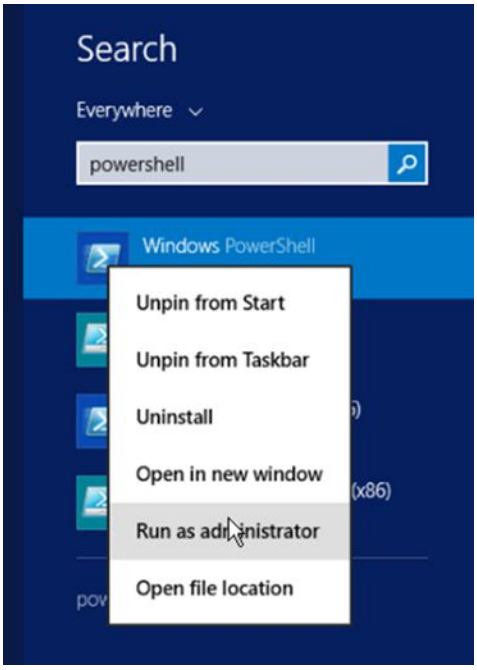
After you receive each security certificate, copy it to the local server where the VIX software is installed. The VIX Service Installation Wizard prompts you for this certificate during the installation process.

2.1.5. PowerShell Version Verification

Before beginning the VIX install, validate the installed Windows PowerShell version. If PowerShell 4.0 is the current installed version, you must install PowerShell 5.1 on your server to replace version 4.0. If PowerShell 5.1 is not installed, the post-installation script fails. To determine the PowerShell version:

1. Choose **Start**, type `PowerShell`, then right-click on **Windows PowerShell** and **run** as an administrator (Figure 7).

Figure 7: Execute Windows PowerShell



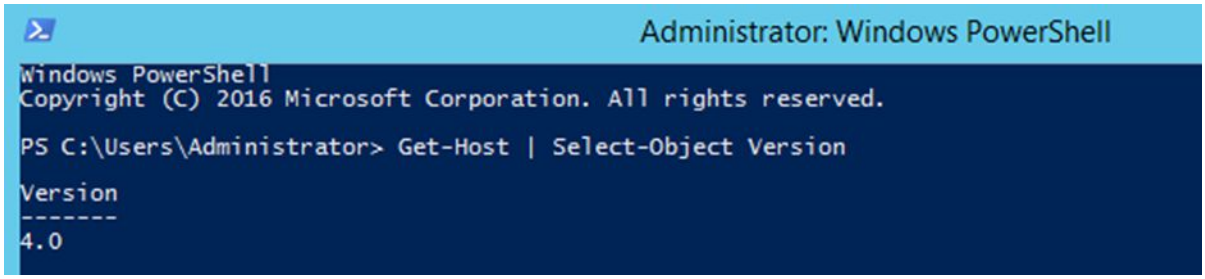
2. Once PowerShell launches, type the command:

   ```
   Get-Host | Select-Object Version
   ```

   Press **[ENTER]** to display the PowerShell version.

3. Notice the first two numbers that appear under Version, then close PowerShell. If the first two numbers under Version are **4.0** (Figure 8), proceed with the next step to install PowerShell 5.1.

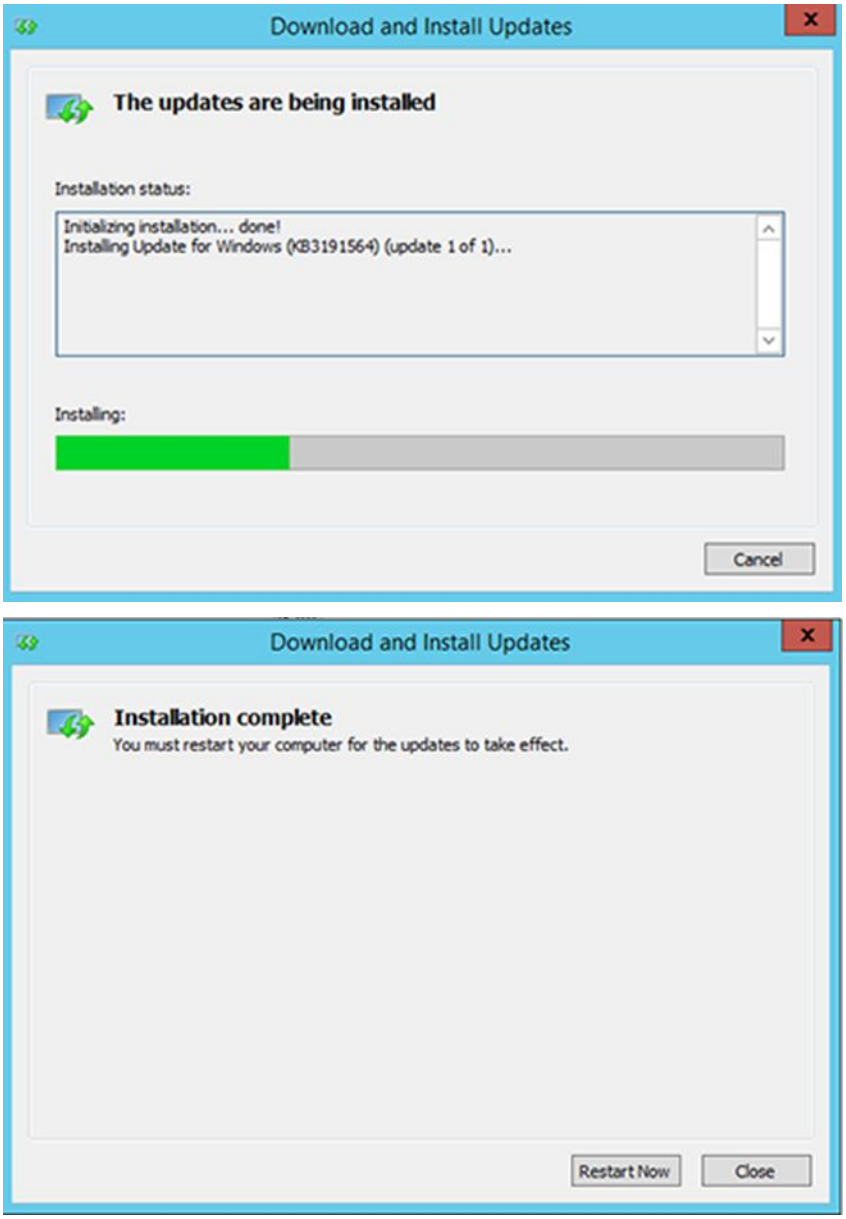
Figure 8: PowerShell Version 4.0 Check



PowerShell 5.1 software can be found in the file Win8.1AndW2K12R2-KB3191564-x64.msu, with direct download available from https://www.microsoft.com/en-us/download/details.aspx?id=54616. To install PowerShell:

1. Follow the on-screen instructions (Figure 9).

Figure 9: PowerShell Setup Dialogs

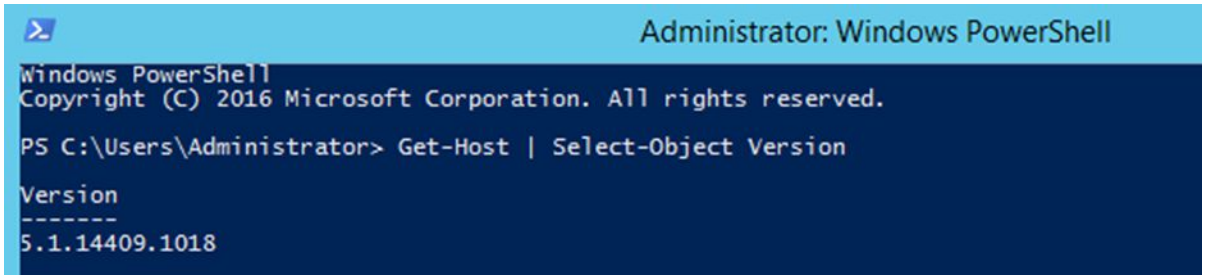


2. After PowerShell 5.1 is installed, a reboot of your server is REQUIRED.

To verify the successful installation of PowerShell:

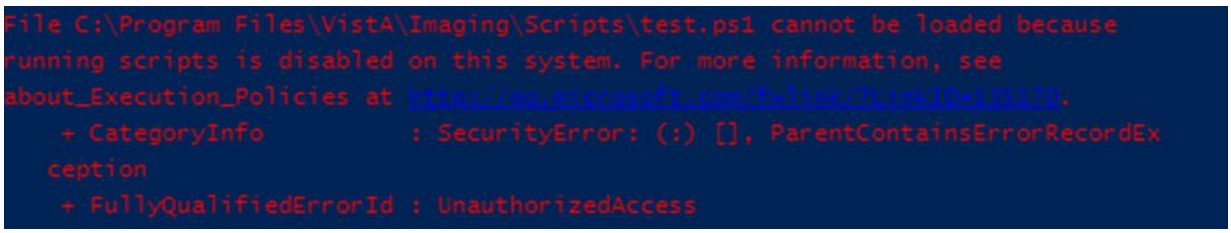
1. Choose **Start**, type `PowerShell`, then right-click on **Windows PowerShell** and **run** as an administrator (Figure 7).
2. Once PowerShell launches, type the command:
   `Get-Host | Select-Object Version`
   Press **[ENTER]** to display the PowerShell version.
3. Notice the first two numbers that appear under Version, then close PowerShell. The first two numbers under Version should display **5.1** (Figure 10) if PowerShell 5.1 installation was successful.

Figure 10: PowerShell Version 5.1 Check



NOTE: PowerShell must be configured to allow scripts to run. An error may occur (Figure 11) that prevents scripts from running.

Figure 11: PowerShell Script Error



To fix the above PowerShell script error:

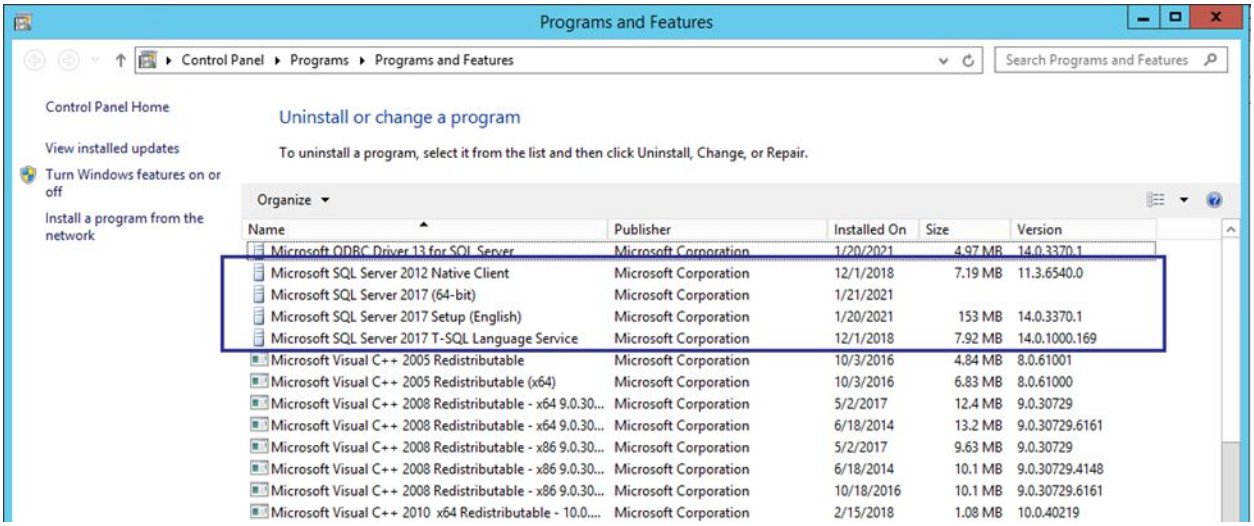
1. Choose **Start**, type `PowerShell`, then right-click on **Windows PowerShell** and **run** as an administrator (Figure 7).
2. Once PowerShell launches, type the command:
   `Set-ExecutionPolicy RemoteSigned -Force`
   Press **[ENTER]** to set the policy to allow scripts to run, then close PowerShell.

2.1.6. SQL Version Verification

Before beginning the VIX install, remove any SQL version older than SQL 2017.

1. Stop the Apache Tomcat Service if it is installed and running.
2. Uninstall all old MS-SQL programs (**Control Panel – Programs – Programs and Features – Uninstall**) (Figure 12).
3. Remove/Delete the folder C:\Program Files\Microsoft SQL Server (include data files if any exist).
4. **RESTART the VIX server before proceeding. You MUST restart the server after uninstalling SQL software.**

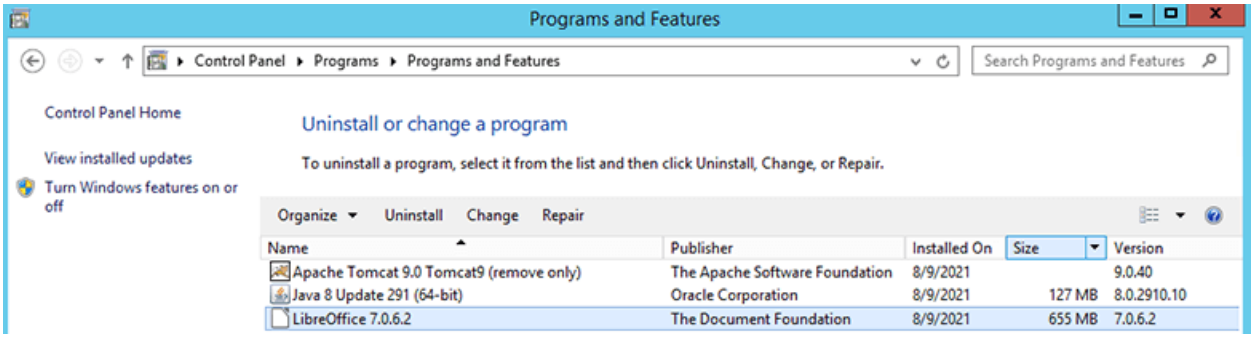
Figure 12: Microsoft SQL Removal



2.1.7. Java Version Verification

Before beginning the VIX install, validate any Java version installed. MAG*3.0*269 VIX installer uninstalls Java 8.0.251, if installed, and installs Java 8.0.291. If the Java version installed is older than Java 8.0.251, you must uninstall manually. The current Java version can be checked using the Control Panel (Figure 13). Reboot your server after Java uninstall.

Figure 13: Java and LibreOffice Version Check



2.1.8. LibreOffice Verification

Before beginning the VIX install, validate any LibreOffice version installed. MAG*3.0*269 VIX installer uninstalls and installs LibreOffice 7.0.6. If the LibreOffice version installed is older than 7.0.6, it must be uninstalled manually. The current LibreOffice version can be checked using the Control Panel (Figure 13).

2.2. New VIX Server Installation

The following steps are used to install a VIX on a server for the first time. Installation should take less than 30 minutes if all preparation steps in the previous sections are complete.

NOTE: Only perform the steps in this section if you are installing the VIX on a single server.

2.3. Preparing Passwords, Activating Components, and Staging Files

NOTE: Use proper safeguards to securely store passwords.

Before starting the VIX installation process, do the following:

1. As already stated in Section 2.1, configuring the MUSE interface requires the MUSE username and MUSE password for the site's online MUSE server. If the MUSE username and password are not documented in existing site VistA Imaging documentation, please contact the local BioMed team or MUSE administrator for the information.
2. Prepare a password to be used for the Apache Tomcat administrator account created as part of the VIX installation process.
    - The password is case sensitive, must contain at least **fourteen (14) alphanumeric characters**, and must contain at least one capital letter and one number.
3. Prepare a password for the Windows account that the VIX installation process creates.
    - The system uses this Windows account, named "apachetomcat" when it is created by the VIX installer, 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 **fourteen (14) alphanumeric characters**, and must contain at least one capital letter and one number.
4. To use the Release of Information (ROI) and DICOM Query Retrieve Service Class Provider (SCP), set up a local VistA service account as specified in *Appendix E: Service Account Settings*.
5. Determine the email address or addresses for notification about invalid ROI periodic processing credentials. The VIX sends 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.
6. Copy the VIX security certificate to the primary drive (usually the C drive) of the VIX server.

2.3.1. VIX Server Installation

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

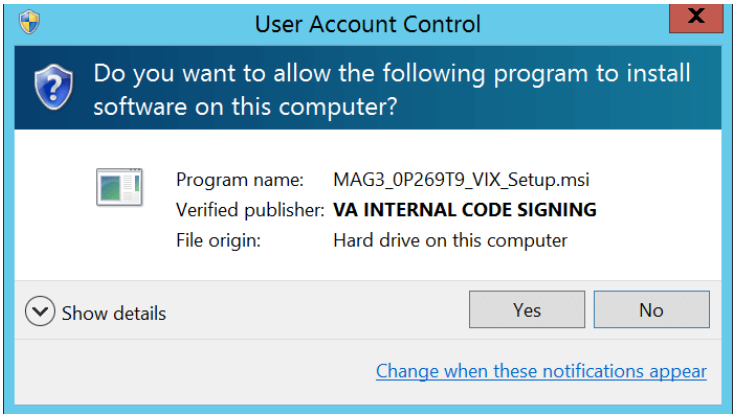
NOTE: These steps presume you have already obtained a serial number for the Laurel Bridge DCF toolkit. These steps also presume the VIX can access the Laurel Bridge license server via the internet.

2.3.1.1. To install the VIX Server

1. Use an administrator-level account to log onto the VIX server.

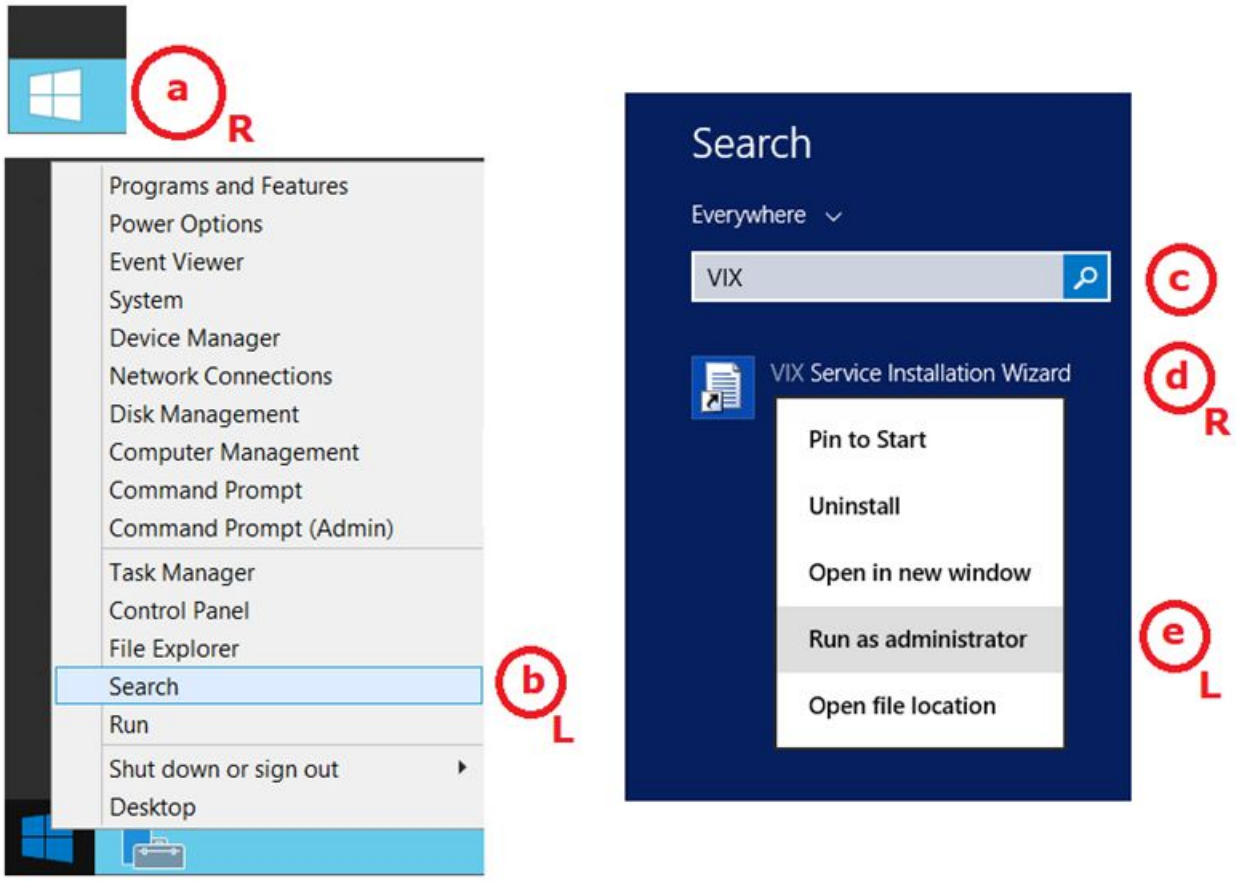
2. If you did not already do this in Section 2.1, copy the latest VIX installer (MAG3_0P269_VIX_SETUP.msi) and the SQLEXPRESS_X64-14_0_1000_169.ZIP (SQL 2017) to C:\temp.
3. Do the following to prepare the VIX Service Installation Wizard:
   a. Right-click the MAG3_0P269_VIX_SETUP.msi file and click on Install.
   b. If prompted with "Do you want to allow the following program from a verified publisher to make changes to this computer?", click **Yes** (Figure 14).

Figure 14: User Account Control - VIX Service Installation Wizard



   c. When the Welcome page displays, click **Next**.
   d. When the Confirm Installation page displays, click **Next**.
   e. When the Installation Complete screen displays, click **Close**.
4. Run the VIX Service Installation Wizard as an administrator (Figure 15).
   a. **R**ight-click **Start**.
   b. **L**eft-click **Search**.
   c. Type **VIX**.
   d. **R**ight-click **VIX Service Installation Wizard**.
   e. **L**eft-click **Run as administrator**.

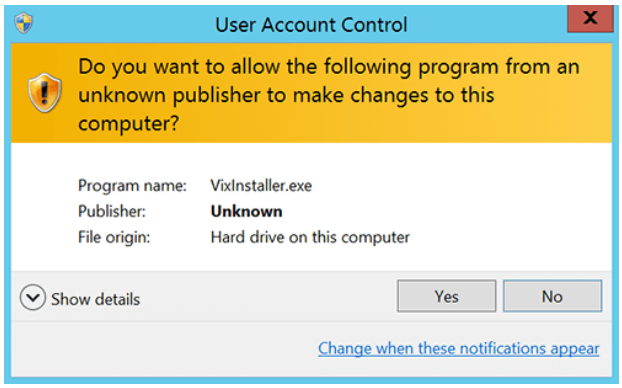
Figure 15: Run the VIX Service Installation Wizard



NOTE: If the VIX Service Installation Wizard does not appear in the Search bar as in Figure 15, open Windows Explorer and navigate to the **C:\Program Files (x86)\Vista\Imaging\VixInstaller** folder, **r**ight-click **VixInstaller.exe** and **l**eft-click **Run as administrator**.

5. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes** (Figure 16).

Figure 16: User Account Control - VIX Installer

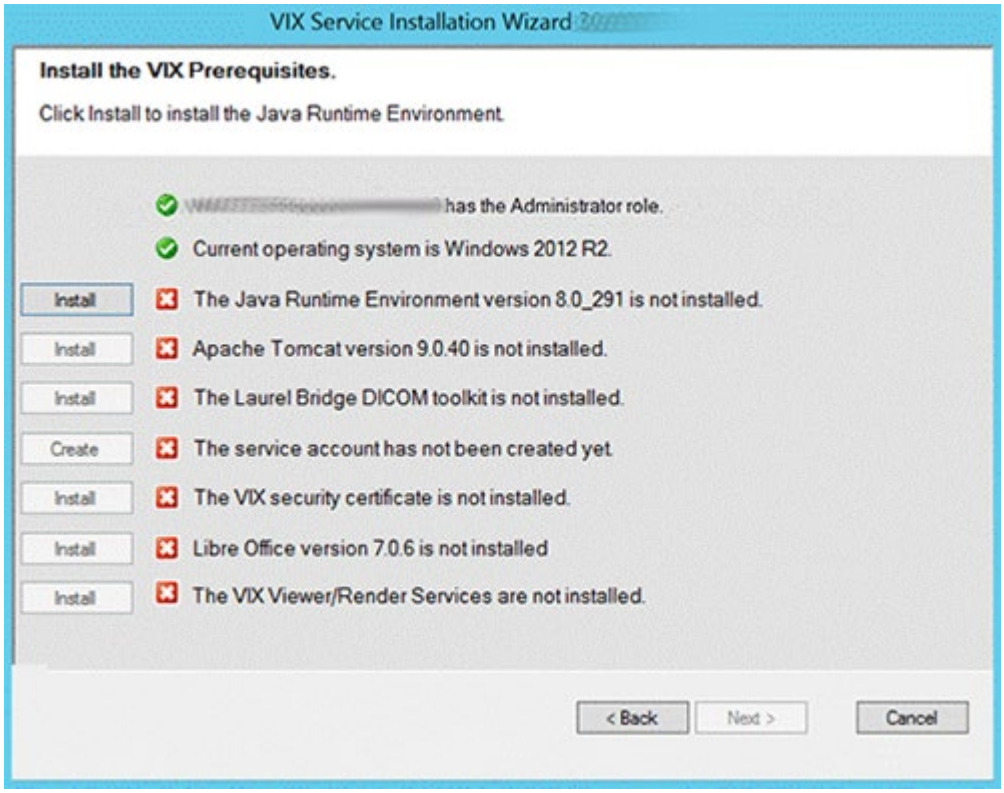


6. When the Welcome page for the VIX Service Installation Wizard displays, click **Next**.

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, the information is in FileMan in VistA). Then, click **Lookup Server Addresses**.
8. Verify the site related information retrieved by the lookup is correct. Then, click **Next**.

   NOTE: The VIX server hostname is blank, and the port number is 0; these values are populated automatically once the VIX is registered with the VistA site service.
9. Please be patient for the VIX Prerequisites page to appear, as it may take a while. When the Install the VIX Prerequisites page displays, verify that the icons for the first two items on the page are ✅.
   a. **<account> has Administrator role** – This line indicates if an administrative account is being used. If not, cancel the installation and restart it using a Windows administrator account.
   b. **Current operating system** – This line indicates if the proper operating system is present. If a non-supported operating system is identified, the installation cannot continue.
10. On the same page, read the line that indicates the state of the Java Runtime Environment. If ✅ displays, skip to the next step. If ❌ displays (Figure 17), do the following:
    a. Click **Install**.
    b. Wait until the status icon for the Java Runtime Environment changes to ✅. This install of Java may take over five minutes to complete. Please be patient, as this step may take a while to complete.

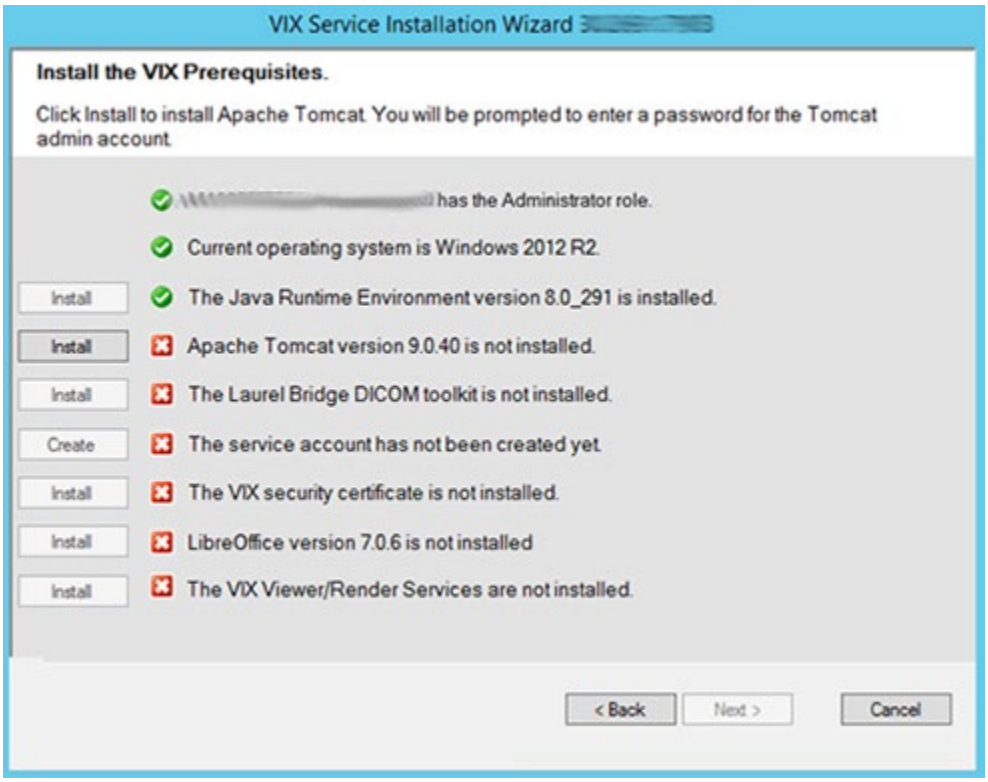
Figure 17: VIX Service Installation Wizard 30.269.5.7925



NOTE: The person installing the VIX software does not need to be in the VHAMASTER domain. The installer's domain should appear with their name. This (and subsequent screenshots) is just an example of what the installer sees.

11. On the same page, read the line that indicates the state of the Apache Tomcat installation. Since you may have reached this page by clicking the **Back** button on a subsequent page, if ✅ displays, skip to the next step. If ❌ displays (Figure 18), do the following:
    a. Click **Install**.
    b. In the dialog box that displays, enter and confirm the Apache Tomcat password that you previously prepared as described in *Preparing Passwords, Activating Components, and Staging Files.* Then, click **OK**.
    c. Wait until the status icon for Apache Tomcat changes to ✅. This install of Tomcat may take over five minutes to complete. Please be patient, as this step may take a while to complete.

Figure 18: VIX Prerequisites - Tomcat Not Installed



12. On the same page, read the line that indicates the state of the Laurel Bridge toolkit. Since you may have reached this page by clicking the **Back** button on a subsequent page, if ✅ displays, skip to the next step. If ❌ displays (Figure 19), do the following:
    a. Click the **Install** button next to the Laurel Bridge item. After a brief delay, the Activate DCF License window opens.

       TIP: The system automatically selects the Network Activation tab and pre-populates about half of the boxes in the window.
    b. Enter all the following information in the Network Activation tab:

NOTE: The system disables the Activate button if any of the following boxes are left blank.

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

ii. **Site** – the name of your site.

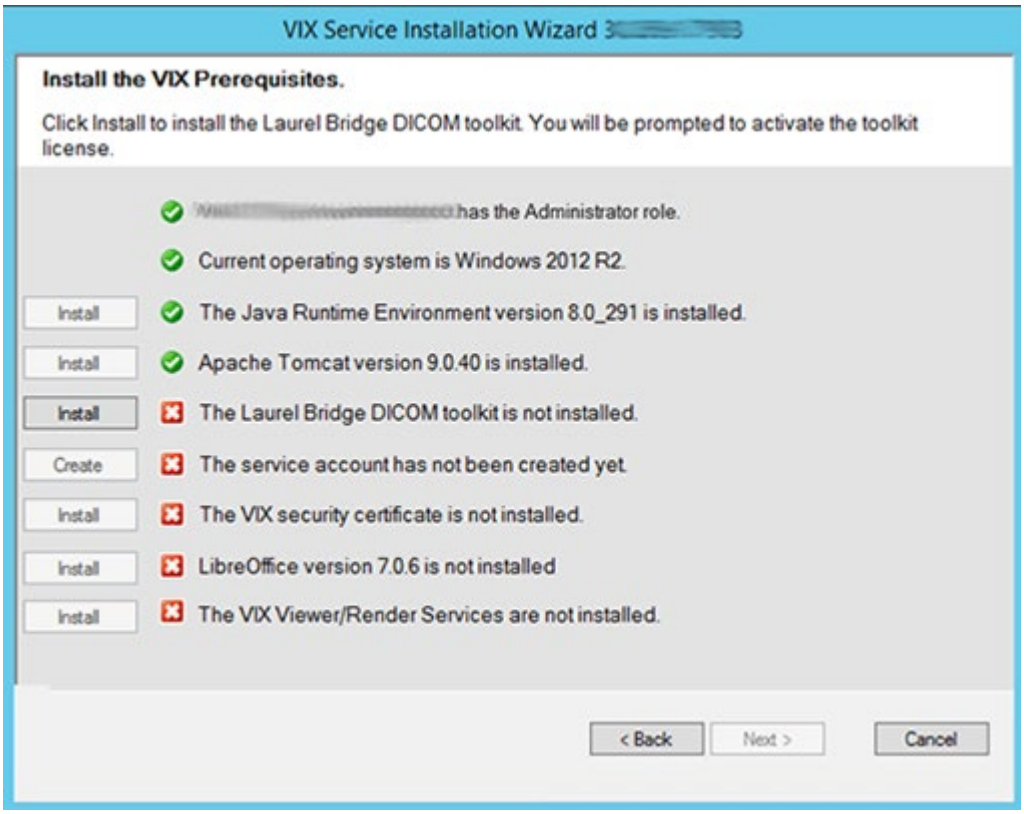
iii. **CPUs** – the number of CPUs on the server hosting the VIX.

iv. **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 displays a green "Success" message.

d. Click **Exit with success**. The Activate DCF License window closes and the updated Laurel Bridge toolkit installs in only a second or two.

Figure 19: VIX Prerequisites - Laurel Bridge Not Installed



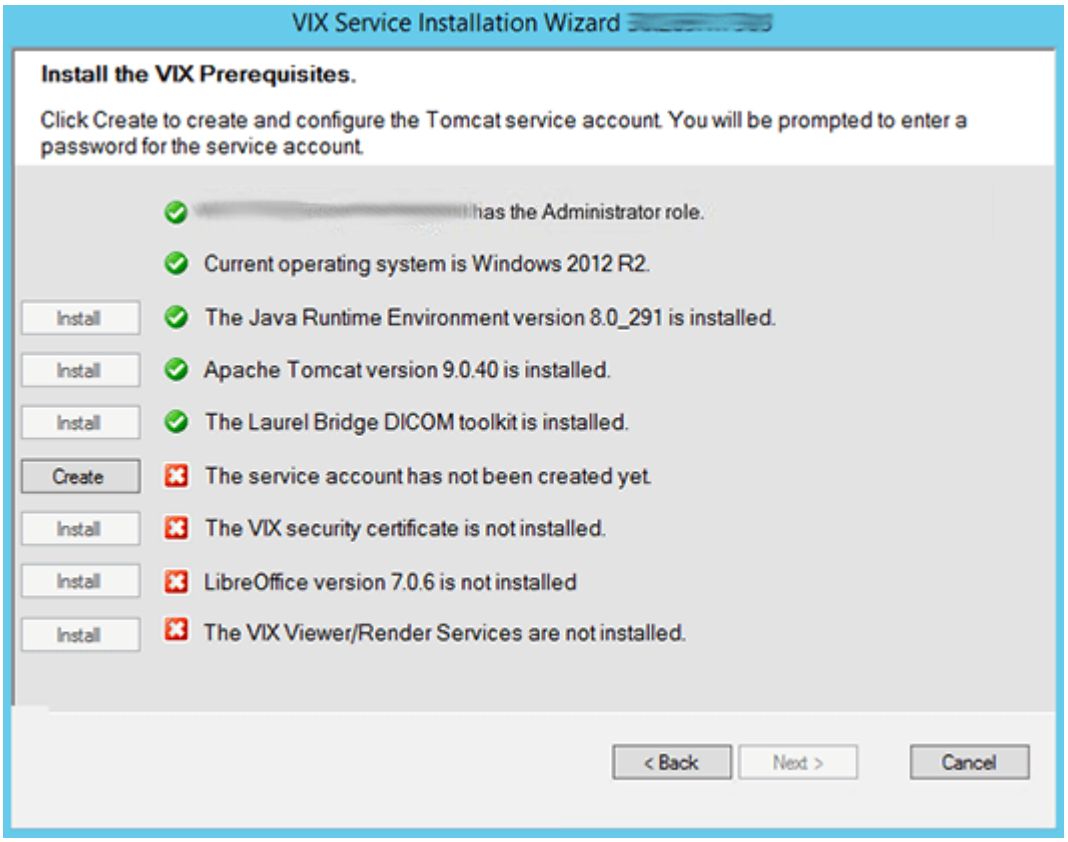
13. On the same page, read the line that indicates the state of the service account. Since you may have reached this page by clicking the **Back** button on a subsequent page, if ✅ displays, skip to the next step. If ❌ displays (Figure 20), do the following:

a. Click **Create**.

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

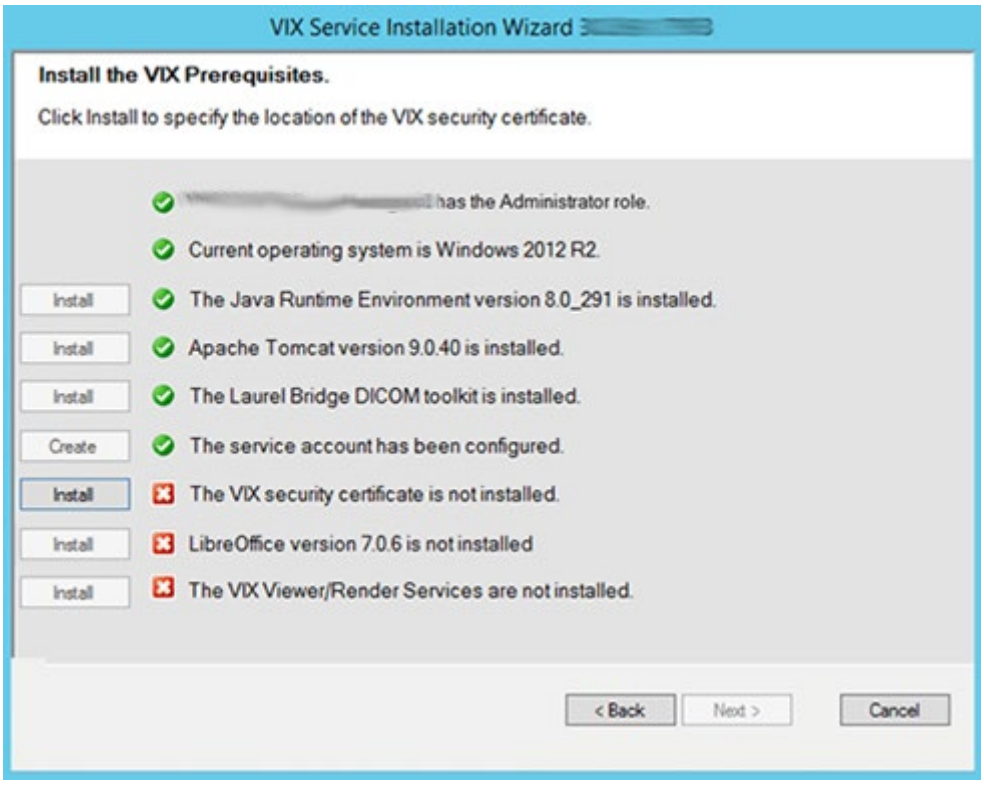
c. Wait until the status icon for the service account changes to ✅.

Figure 20: VIX Prerequisites - Service Account not Created



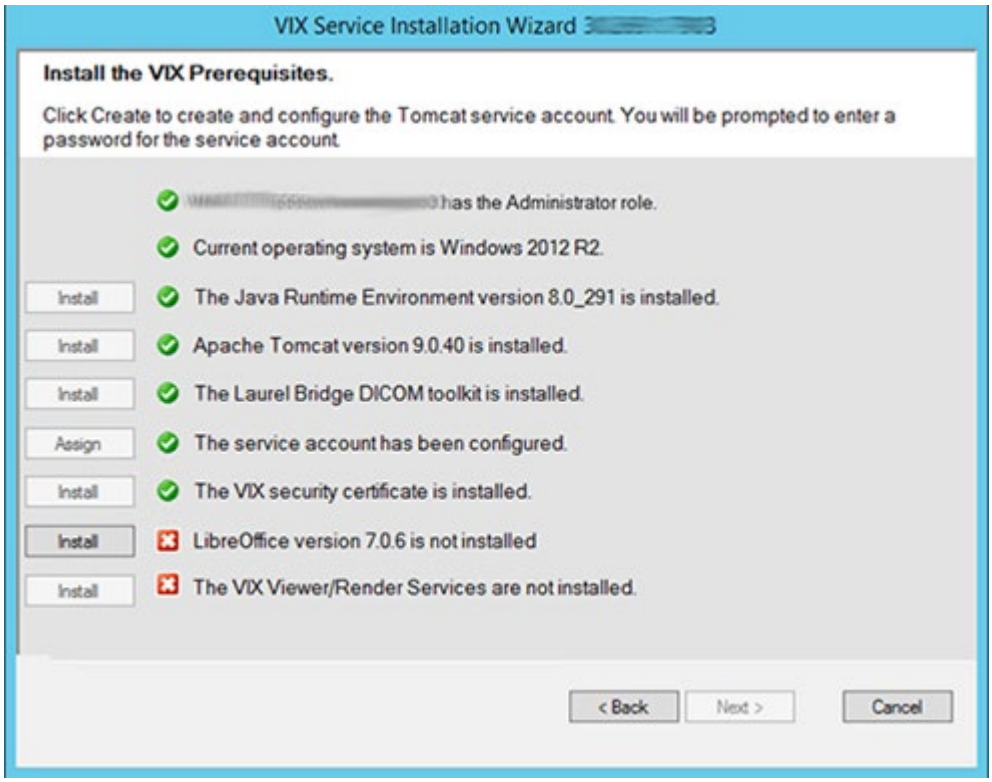
14. On the same page, check the line that indicates the state of VIX security certificate. Since you may have reached this page by clicking the **Back** button on a subsequent page, if ✅ displays, skip to the next step. If ❌ displays (Figure 21), do the following:
    a. Click **Install**.
    b. In 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**.

Figure 21: VIX Prerequisites - VIX Security Certificate not Installed



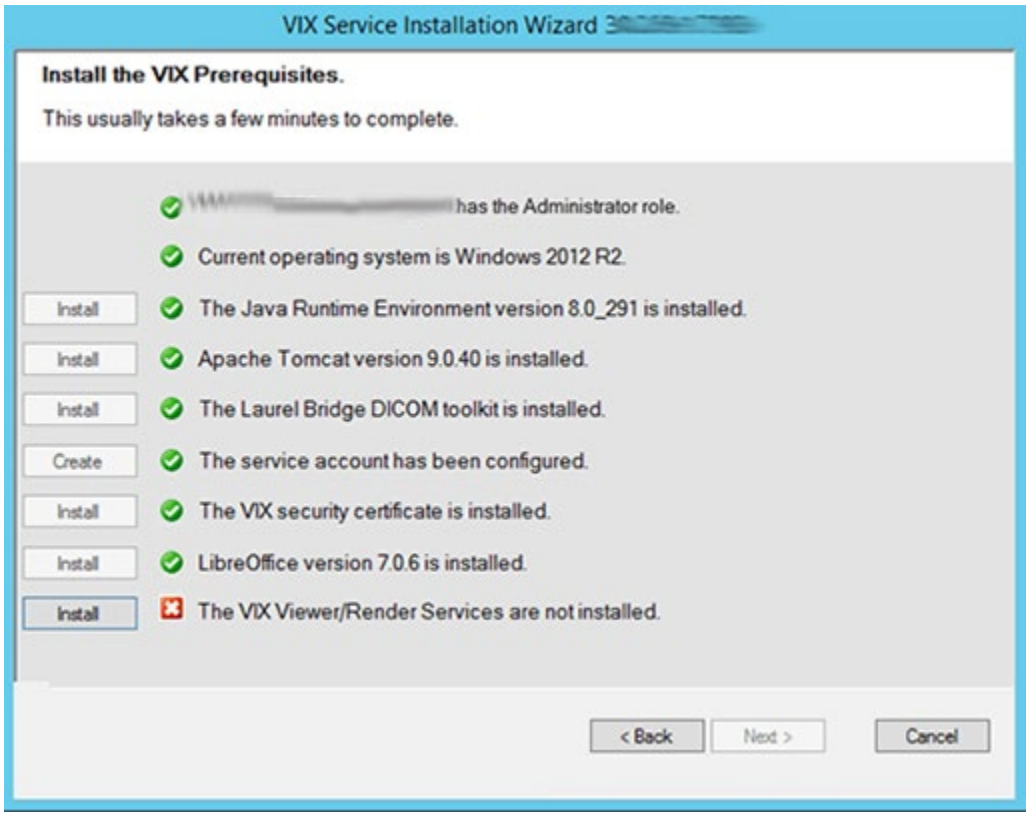
15. On the same page, read the line that indicates the state of the LibreOffice installation. If ✅ displays, skip to the next step. If ❌ displays (Figure 22), do the following:
    a. Click **Install**.
    b. Wait until the status icon for LibreOffice changes to ✅. (This install of LibreOffice may take several minutes to complete. Please be patient, as this step may take a while to complete.)

Figure 22: VIX Prerequisites - LibreOffice not Installed



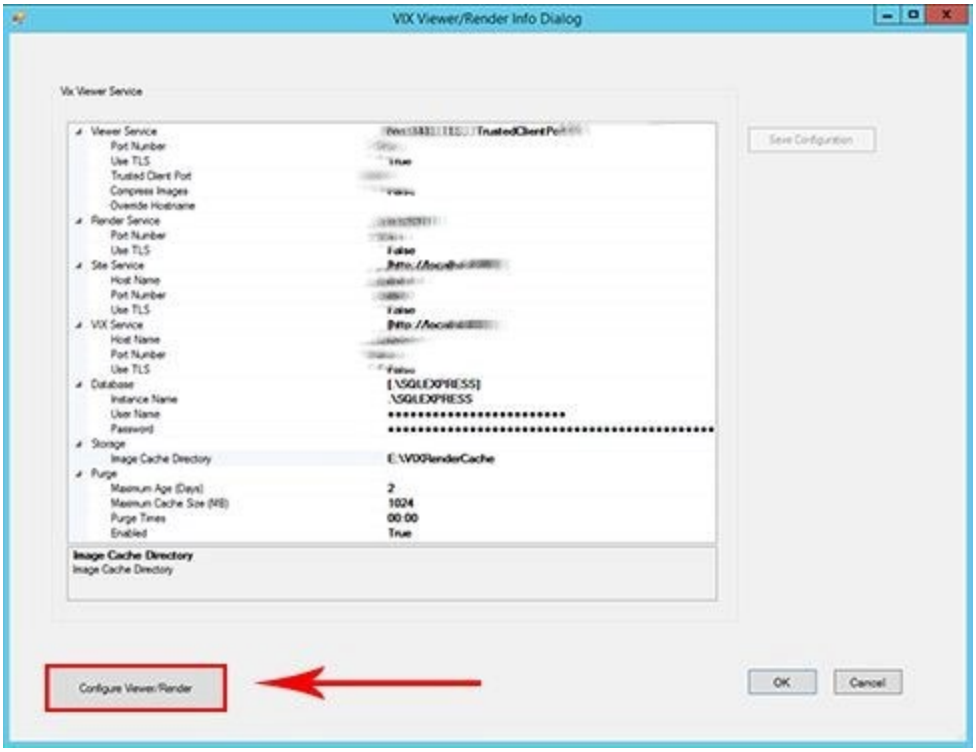
16. Check the line that indicates VIX Viewer/Render Services. Since you may have reached this page by clicking the **Back** button on a subsequent page, if displays, skip to the next step. If displays (Figure 23), do the following.
    a. Click **Install**.

Figure 23: VIX Prerequisites - VIX Viewer/Render Services not Installed



a. Click **Configure Viewer/Render** (Figure 24).

Figure 24: VIX Viewer/Render Info Dialog



b. Verify the following settings:
   i. Verify the viewer port number is REDACTED.
   ii. Verify the trusted client port is REDACTED.
   iii. Verify Site Service hostname is localhost.
   iv. Verify Site Service port is REDACTED.
   v. Verify VIX Service hostname is localhost.
   vi. Verify instance name is ".\SQLEXPRESS".
c. Edit image cache directory drive to the dedicated VIX cache drive. (i.e. "E:\VIXRenderCache")
d. If setting values were modified, click the **Save Configuration** button in the top right corner.
e. Click **OK**.
f. The installation updates the VIX Viewer/Render Services in the background. This takes approximately three to five minutes to complete.

17. If prompted to install SQL Server, click **OK** and select (Figure 25) the SQLEXPRESS_X64-14_0_1000_169.ZIP file in the temporary folder in C:\temp. Depending on your system, this step may take up to twenty minutes (Figure 26).

Figure 25: Select the SQLEXPRESS_X64-14_0_1000_169.ZIP dialog

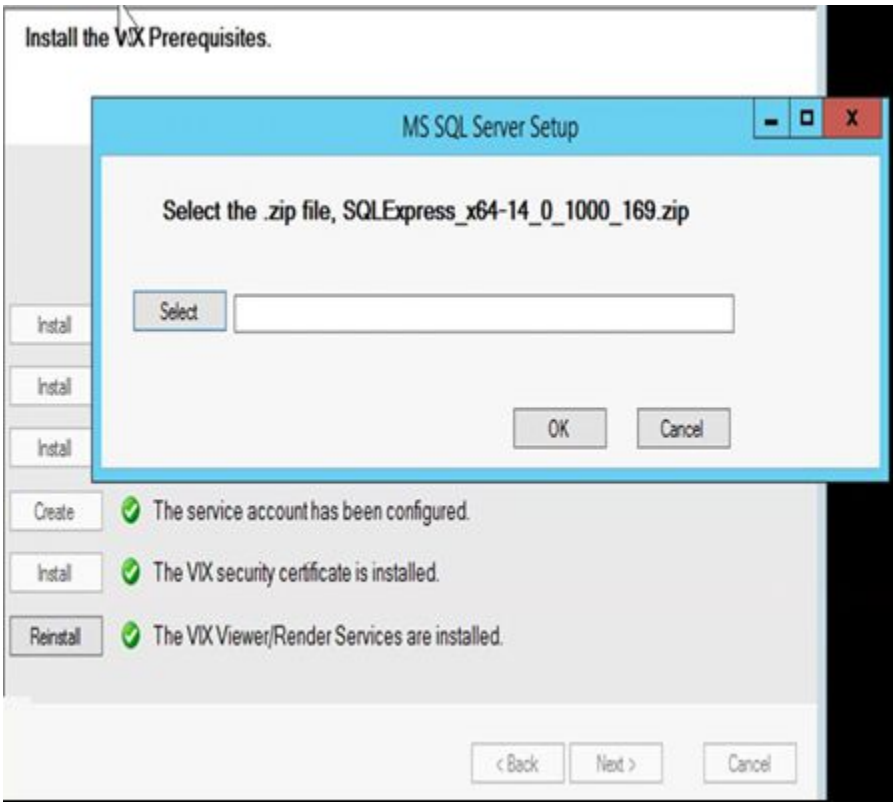
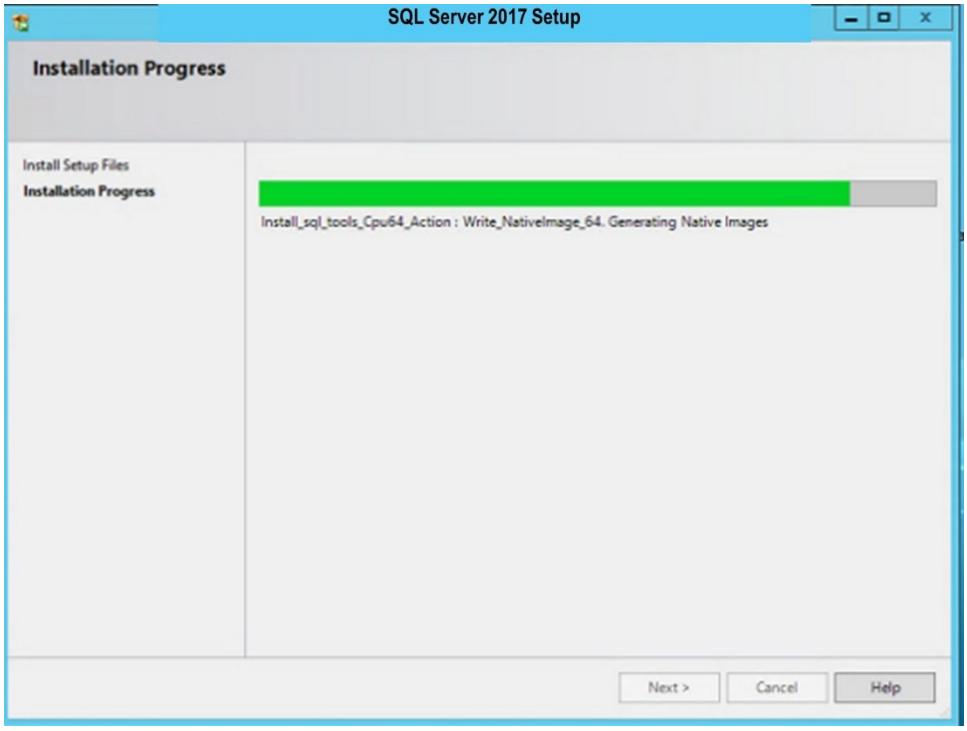
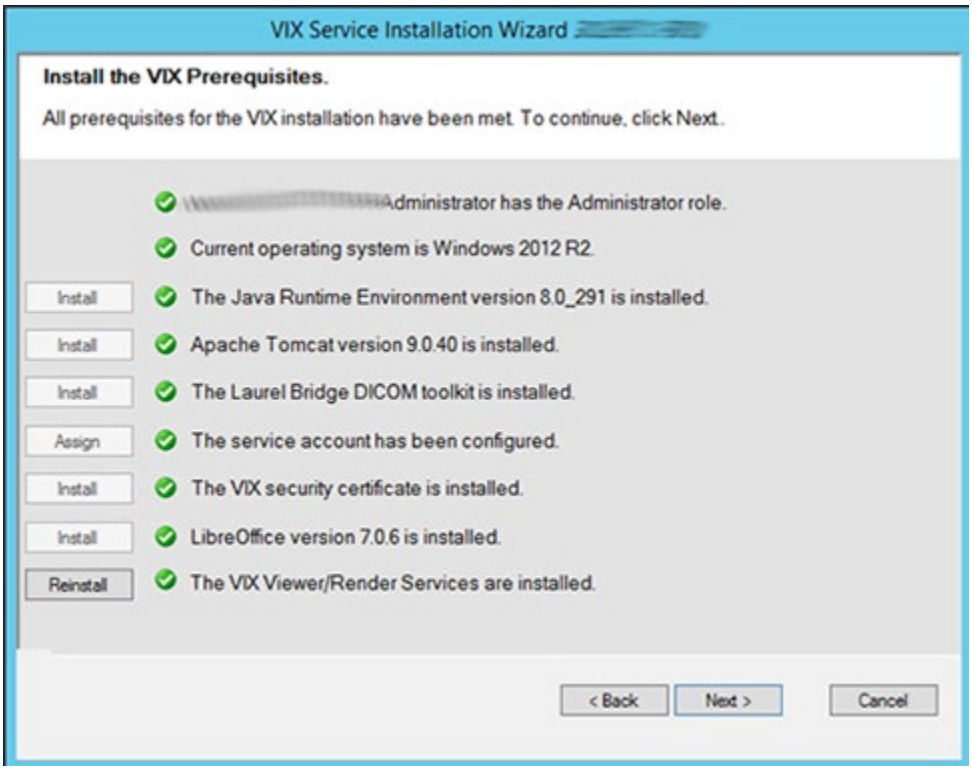


Figure 26: SQL Server Setup



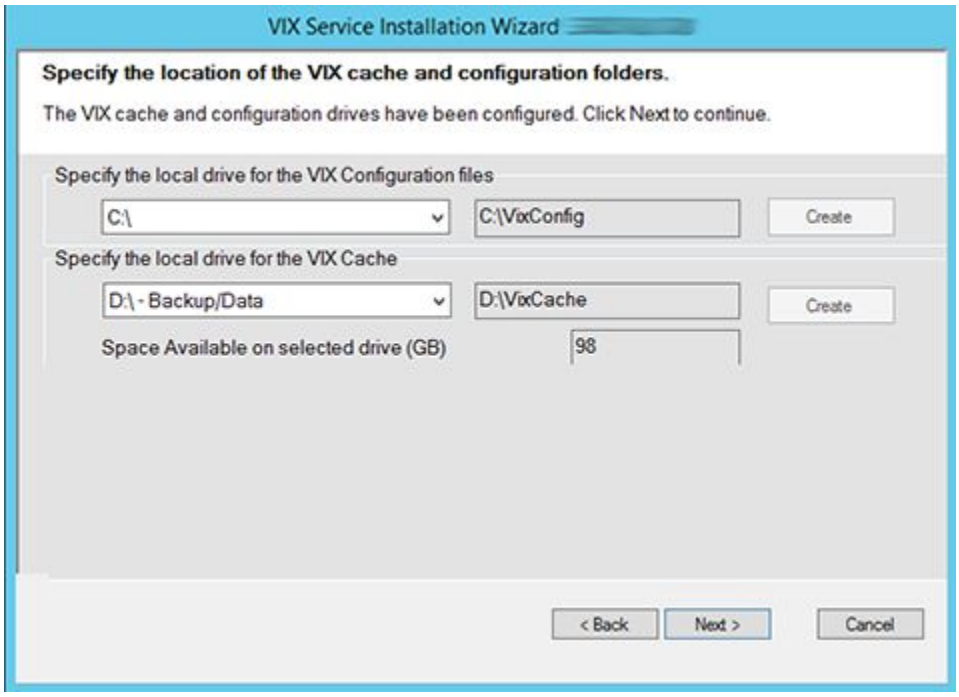
18. In the Install the VIX Prerequisites page, confirm that all the icons are ✅. Then, click **Next** (Figure 27).

Figure 27: VIX Service Installation Wizard Prerequisites Complete



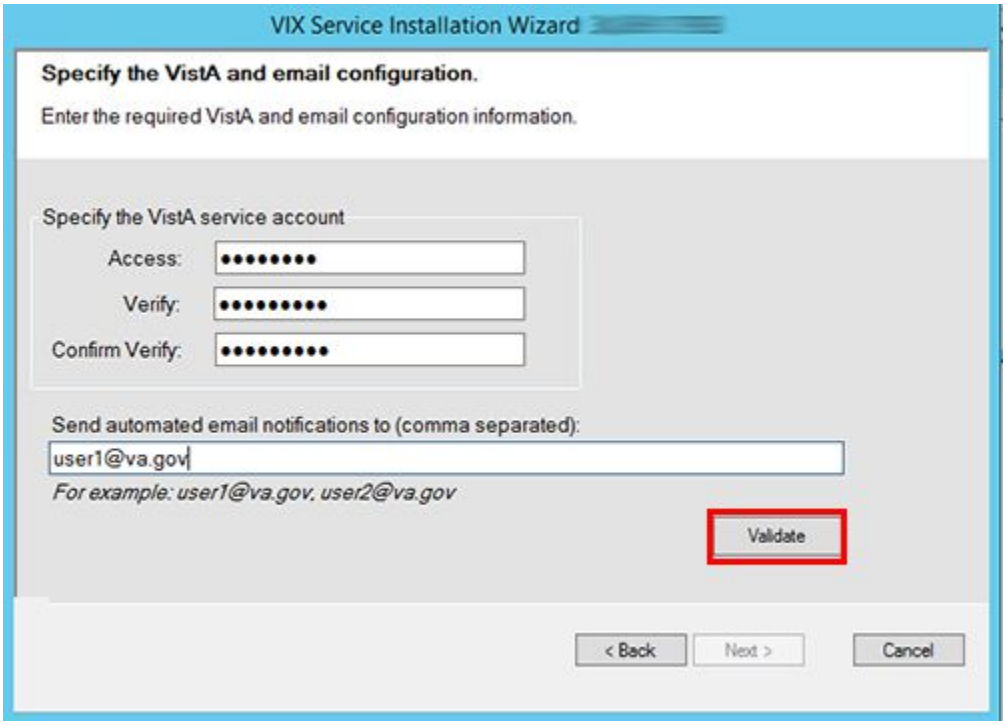
19. In the Specify the location page, select the drive for the VIX configuration files to reside. Then, click **Create**.
20. On the same page, select the drive where to create the VIX cache. Select the "C:\" drive for the VixConfig folder and the appropriate VixCache drive for your site (D: is displayed as an example in Figure 28). Click each **Create** button to create the folders.

Figure 28: VIX Cache and Configuration Folder Creation



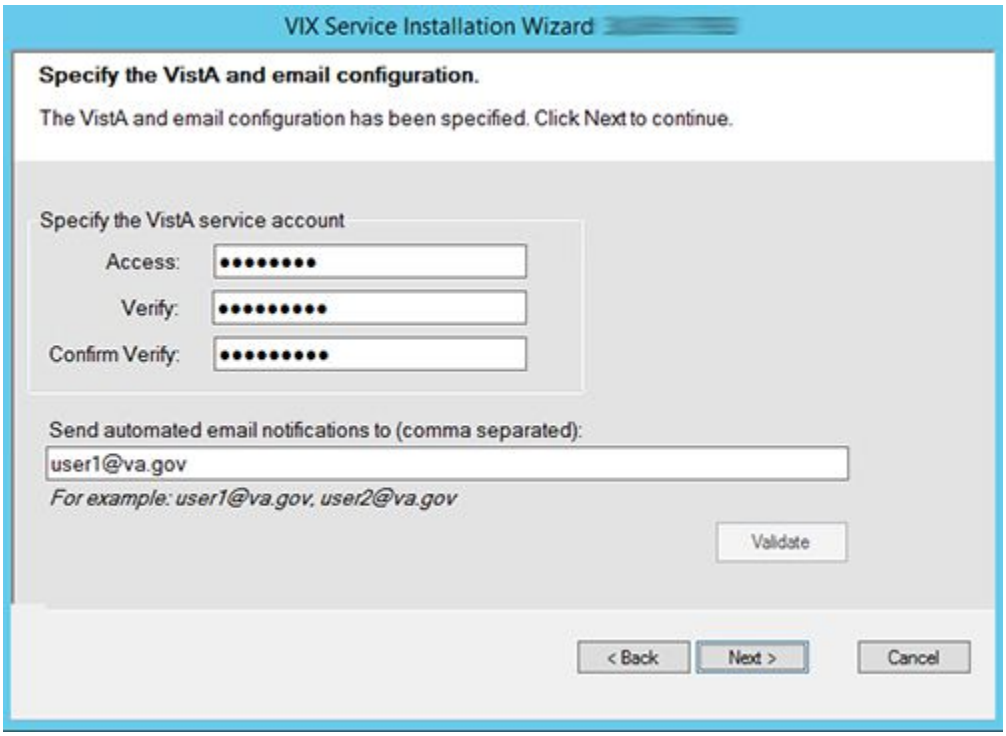
21. Click **Next**.
22. In the VistA and Email Configuration (Figure 30), perform the following:
    a. Specify the access and verify codes for the account with the VistA credentials. The VIX uses this account for periodic processing of ROI disclosure requests and DICOM query retrieve SCP requests. This account must have valid VistA credentials with the settings specified in *Appendix E: Service Account Settings*
    b. Specify the email address that gets notifications for invalid 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.
    c. Click **Validate** (Figure 29).

Figure 29: VistA and Email Configuration - Validate



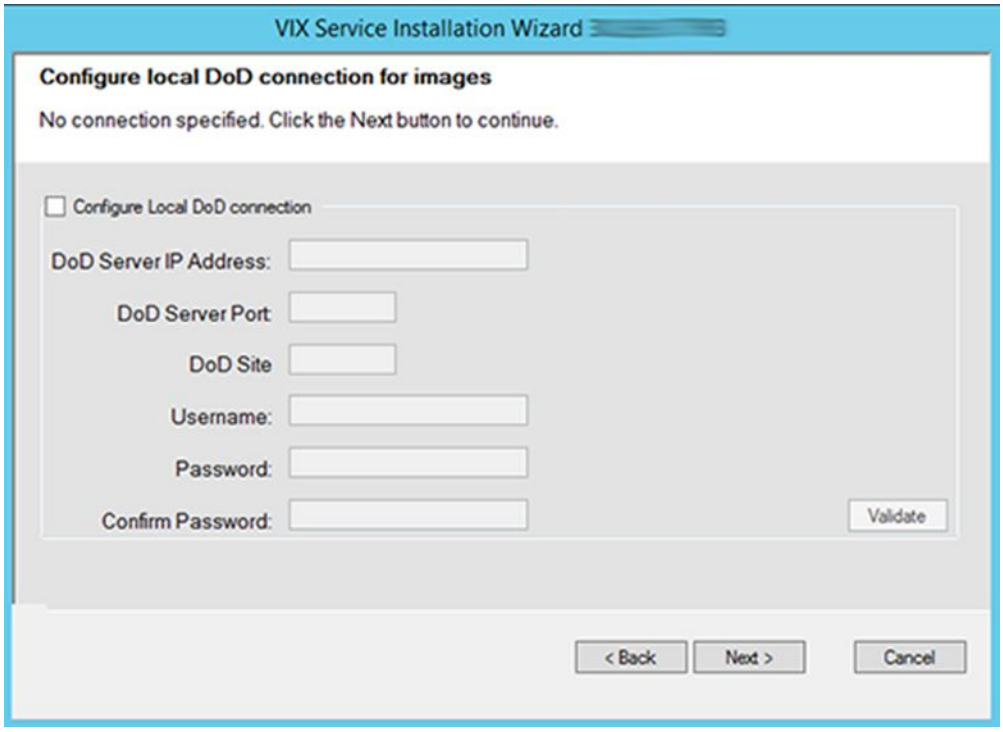
The VIX installation program checks the information. If it detects an error, it displays a tooltip with information about the error. When it validates the configuration, Next becomes available. Click **Next** (Figure 30).

Figure 30: VistA and Email Configuration - Next



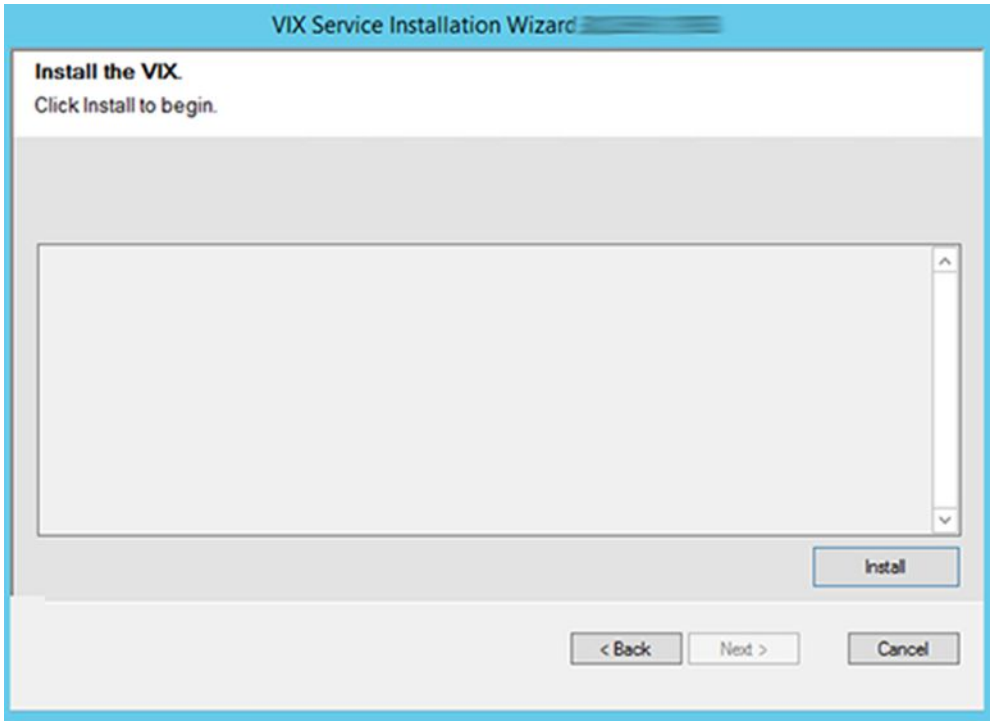
23. In the Configure Local DoD connection page (Figure 31), complete one of the following:
    a. If your site has no local network connection to a DoD facility, click **Next** (this is the case at most VA sites).
    b. If your site has a local network connection to a DoD facility, enter connection information for the DoD's PACS Integrator server. After entering the connection information, click **Validate** to test the connection. Then, click **Next.**

Figure 31: Local DoD Connection for Images Configuration



24. On the Install the VIX page (Figure 32), click **Install**. (The information on this page is saved in C:\Program Files (x86)\VistA\Imaging\VIXInstaller for future reference or troubleshooting.) This starts the installation process.

Figure 32: VIX Install Start



25. During the final install, a PowerShell script utility pops up (Figure 33, Figure 34, Figure 35) to perform additional install tasks and closes when complete.

    NOTE: The PowerShell pop-up performs various configuration and certificate tasks and executes patch specific post-scripts.

    NOTE: If the MUSE service is not enabled, the PowerShell pop-up may display a red error message in the MUSE check section. See Appendix A: Enable MUSE Functionality.

Figure 33: PowerShell Pop-up Script Top Portion

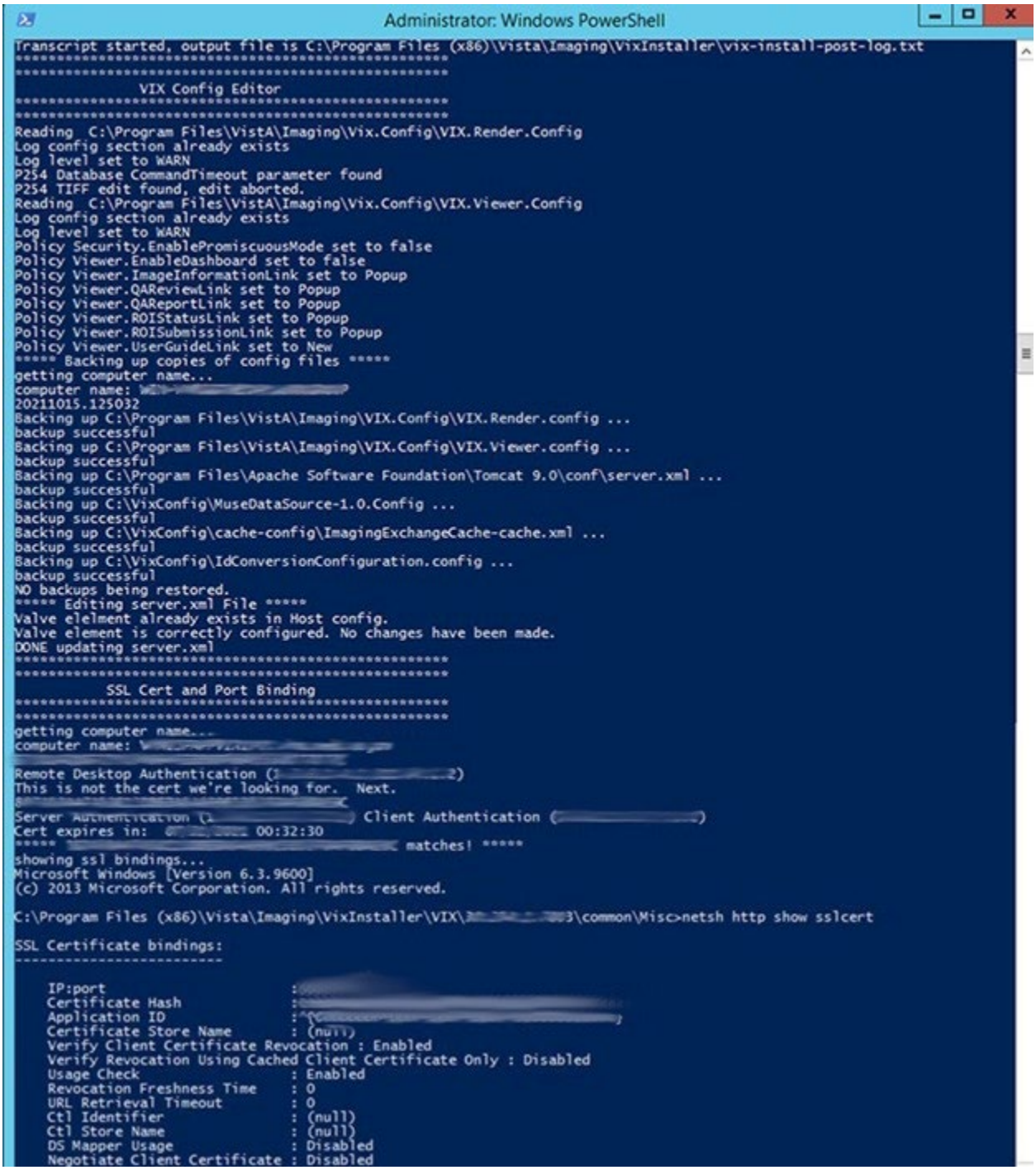


Figure 34: PowerShell Pop-up Script Middle Portion

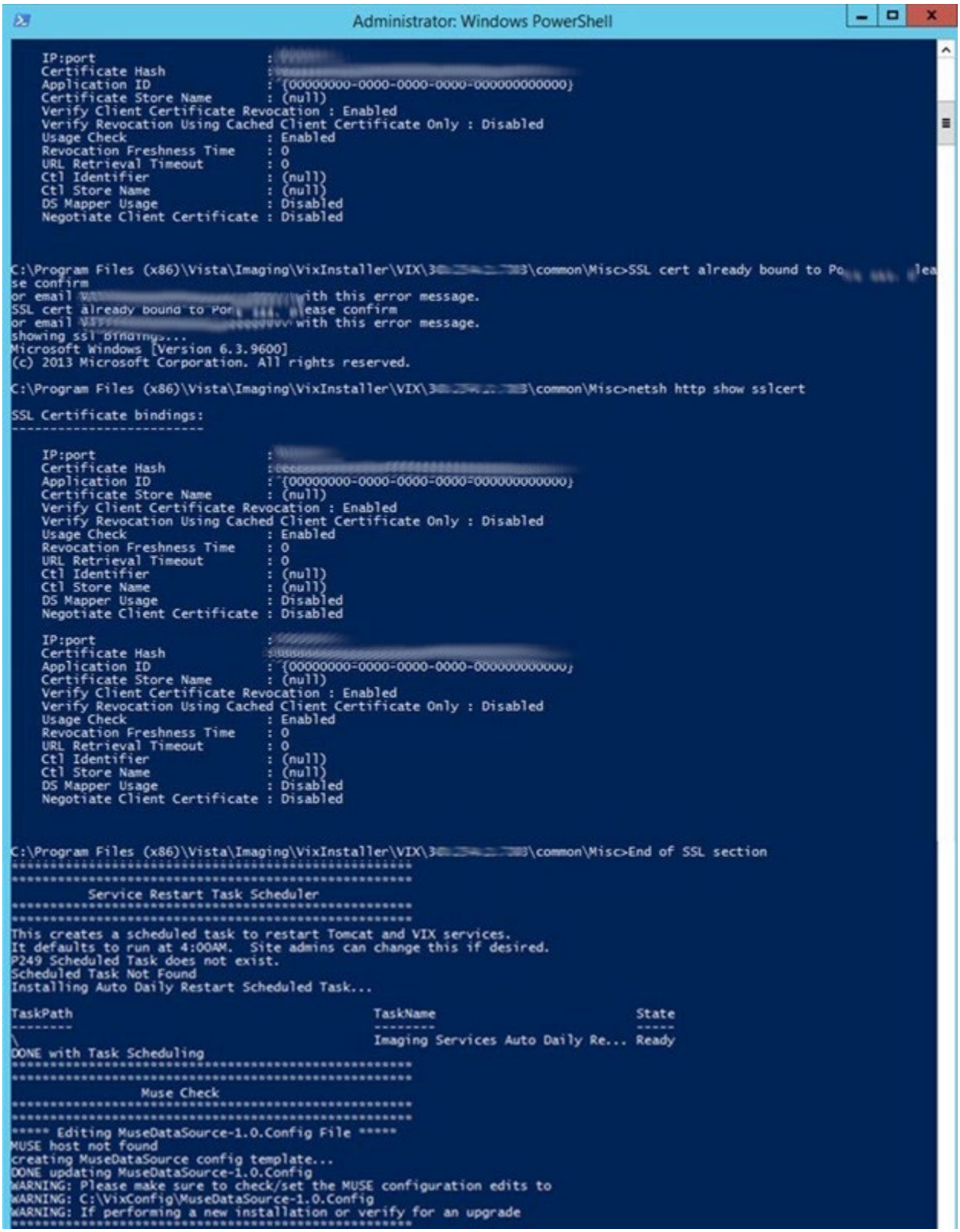
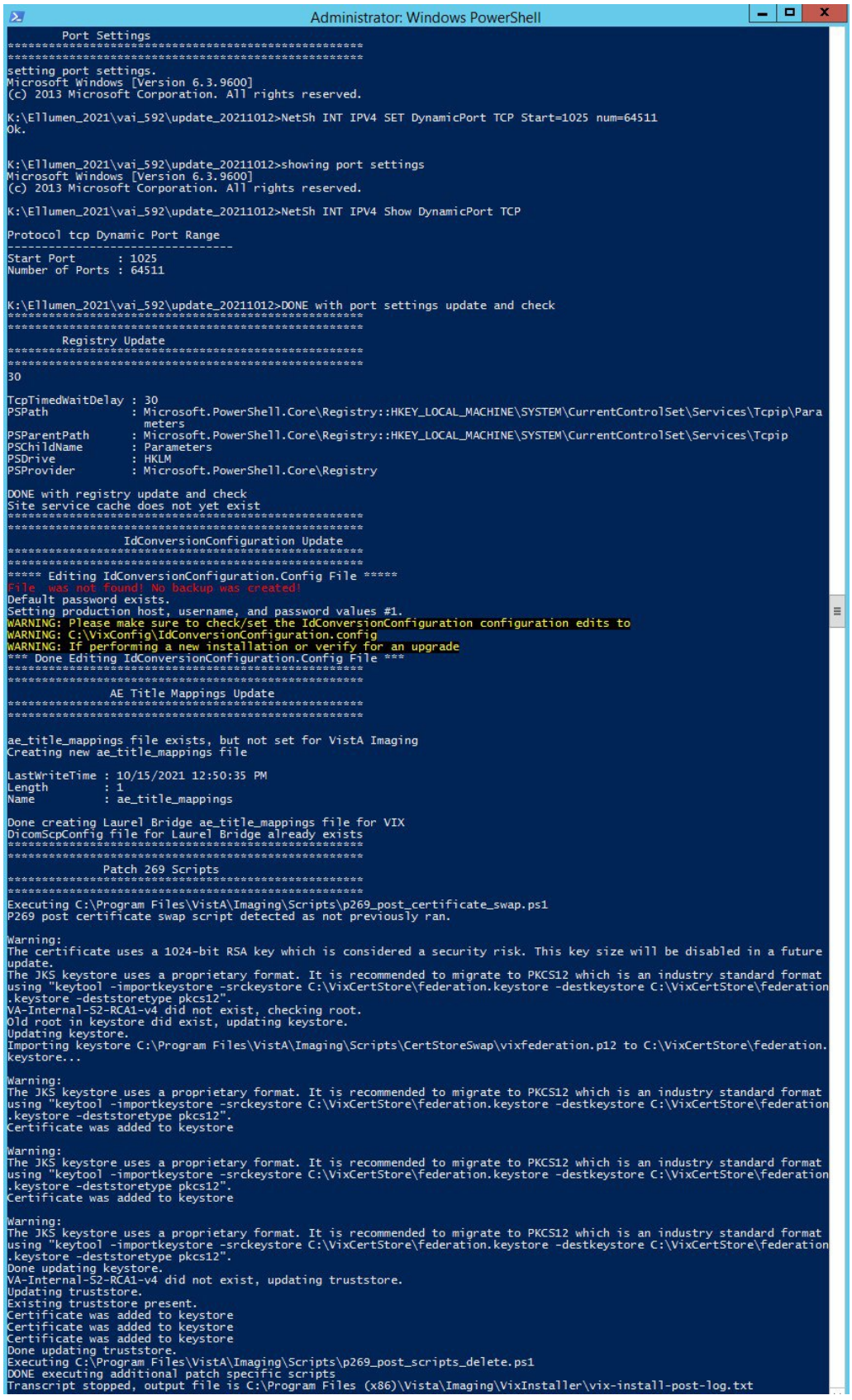
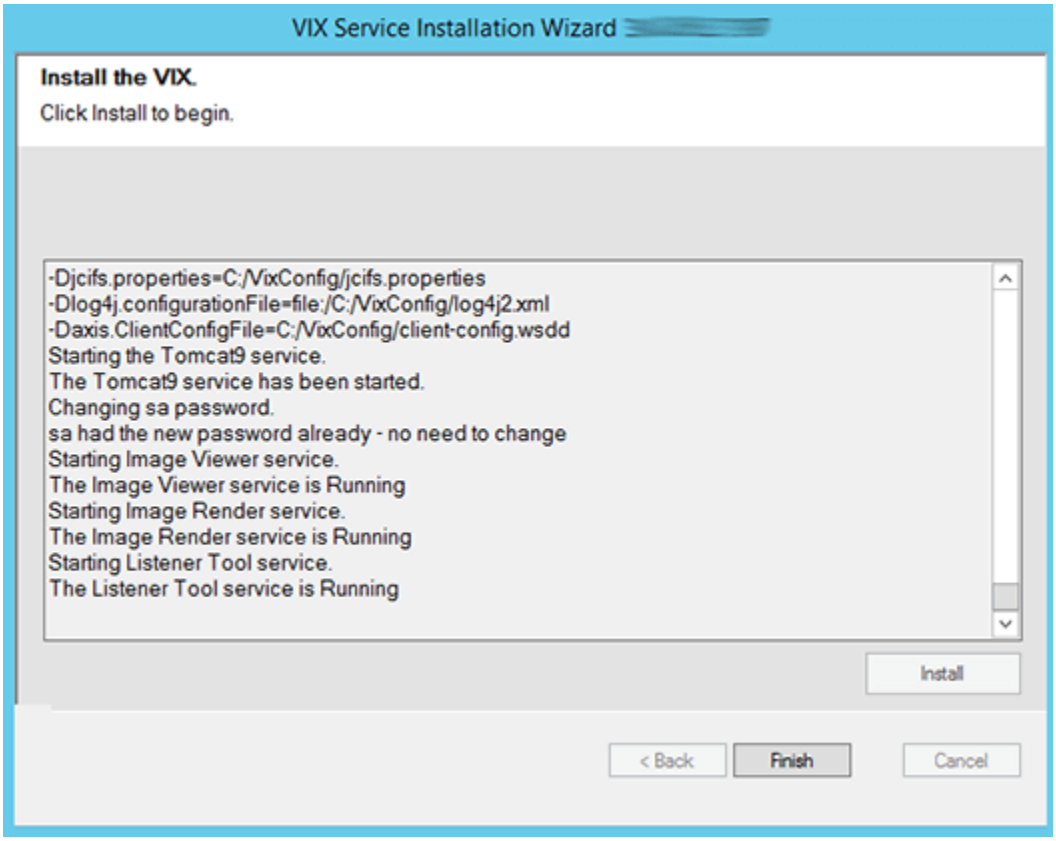


Figure 35: PowerShell Pop-up Script Bottom Portion



26. The VIX starts automatically (Tomcat and Viewer/Render services) when the installation is complete. When the installation is complete, click **Finish** to exit the wizard (Figure 36). The VIX Service Installation Wizard closes.

Figure 36: VIX Install Complete



The VIX cannot be used until it is activated and registered with the VistA Site Service. See the next section for details.

2.4. Activating a New VIX

After the VIX is installed, it is 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 begins to be actively used, both by clinicians at your site and 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 causes errors and timeout issues for Clinical Display users.

2.4.1. 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:

2. Enter a National ticket to Clin 3 for a site service update.
   a. Paste the lines in the preceding step into the ticket.
   b. Include "Add VIX server to Site Service database."
3. Clin 3 notifies you, typically within five business days, when the site service registration is complete.
4. Continue to *Post-Installation for New VIX Installations and Updating Existing VIX Installations.*

3. Updating an Existing VIX

This chapter explains how to update an existing VIX server. An installation checklist that summarizes this process can be found in *Appendix F: VIX Install Checklist*.

3.1. Preparing for a VIX Update

Preparing for a VIX update involves:

- Configuring the MUSE interface. This requires the MUSE username and MUSE password for the site's online MUSE server. If the MUSE username and password are not documented in existing site VistA Imaging documentation, please contact the local BioMed team or MUSE administrator for the information.
- Acquiring Installation File.
    - Copy MAG3_0P269_VIX_SETUP.msi to C:\temp.
    - Copy the MAG3_0P284_VIX_SETUP.msi to C:\temp for the backup plan if not already present.
- Verify the MAG*3.0*269 VistA KIDs package has been installed, see *VistA Software Dependencies.*
- Ensure downtime has been scheduled to install the VIX service. Local administrations of the applications and services impacted by an offline VIX should be contacted prior to installing the MAG3_0P269_VIX_SETUP.msi. The installation needs to be coordinated to avoid any disruption of services. This communication should be done in advance of the VIX update, see *Scheduling Downtown and Impact of a VIX Update.*

TIP: VIX-specific account passwords and security key assignments established for older VIX systems automatically carry over to new VIX systems.

NOTE: It is strongly suggested to restart the VIX Server prior to updating an existing VIX.

3.1.1. 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.

3.1.2. Scheduling Downtown and Impact of a VIX Update

You need to schedule downtime with appropriate personnel for the duration of the VIX installation. Schedule 1 to 2 hours for the downtime and notify users of the impact of the VIX update.

While the VIX server is being updated, VIX assisted functions are unavailable. The list of known applications and services impacted by a local offline VIX includes:

- Clinical Display access to remote images may be temporarily inaccessible.
- VistARad access to remote images and other teleradiology features.
- DICOM Importer client.
- Local JLV user display of images (local or remote).
- Signed Informed Consent ability to store new consents.

- Any new Ingest consuming application.
- Integrated Visualization System (IVS) mobile application access to local images.
- Enterprise DICOM Q/R functionality.
- Access to DoD images or artifacts.
- Access to VA Cerner images or artifacts.
- Any other external application calling a local VIX service directly.

Table 1 summarizes how a VIX outage affects clinicians.

Table 1: Functions Affected by VIX Updates

Clinical Group	Impact
Local Clinical Display Users	DoD images are inaccessible for the duration of the VIX shutdown. Remote VA images may be temporarily inaccessible. Clinical Display attempts 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 ensure that Clinical Display is no longer using pre-VIX remote image views for remote sites.
Local VistARad Users	Remote exam data and images and monitored exam lists are unavailable. For additional information, refer to the documentation for VistARad.
Remote VA or DoD Clinicians requesting Images or Artifacts	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 are unable to retrieve locally stored images for the duration of the VIX shutdown.
Local DICOM Importer Users	The DICOM importer client cannot log into VistA and process imports for the duration that the VIX is down.
VIX Image Viewer/JLV Users	Clinical users of JLV cannot access images or artifacts (local or remote) using the VIX image viewer.
iMedConsent Users	Patients' consent forms are unavailable. Currently, this results in multiple unsigned Text Integration Utility (TIU) notes in Computerized Patient Record System (CPRS) due to CVIX and iMedConsent Web (ICW) deficiencies until the necessary corrective action(s) can be deployed by both the CVIX and ICW development teams.
IVS Mobile Application Users	IVS mobile application users cannot access local images.

3.2. Preparing Service Account and Passwords

New with MAG*3.0*269: Before starting the VIX server update process, identify your DICOM query retrieve/Release of Information (ROI) periodic processing VistA Imaging VistA service account. It is suggested to update the name of the VistA service account as described in *Appendix E: Service Account Settings*. To ensure DICOM query retrieve/ROI periodic processing functionality, update the SSN of the service account and verify it has the security keys, secondary menu options, a value for the INITIAL field, and additional options as described in *Appendix E: Service Account Settings*.

Locate the current password used for the Apache Tomcat administrator account and DICOM query retrieve/ROI periodic processing VistA Imaging VistA service account credentials.

- The Apache Tomcat administrator password is case sensitive, must contain at least **fourteen (14) alphanumeric characters**, and must contain at least one capital letter and one number.

3.3. Pre-Installation Configuration

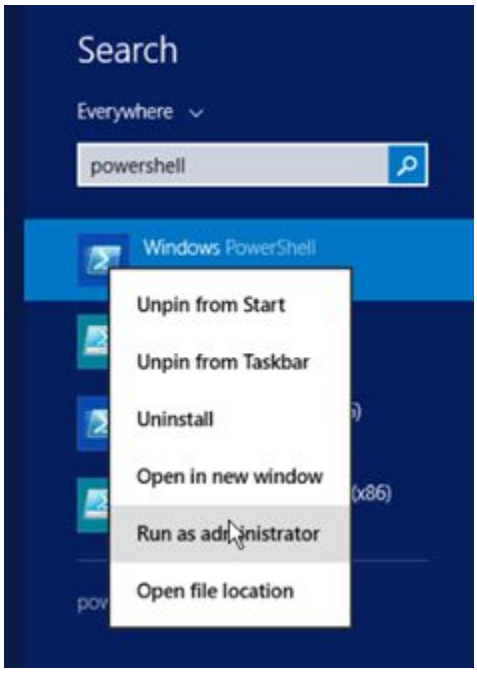
New with MAG*3.0*269: Due to the VA group policy restriction or rules, there may be an issue found while the VIX installer wizard is setting file system access rules.

Check the current size of the YOUR_DRIVE_LETTER:\VixCache folder. Open Windows Explorer and navigate to the YOUR_DRIVE_LETTER:\VixCache folder. Left-click on the VixCache folder and right-click on properties. Note the current size of the VixCache folder.

If the current size of the VixCache folder exceeds 2 GB it is suggested to clear (delete) the contents of the subfolders in the YOUR_DRIVE_LETTER:\VixCache folder to avoid lengthy installation times and potentially prevent a hanging install. Use the following steps to delete the contents of the YOUR_DRIVE_LETTER:\VixCache folder:

1. Run PowerShell as an administrator (Figure 37).
    a. Right-click **Start**.
    b. Left-click **Search**.
    c. Type **powershell**.
    d. Right-click **Windows PowerShell**.
    e. Left-click Run as administrator.

Figure 37: Execute Windows PowerShell



2. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes**.
3. Once PowerShell launches, **type** the command:

   ```
   $vixLocalCachePath =
   [System.Environment]::GetEnvironmentVariable('vixcache') -
   replace "/", "\"
   ```

   Then press **[ENTER]** to set the path of YOUR_DRIVE_LETTER:\VixCache.

   NOTE: If the system variable for the vixcache is not set, use the below command instead and replace YOUR_DRIVE_LETTER with your drive letter of the VixCache folder.

   ```
   $vixLocalCachePath = "YOUR_DRIVE_LETTER:\VixCache"
   ```

4. Now **type** the command:

   ```
   Get-ChildItem -Path "\\?\$($vixLocalCachePath)" -Recurse |
   Foreach-object {Remove-item -Recurse -Force -path
   $_.FullName}
   ```

   Then press **[ENTER]** to delete the sub-folders in YOUR_DRIVE_LETTER:\VixCache.
5. Once the command completes, close PowerShell.

3.4. Performing a VIX Server Update

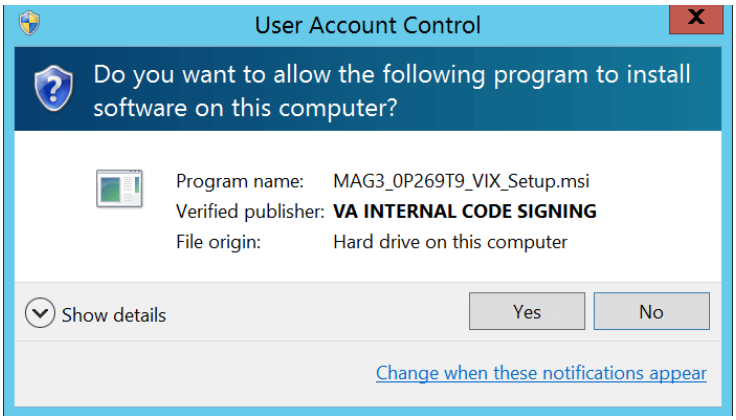
Use the following steps to update a VIX server.

NOTE: You do not have to stop any currently running services because this install process automatically stops them for you.

1. Use an administrator-level account to log onto the VIX server.

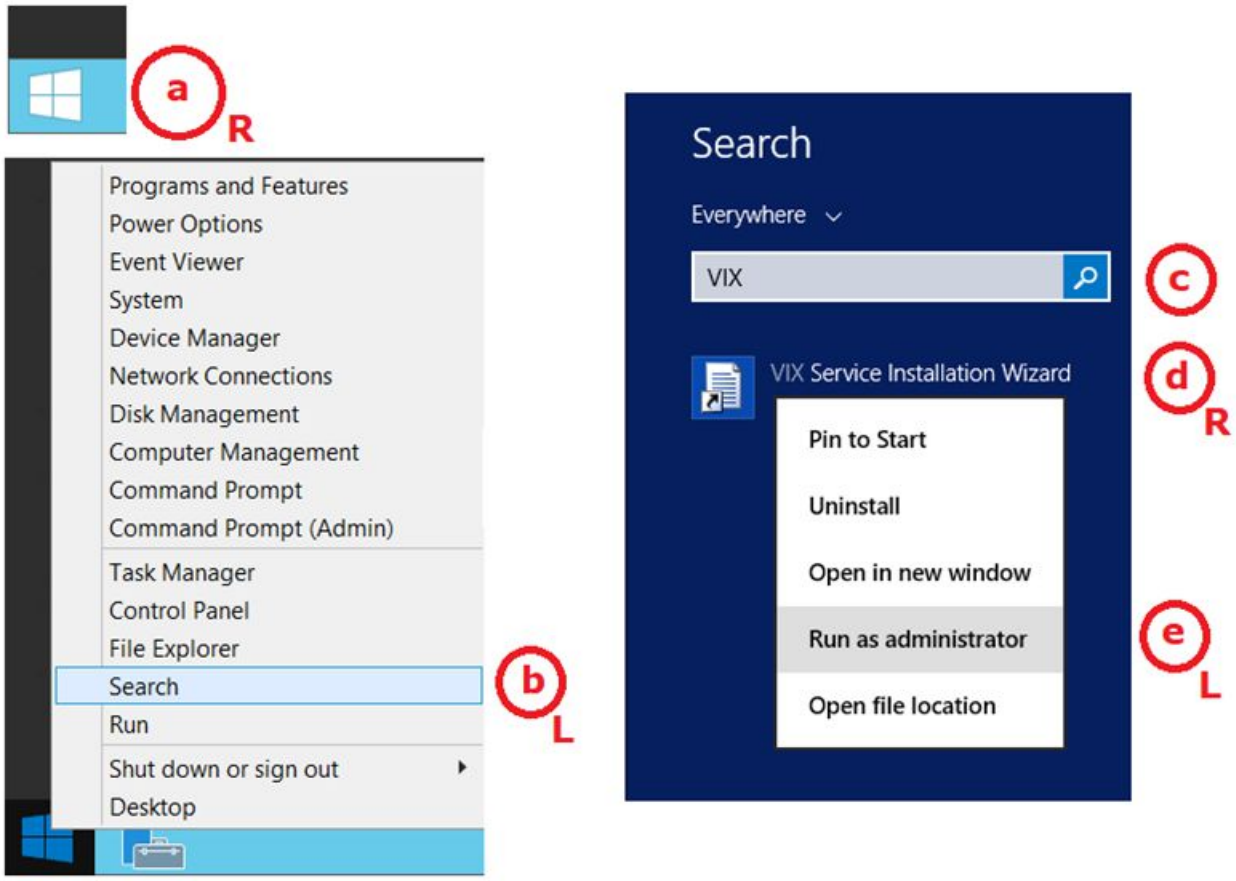
2. If you did not already do so in Section 0, copy the VIX installation file `MAG3_0P269_VIX_SETUP.msi` to C:\temp on the VIX server. (Download if required, see the patch description of the patch for the download location).
3. Go into Control Panel/Programs/Programs and Features, and remove the prior VIX Service Installation Wizard by right-clicking on it and choosing Uninstall.
4. To Install the VIX Service Installation Wizard perform the following steps:
   a. Right-click the **VIX installation** file (MAG3_0P269_VIX_SETUP.msi) and click on Install.
   b. If prompted with "Do you want to allow the following program from a verified publisher to make changes to this computer?", click **Yes** (Figure 38)

Figure 38: User Account Control - Vix Service Installation Wizard



   c. When the Welcome page displays, click **Next**.
   d. When the Confirm Installation page displays, click **Next**.
   e. When the Installation Complete screen displays, click **Close**.
5. Run the VIX Service Installation Wizard as an administrator (Figure 39).
   a. **R**ight-click **Start**.
   b. **L**eft-click **Search**.
   c. Type **VIX**.
   d. **R**ight-click VIX Service Installation Wizard.
   e. **L**eft-click Run as administrator.

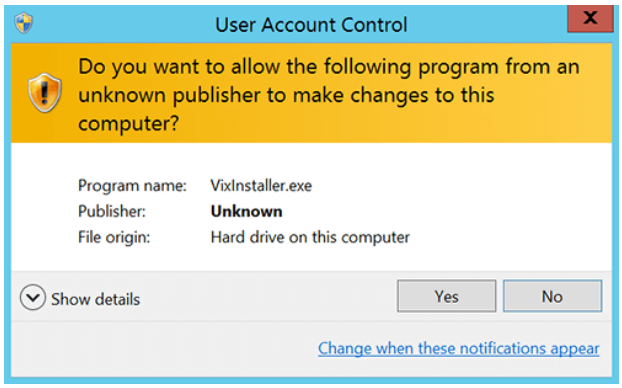
Figure 39: Run the VIX Service Installation Wizard



NOTE: If the VIX Service Installation Wizard does not appear in the Search bar as in Figure 39, open Windows Explorer and navigate to the **C:\Program Files (x86)\Vista\Imaging\VixInstaller** folder, **r**ight-click **VixInstaller.exe** and **l**eft-click **Run as administrator**.

6. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes** (Figure 40).

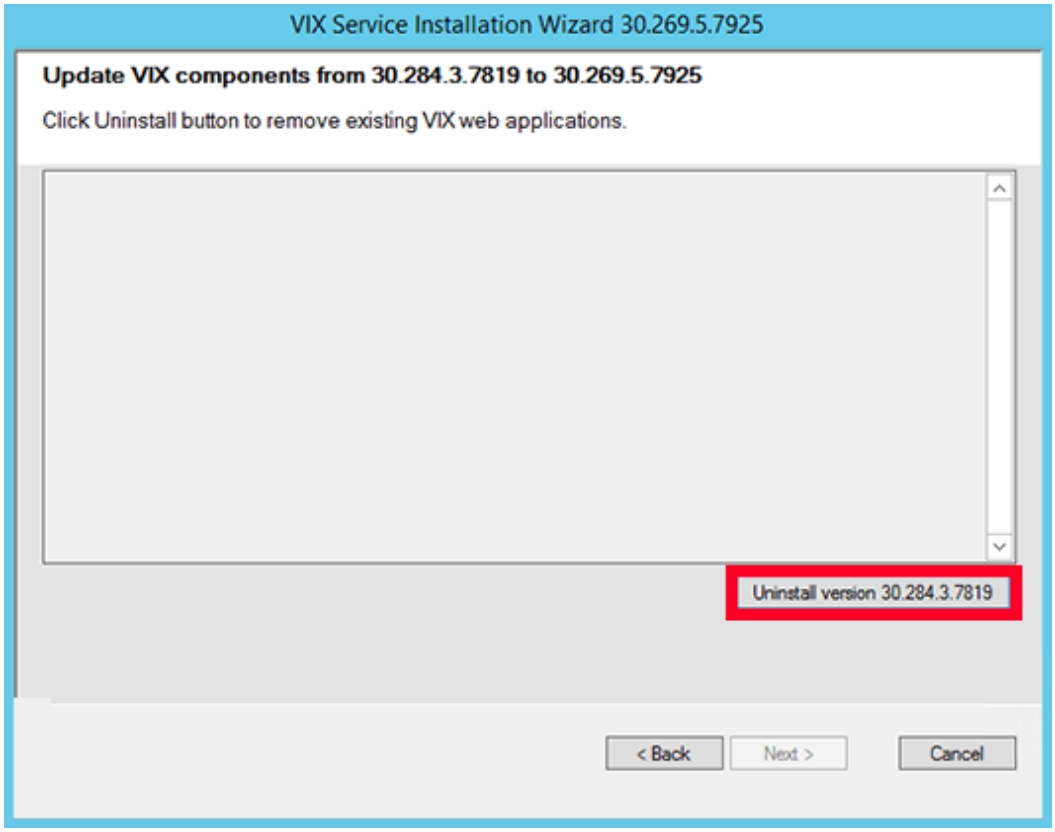
Figure 40: User Account Control - VixInstaller



7. When the Welcome page for the VIX Service Installation Wizard displays, click **Next.**

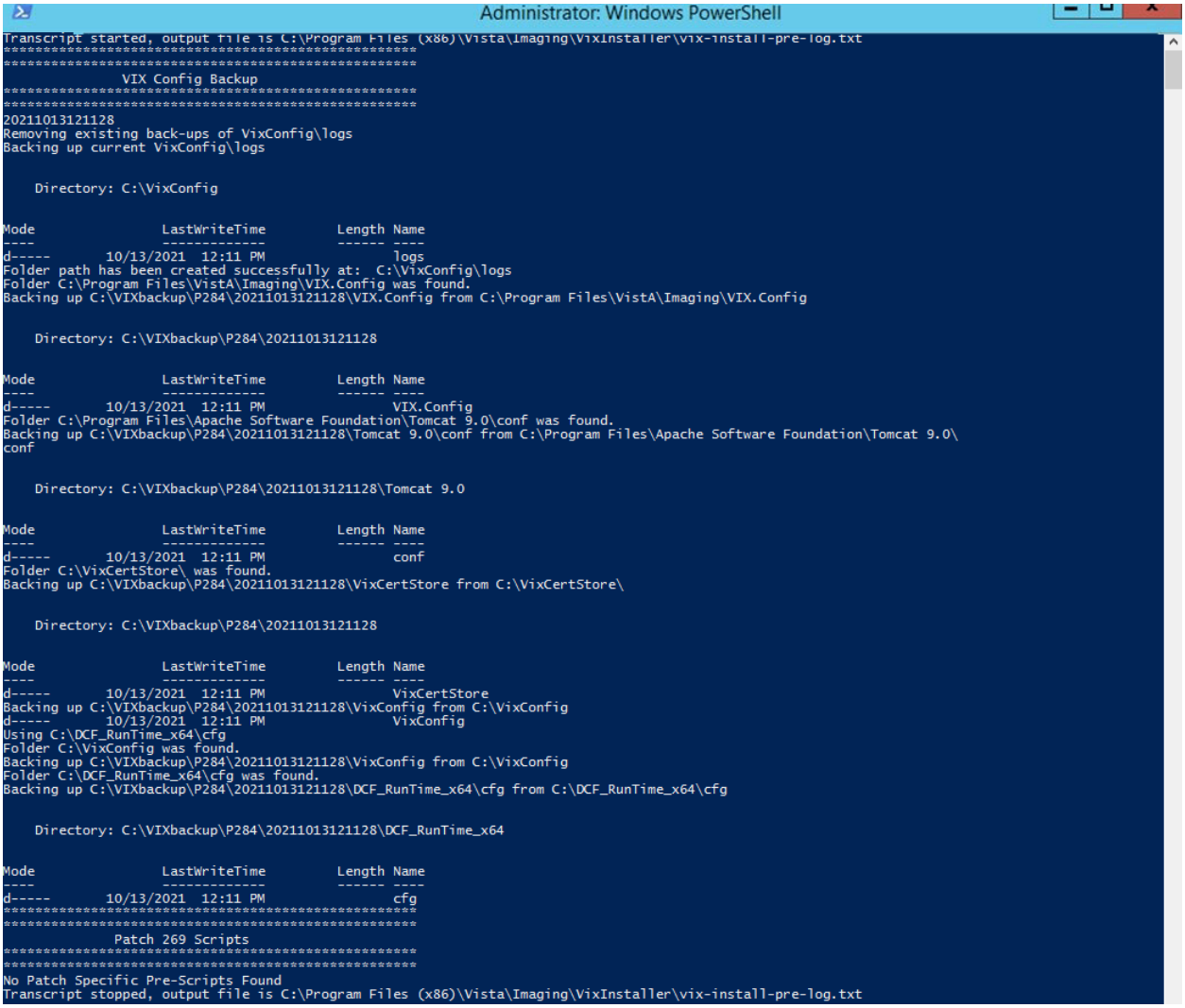
8. **Click** on the button labeled **Uninstall version 30.284.3.7819** to uninstall (Figure 41) the pre-existing VIX software. (If it is not already stopped, the wizard gracefully stops the VIX service before performing the uninstall.)

Figure 41: Update VIX Components



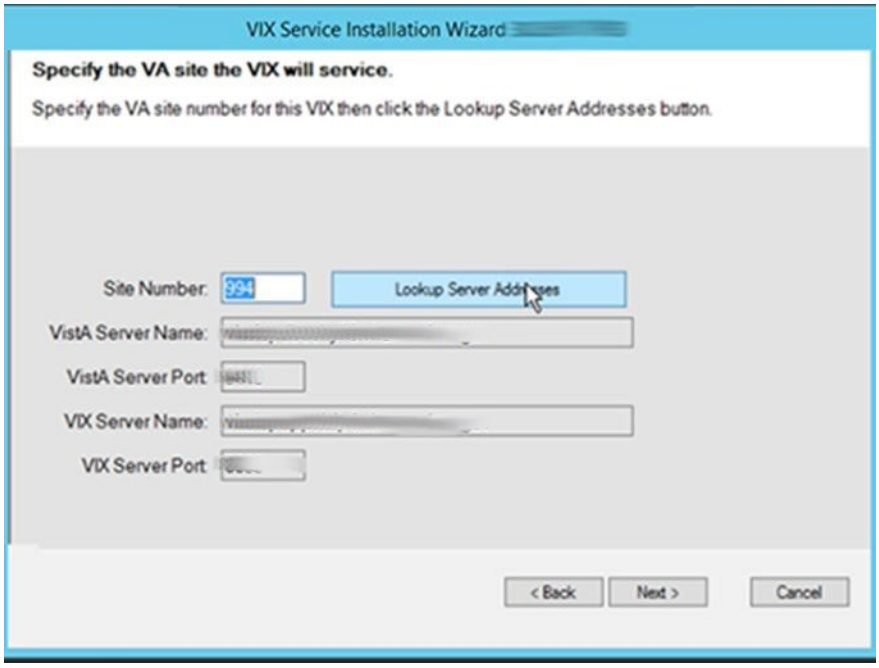
9. During the uninstall, a PowerShell script utility pops up (Figure 42) to perform back-ups of prior configuration files and, if present, execute any patch-specific pre-scripts. The PowerShell window closes when complete.

Figure 42: Update VIX Components PowerShell Pop-up Script



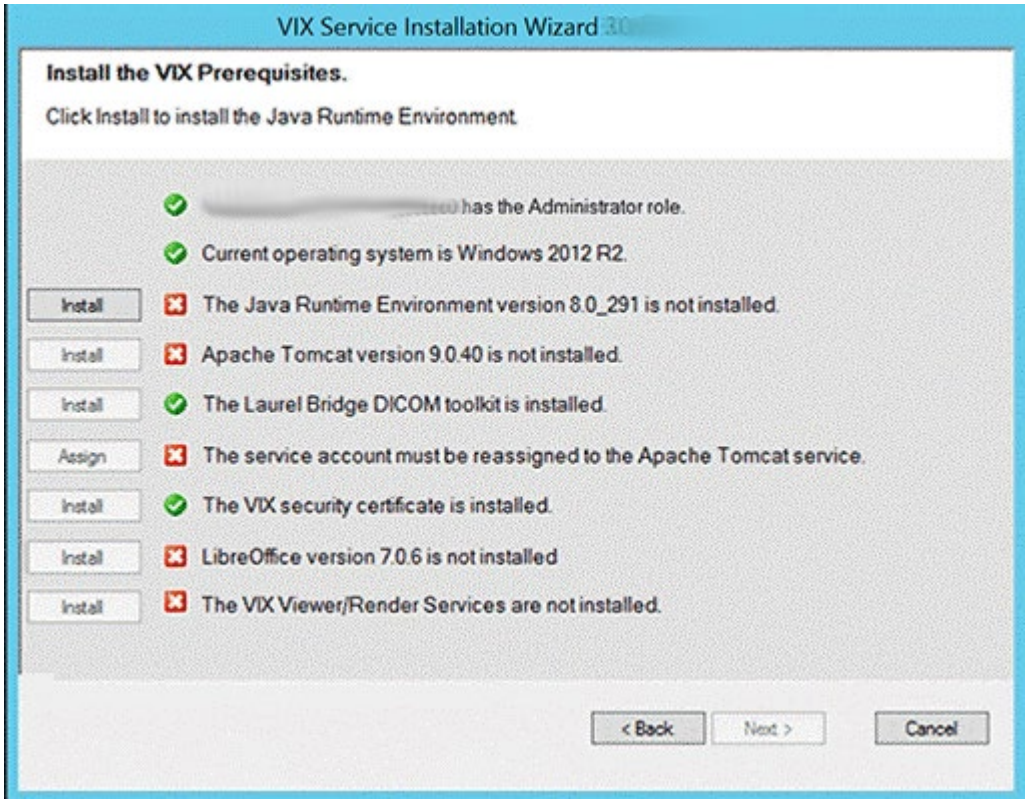
10. When the Uninstall is complete, **Press Next to continue** displays in the VIX Service Installation Wizard, click **Next.**
11. In the **Site Number** field of the "Specify the VA Site the VIX will service" page, verify that the **Site Number** box shows your STATION NUMBER (field (#99) in the INSTITUTION file (#4) of your site, the information is in FileMan in VistA).
12. Confirm the connection by clicking **Lookup Server Address**. Then click **Next** (Figure 43).

Figure 43: VIX Service Installation Wizard



13. Please be patient for the VIX Prerequisites page to appear, as it may take a while. When the Install the VIX Prerequisites page displays, read the line that indicates the state of the Java Runtime Environment. If ✅ displays, skip to the next step. If ❌ displays (Figure 44), do the following:
    a. Click **Install**.
    b. Wait until the status icon for the Java Runtime Environment changes to ✅. (This install of Java may take over five minutes to complete. Please be patient, as this step may take a while to complete.)

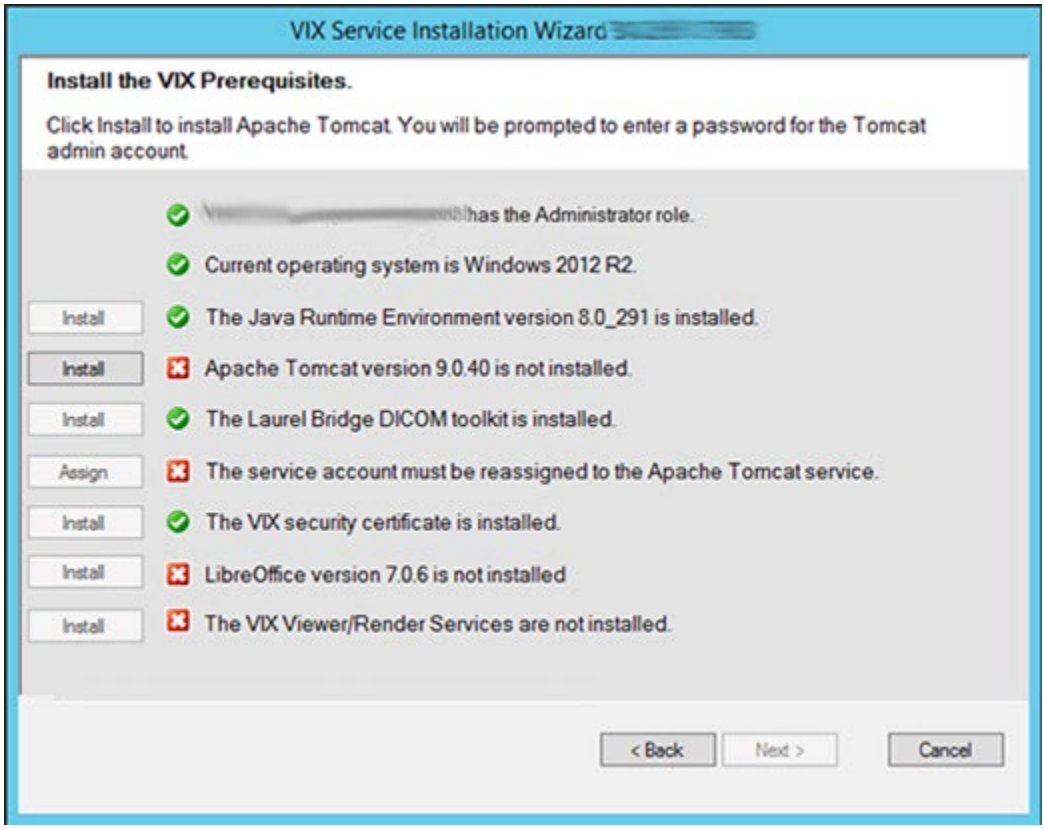
Figure 44: VIX Prerequisites - Java Not Installed



NOTE: The person installing the VIX software does not need to be in the VHAMASTER domain. The installer's domain should appear with their name. This (and subsequent screenshots) is just an example of what the installer sees.

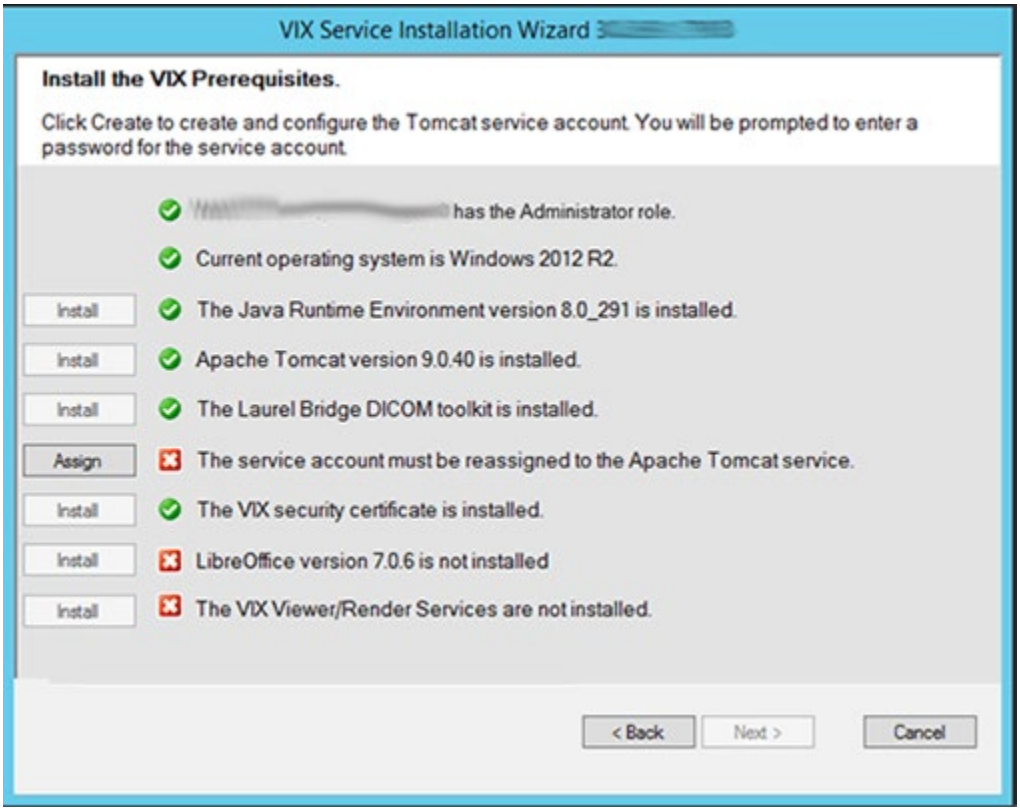
14. On the same page, read the line that indicates the state of the Apache Tomcat installation. If ✓ displays, skip to the next step. If ✗ displays (Figure 45), do the following:
    a. Click **Install**.
    b. Wait until the status icon for Apache Tomcat changes to ✓. (This install of Tomcat may take over five minutes complete. Please be patient, as this step may take a while to complete.)

Figure 45: VIX Prerequisites - Tomcat Not Installed



15. On the same page, check the line that indicates the state of the Laurel Bridge toolkit. Verify ✅ displays. If ❌ displays, refer to the *Laurel Bridge DCF Toolkit* instructions to obtain an updated serial number and activation code.
16. On the same page, read the line that indicates the state of the service account. If ✅ displays, skip to the next step. If ❌ displays, do the following:
    a. Click **Assign** (Figure 46).

Figure 46: Apache Tomcat Service Account Password

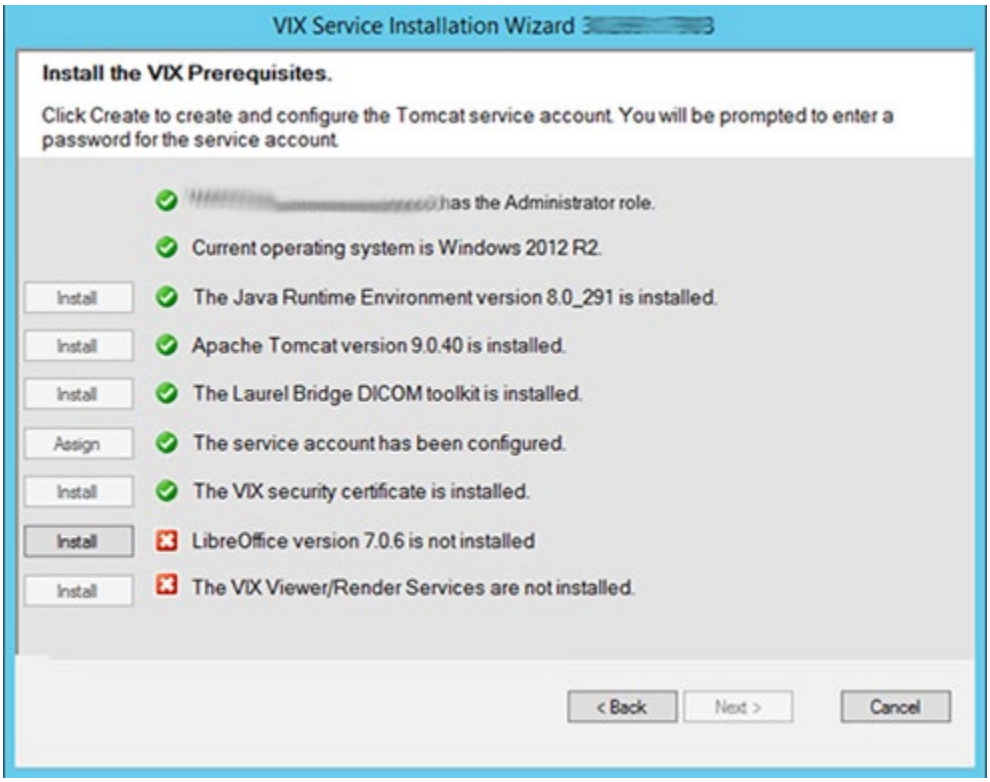


b. In the dialog box that displays enter the Windows service account password that you previously prepared in *Preparing Passwords, Activating Components, and Staging Files*. Then click **OK**.
   - The password is case sensitive, must contain at least **fourteen (14) alphanumeric characters,** and must contain at least one capital letter and one number.

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

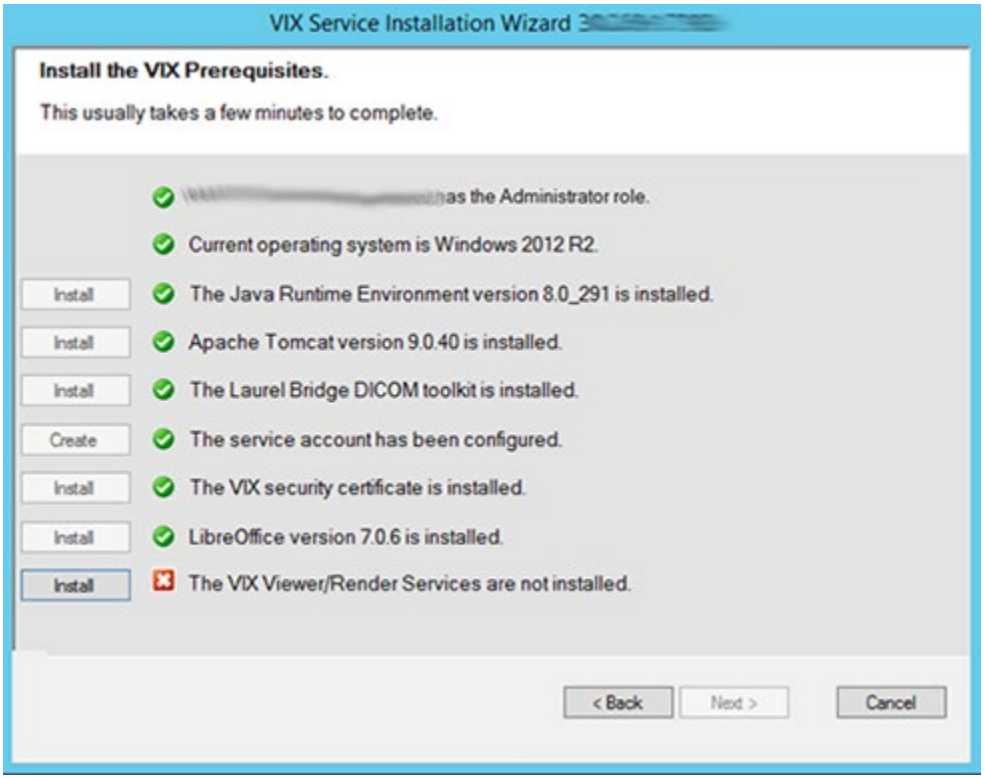
17. On the same page, check the line that indicates the state of VIX security certificate. Verify ✅ displays.
18. On the same page, read the line that indicates the state of the LibreOffice installation. If ✅ displays, skip to the next step. If ❌ displays (Figure 47), do the following:
    a. Click **Install**.
    b. Wait until the status icon for LibreOffice changes to ✅. (This install of LibreOffice may take several minutes to complete. Please be patient, as this step may take a while to complete.)

Figure 47: VIX Prerequisites - LibreOffice Not Installed



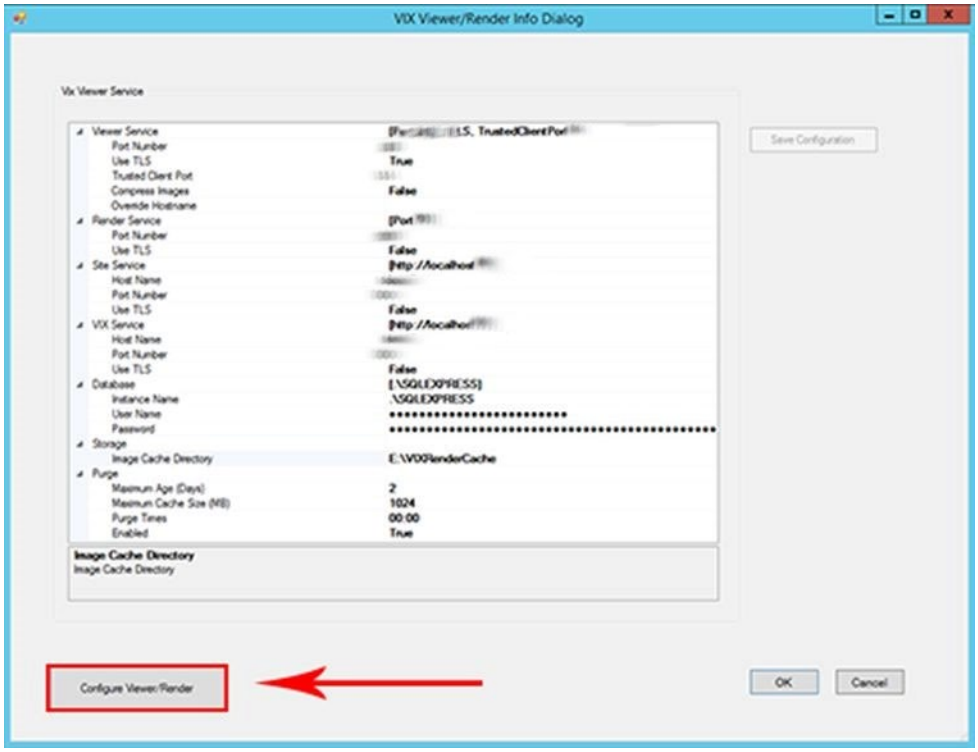
19. Read the line that indicates VIX Viewer/Render Services.
    a. If displays, click **Install** (Figure 48). If displays, click **Reinstall.**

Figure 48: All Services Except VIX Viewer/Render Installed or Configure



b. Click **Configure Viewer/Render** (Figure 49).

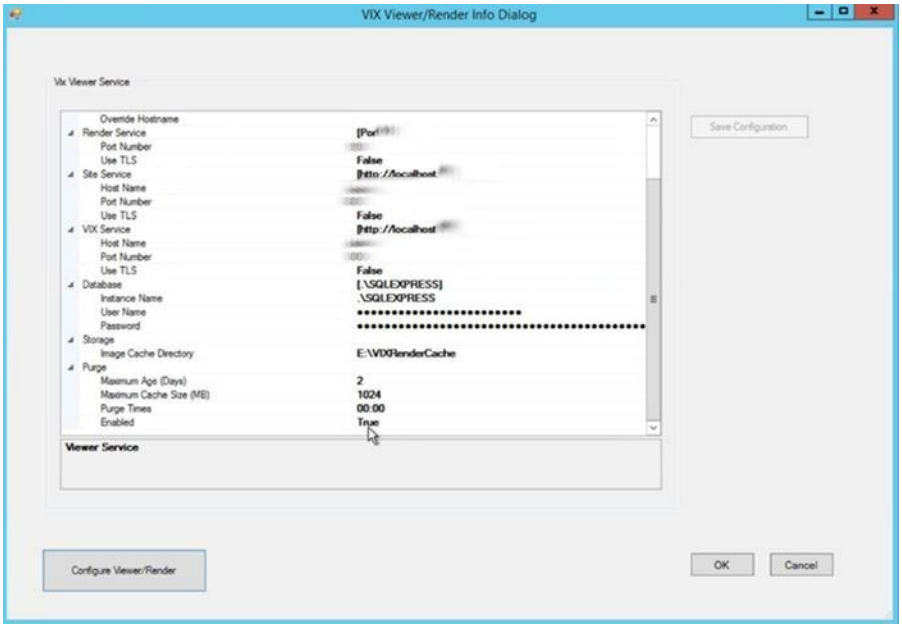
Figure 49: VIX Viewer/Render Info Dialog Screenshot



c. Verify the following settings:
   i. Verify the viewer port number is REDACTED.
   ii. Verify the trusted client port is REDACTED.
   iii. Verify Site Service > Host Name is localhost.
   iv. Verify Site Service > Port Number is REDACTED.
   v. Verify VIX Service > Host Name is localhost.
   vi. Verify Database > Instance Name is ".\SQLEXPRESS
d. Verify the image cache directory drive is the dedicated VIX cache drive. (i.e. "E:\VIXRenderCache").

   NOTE: The 'Save Configuration' button does not activate unless you changed the configuration (Figure 50).

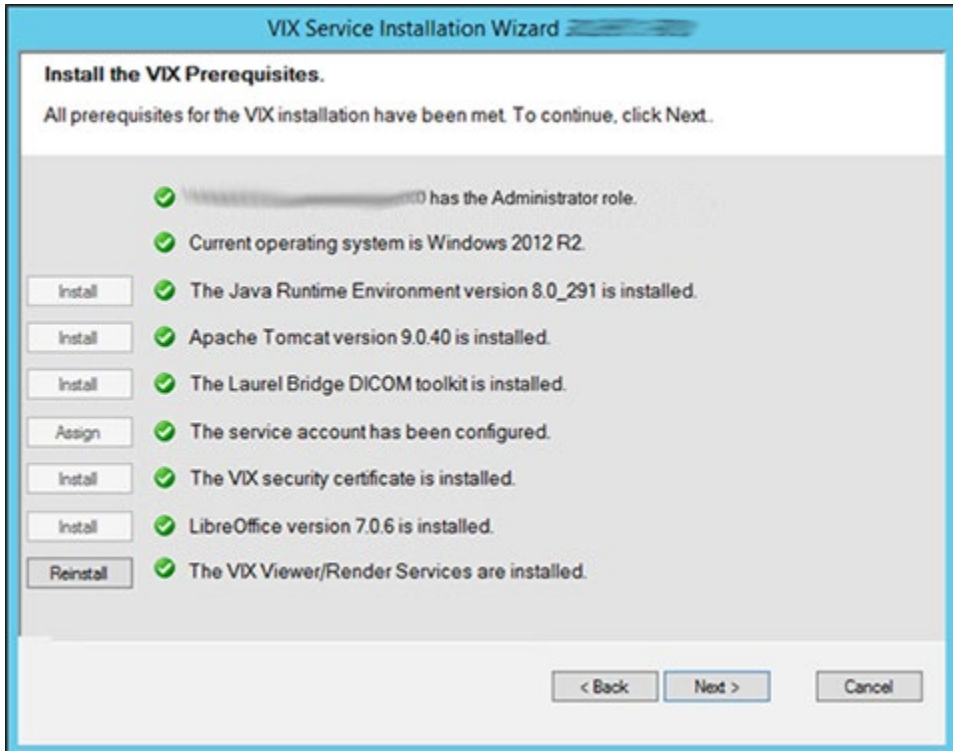
Figure 50: Save/Configuration Button



e. Click **OK**.
f. The installation updates the VIX Viewer/Render Services in the background. This takes approximately three to five minutes to complete.

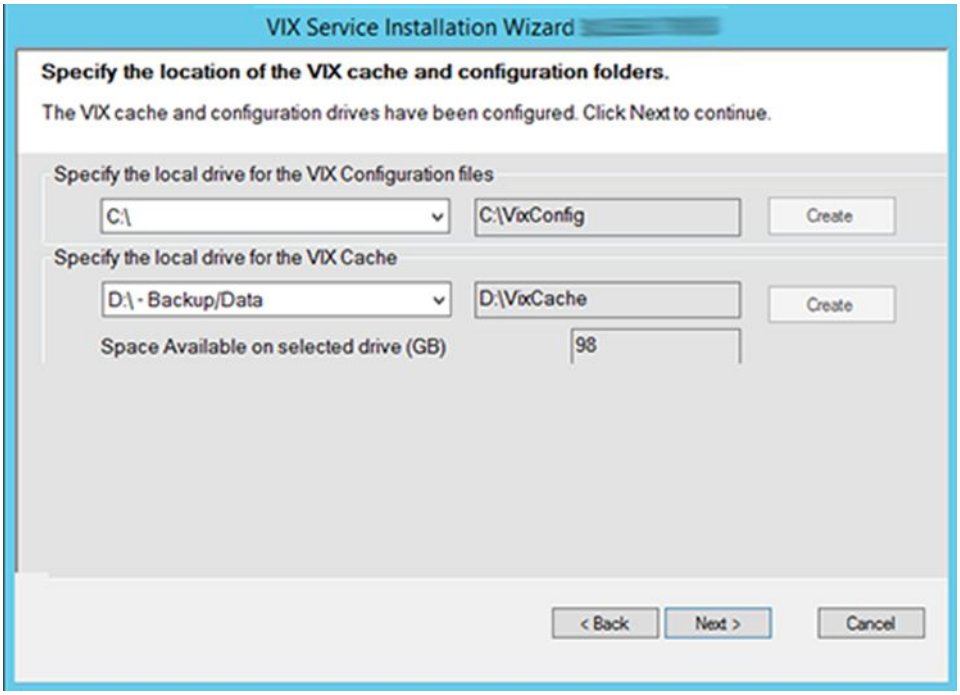
20. Once the VIX Viewer/Render Services have updated, the Install the VIX Prerequisites page updates with a ✔ icon. Confirm that all the icons are ✔ and click **Next** (Figure 51).

Figure 51: All VIX Prerequisites Installed or Configured



21. In the Specify the location page, if you want to keep your existing locations, click **Next**. If you want to change them, select the "C:\" drive for VixConfig folder and the dedicated VIX cache drive for the VixCache folder for your site. Ensure the dedicated VIX cache drive correctly points to the drive letter that is currently being used, for example, "D:\VIXCache" as displayed in Figure 52. For each folder, click **Create** to confirm and create the folders.

Figure 52: VIX Cache and Configuration Folder Creation



22. In the Specify the VistA and Email Configuration, specify the access and verify codes for the account with the VistA credentials. If the email address(es) has changed, specify the email address(es) that gets notifications for invalid credentials. You can enter several email addresses, separated by a comma. Click **Validate** (Figure 53).

    NOTE: The VIX uses this account for periodic processing of ROI disclosure requests and DICOM query retrieve SCP requests. The account must be valid VistA credentials and have the settings described in *Appendix E: Service Account Settings*.

    NOTE: The VIX sends an email notification to the address or addresses specified if the ROI periodic processing credentials are expired or invalid.

23. In the Specify the VistA and Email Configuration, after it validates the configuration, **Next** becomes available. Click **Next** (Figure 54).

    NOTE: During VistA Configuration validation, the VIX installation program checks the information. If the installation program detects an error, it displays a tooltip with information about the error.

Figure 53: Specify the VistA and Email Configuration - Before Validate

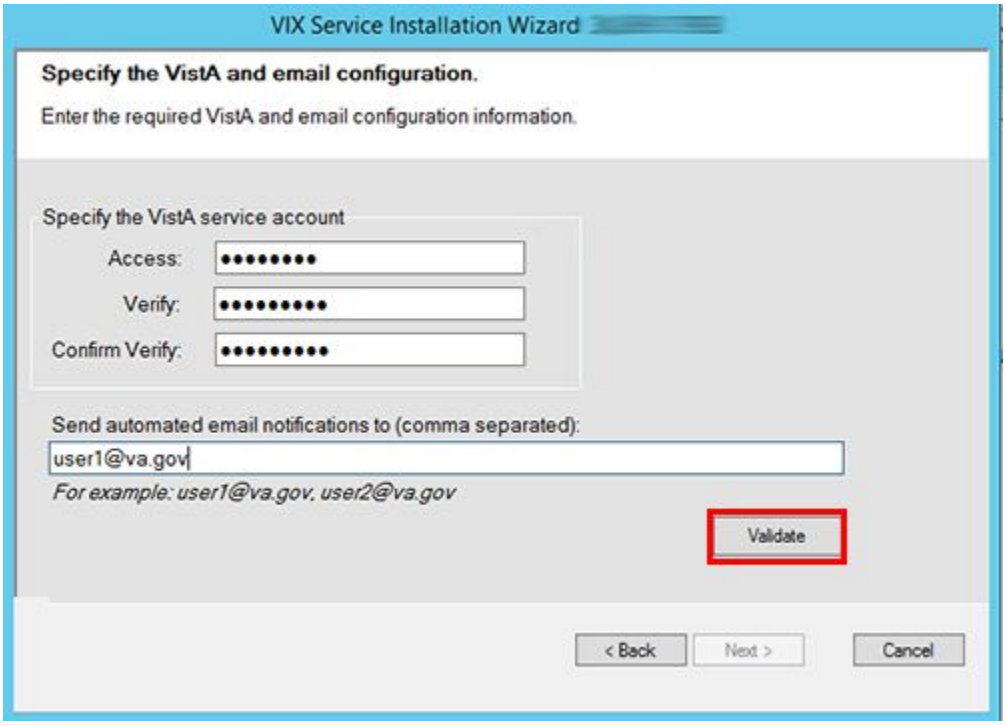
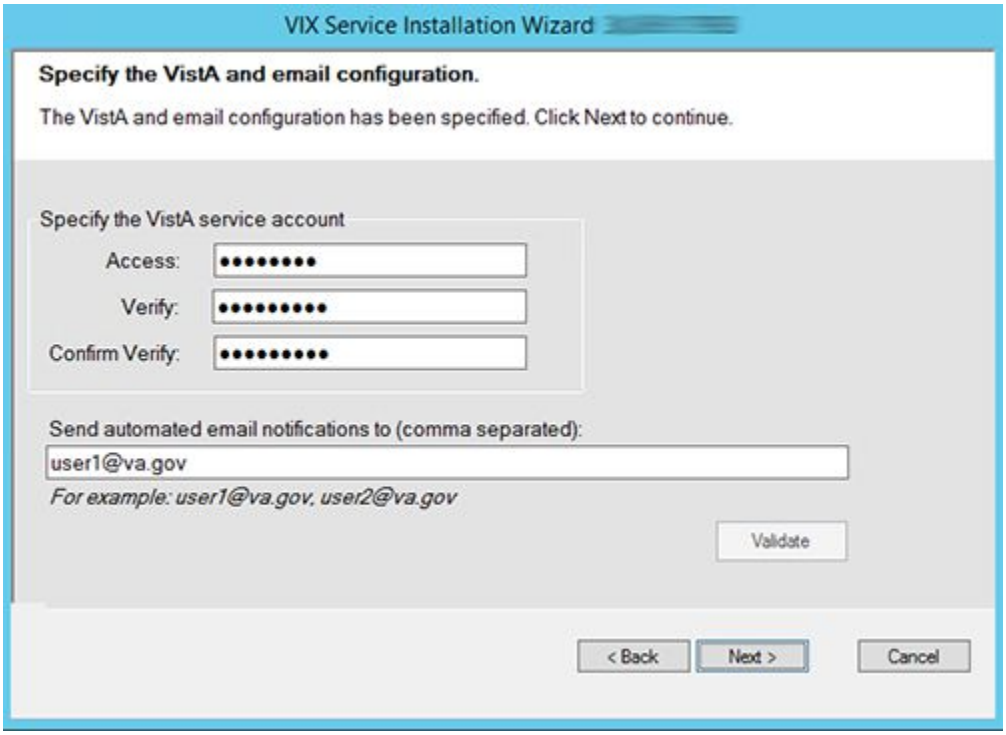


Figure 54: Specify the VistA and Email Configuration - After Validate

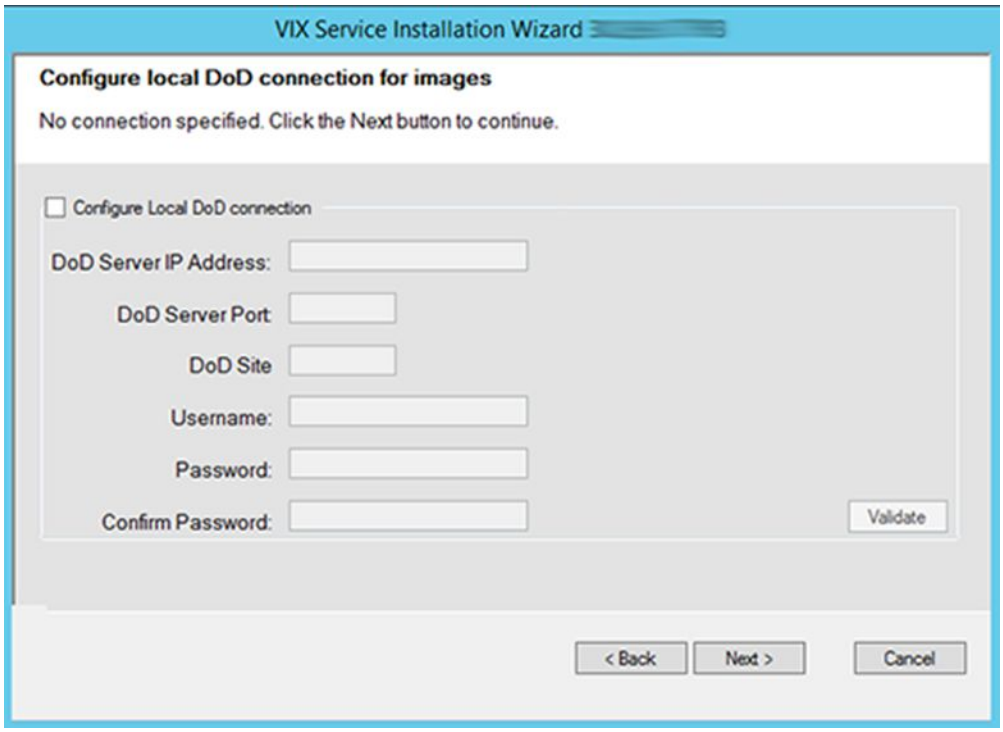


24. In the Configure Local DoD connection page (Figure 55), if the DoD connection information has not changed since the last time you ran the installer and you want to keep the existing values, click **Next.**

    If you want to change the DoD connection information, perform the following:

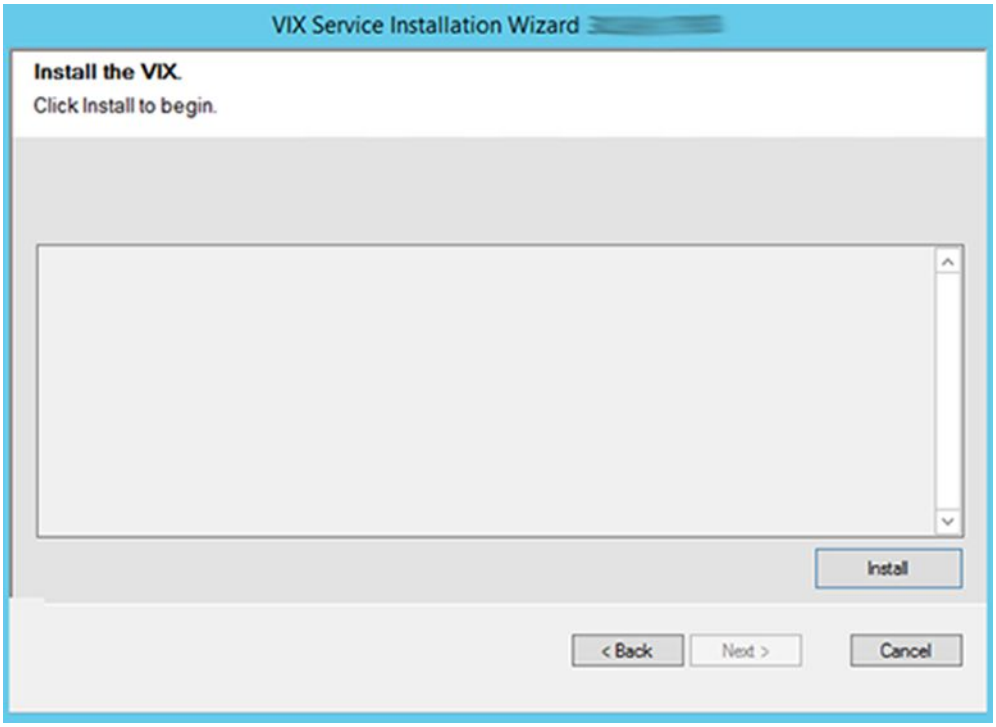
a. If your site has no local network connection to a DoD facility, click **Next**. This is the case at most VA sites.
b. If your site has a local network connection to a DoD facility, enter connection information for the DoD's PACS Integrator server. After entering the connection information, click **Validate** to test the connection. Then, click **Next**.

Figure 55: Configure Local DoD connection



25. On the Install the VIX page (Figure 56), click **Install.** (The information on this page is saved in C:\Program Files (x86)\VistA\Imaging\VIXInstaller for future reference or troubleshooting.) This starts the installation process.

Figure 56: Begin the VIX Install



26. During the final install, a PowerShell script utility pops up (Figure 57, Figure 58, and Figure 59) to perform additional install tasks and closes when complete.

    NOTE: The PowerShell pop-up performs various configuration and certificate tasks and executes patch specific post-scripts.

    NOTE: If the MUSE service is not enabled, the PowerShell pop-up may display a red error message in the MUSE check section. See Appendix A: Enable MUSE Functionality.

Figure 57: PowerShell Pop-up Script Top Portion

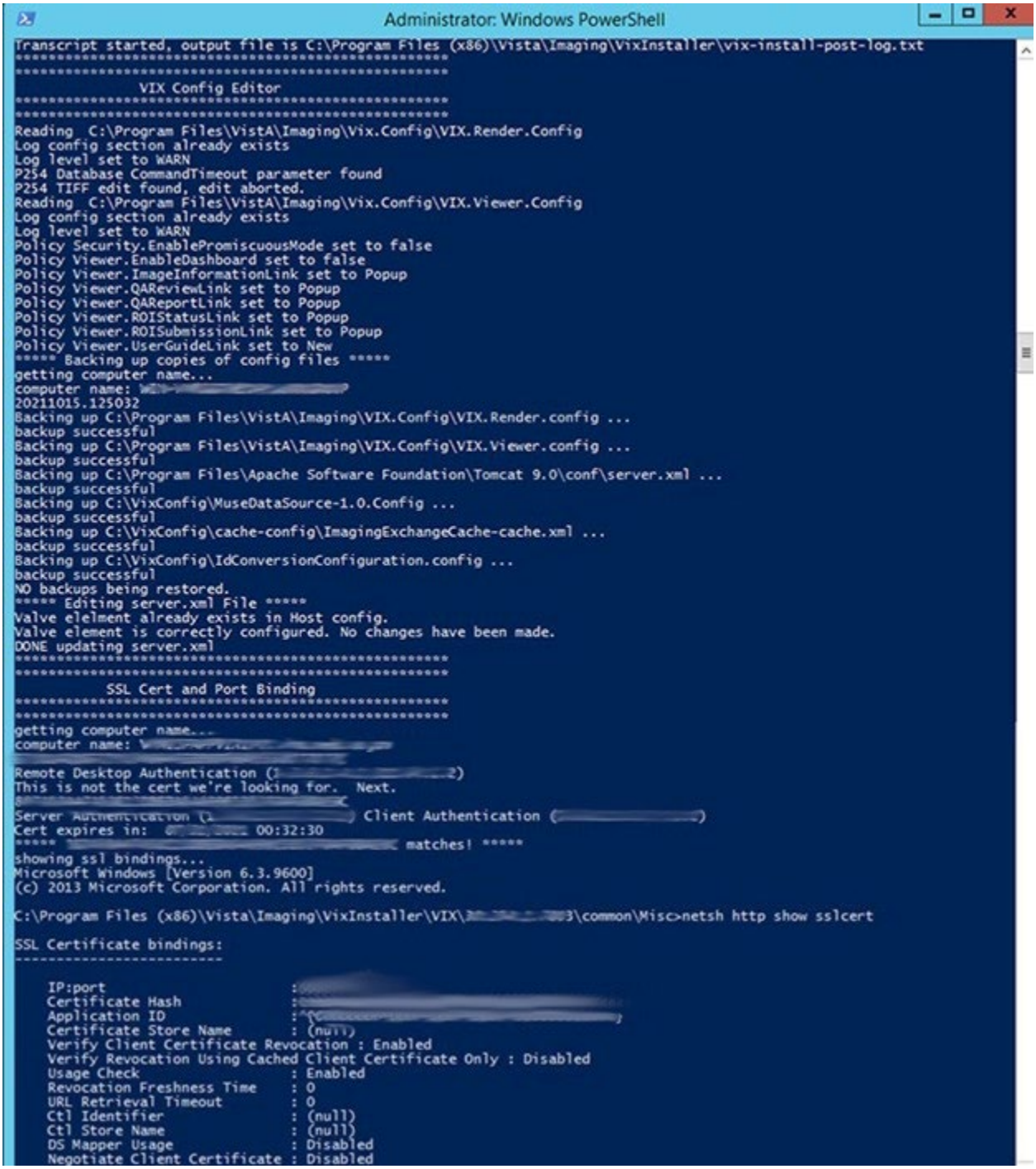


Figure 58: PowerShell Pop-up Script Middle Portion

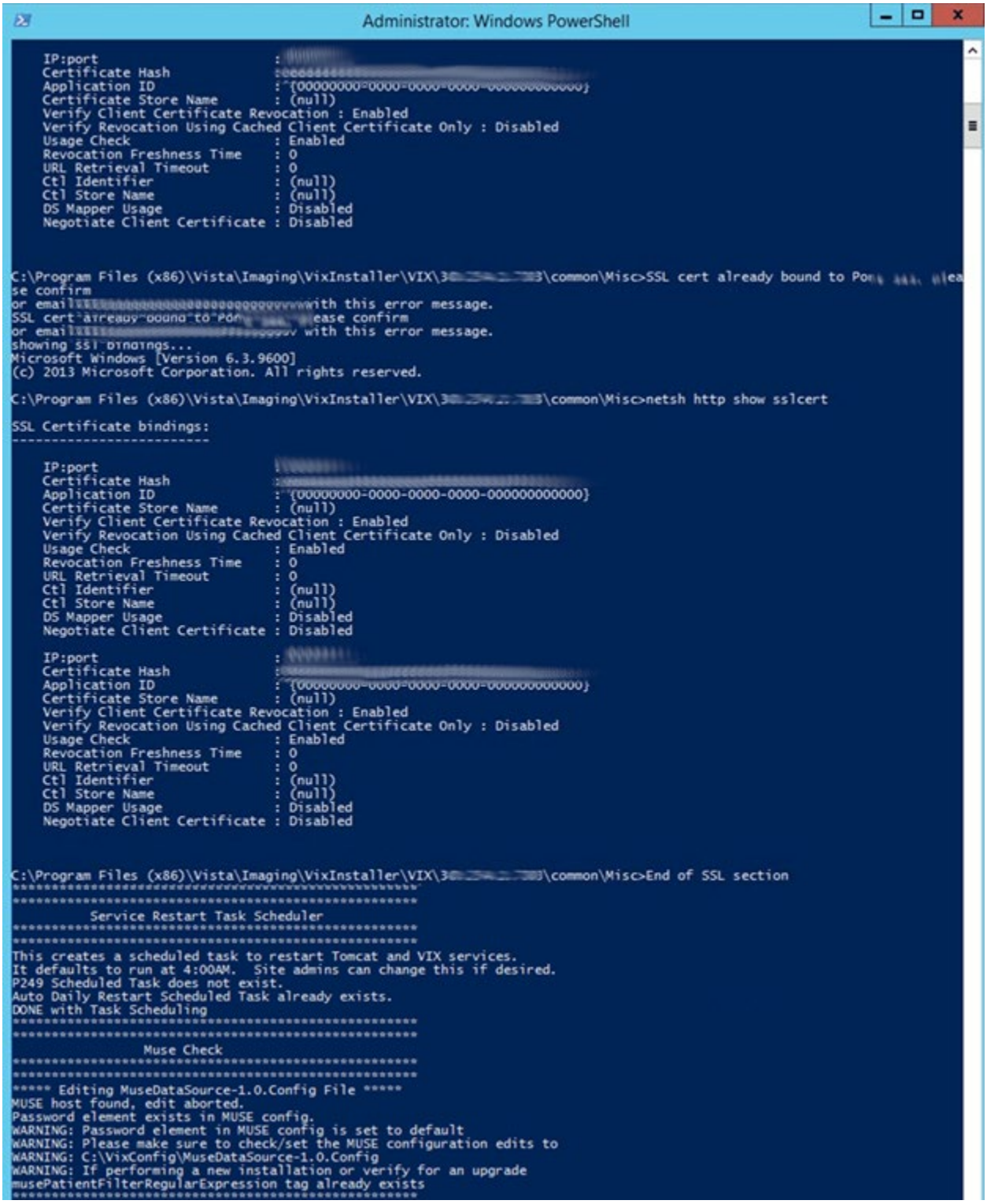
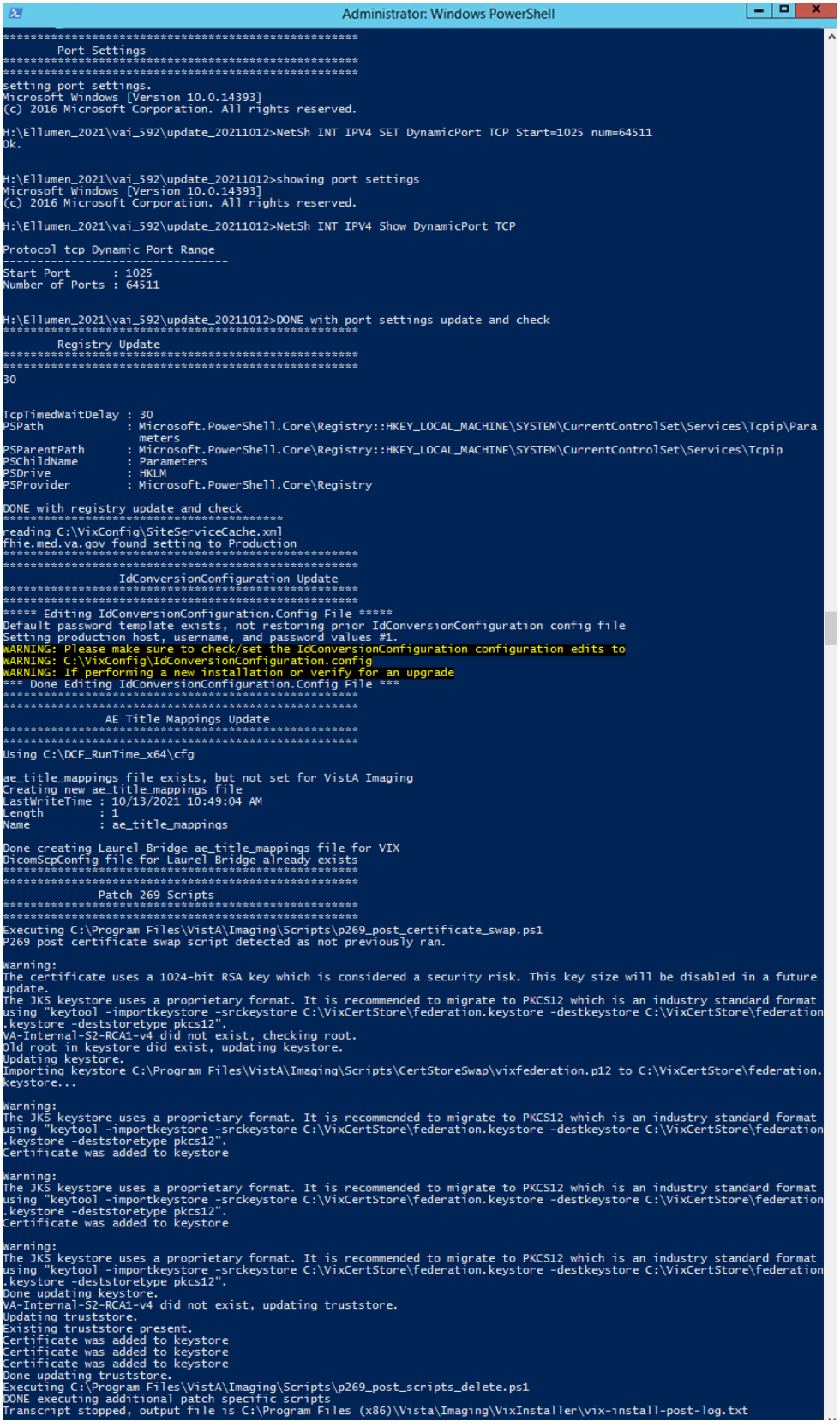
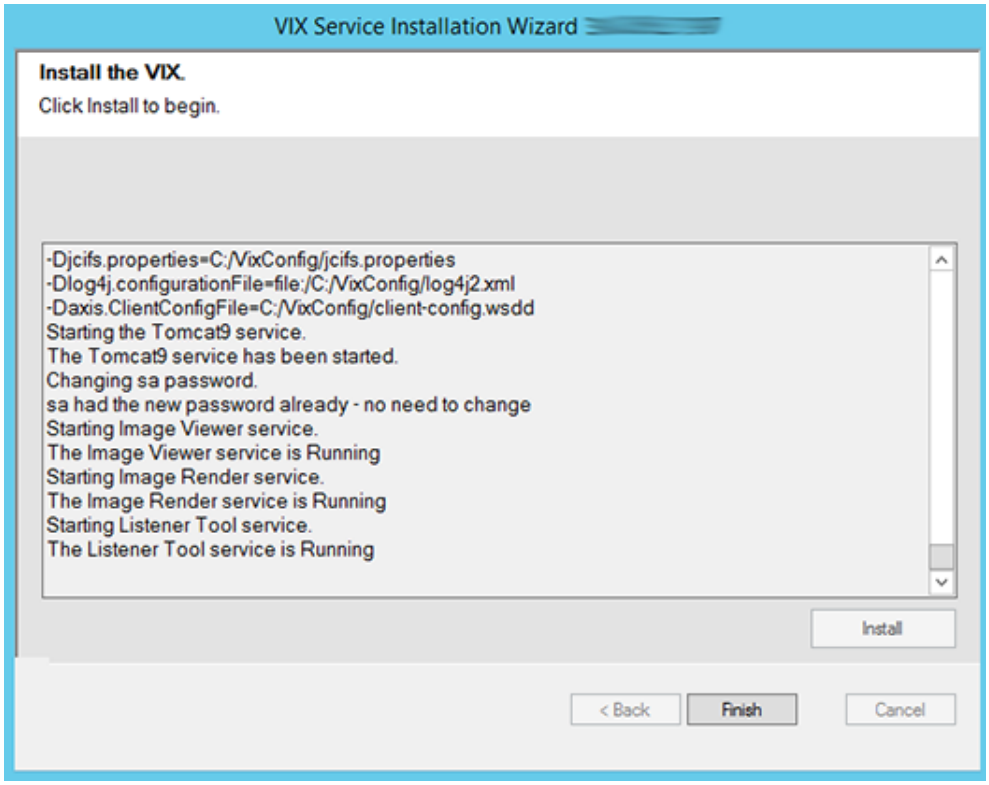


Figure 59: PowerShell Pop-up Script Bottom Portion



27. When the installation completes, the VIX automatically starts the Tomcat, Viewer/Render, and Listener Tool services. Click **Finish** to exit the wizard (Figure 60). The VIX Service Installation Wizard closes.

Figure 60: VIX Installation Complete



28. Continue to *Post-Installation for New VIX Installations and Updating Existing VIX Installations.*

4. Post-Installation for New VIX Installations and Updating Existing VIX Installations

4.1. Post-Installation Configuration

New with MAG*3.0*269: Perform the following post-installation steps to allow for login to the new VIX Tools page described in the *Verifying Access to the VIX Tools and VIX Transaction Log* section.

1. Open Windows Explorer and navigate to the **C:\Program Files\Vista\Imaging\VIX.Config** folder. Run Notepad, Notepad++, or WordPad as an administrator and open the **VIX.Viewer.Config** file.
2. Add the following line as shown in Figure 61 inside the opening and closing Policies tags (if it does not already exist)

   ```
   <add name="Dashboard.RequireAdministrator" value="false" />
   ```

   Save the VIX.Viewer.Config file after updating.

   NOTE: If a policy for "Dashboard.RequireAdministrator" already exists, ensure the value is set to "false".

Figure 61: VIX.Viewer.Config File Policies

3. Execute the restart script (Restart_VIX_Services.ps1) to restart the Apache Tomcat service, VIX Viewer and VIX Render services, and Listener Tool, see *Appendix C: Restart Script*.

4.2. MUSE Configuration

Please refer to *Appendix A: Enable MUSE Functionality* to configure the MUSE (if not previously configured).

4.3. McAfee Exclusions

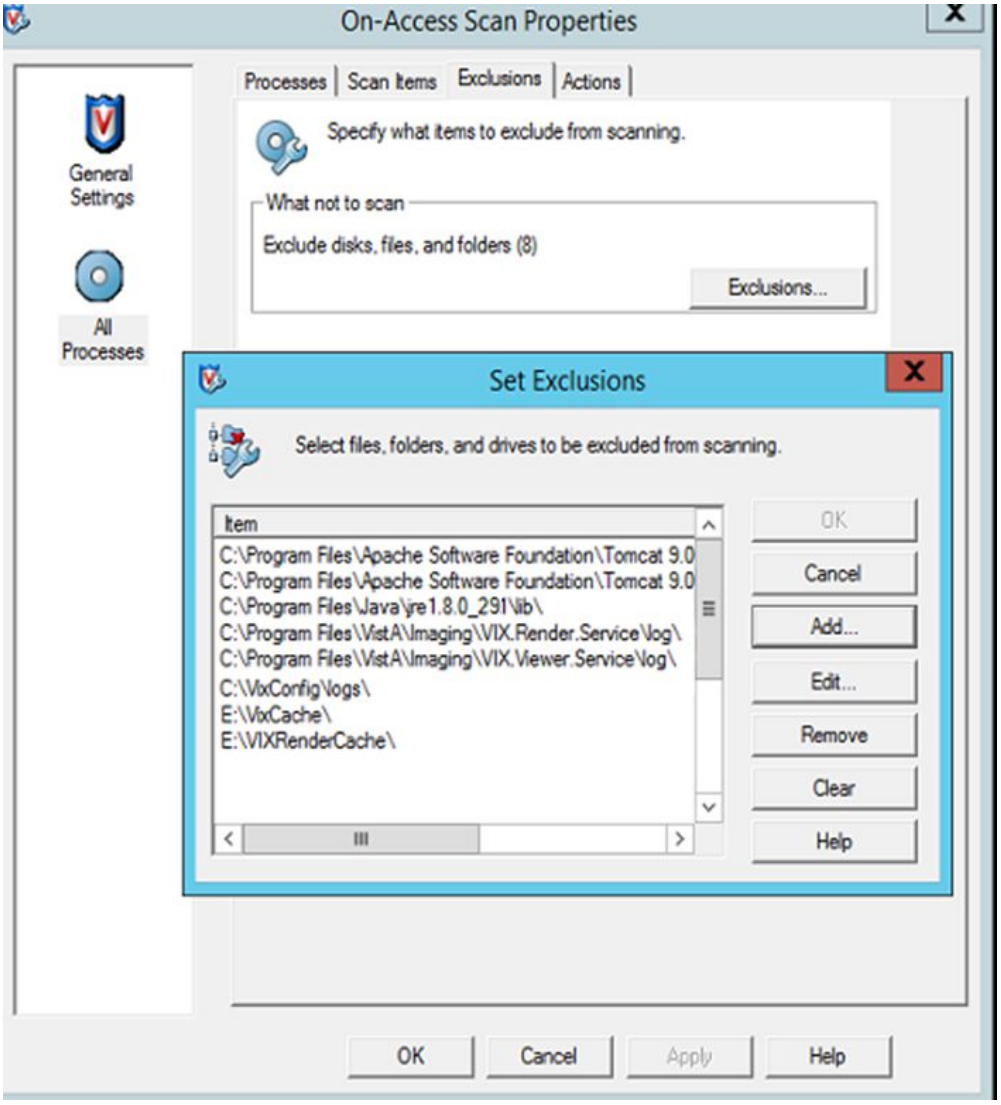
Exclude the following directories using McAfee On-Access Scan Properties (Figure 62). Make sure "Also exclude subfolders" is checked, so subfolders are excluded as well:

- C:\Program Files\Java**jre1.8.0_291\lib**

NOTE: Excluding the above Java subfolder is necessary with **MAG*3.0*269.**

- C:\Program Files\Apache Software Foundation**Tomcat 9.0\lib**
- C:\Program Files\Apache Software Foundation**Tomcat 9.0\logs**
- C:\Program Files\VistA\Imaging\VIX.Render.Service\log
- C:\Program Files\VistA\Imaging\VIX.Viewer.Service\log
- C:\VixConfig\logs
- <cache drive>:\VixCache
- <cache drive>:\VIXRenderCache

Figure 62: Set Exclusions Dialog



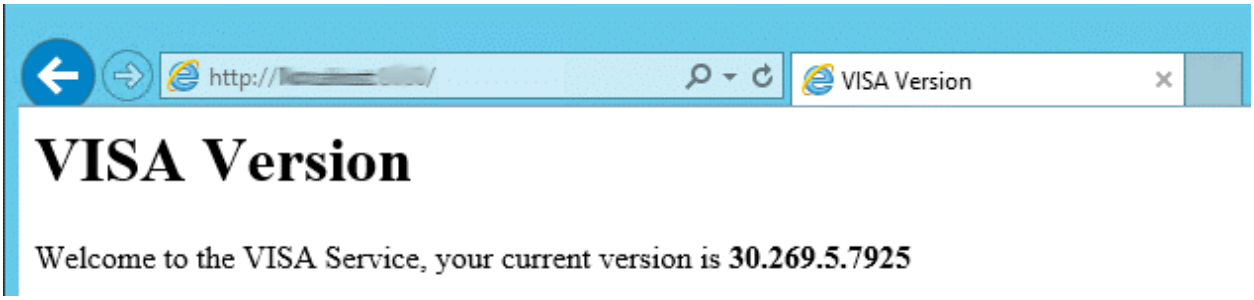
Click **OK** in the Set Exclusions window. Then click **OK** in the McAfee On-Access Scan Properties window.

4.4. Verifying Installation/Upgrade is Complete

Verify that your installation is complete by obtaining the current version (Figure 63). Follow these steps:

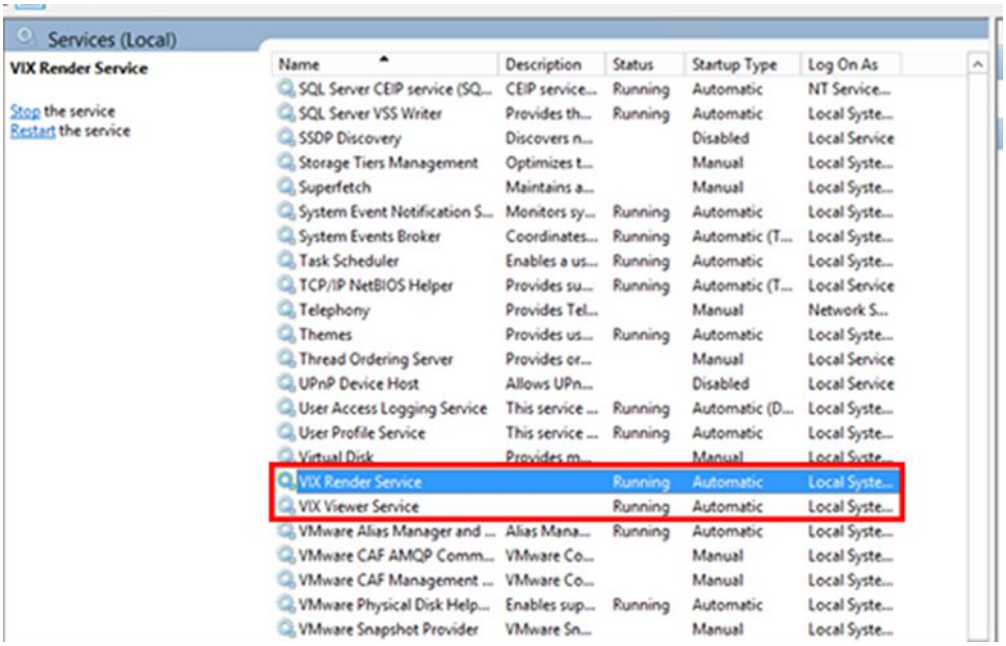
1. Go to the VIX homepage: **http://*FQDN of VIX server*:REDACTED/**
2. The current version is listed in the format XX.XXX.X.X. The first two digits represent Version 3.0 of the VistA Imaging system. The next three digits are the number of the latest patch that has affected the VIX. This patch number should match the number of the VIX component you have most recently installed.

Figure 63: VISA Version Verification



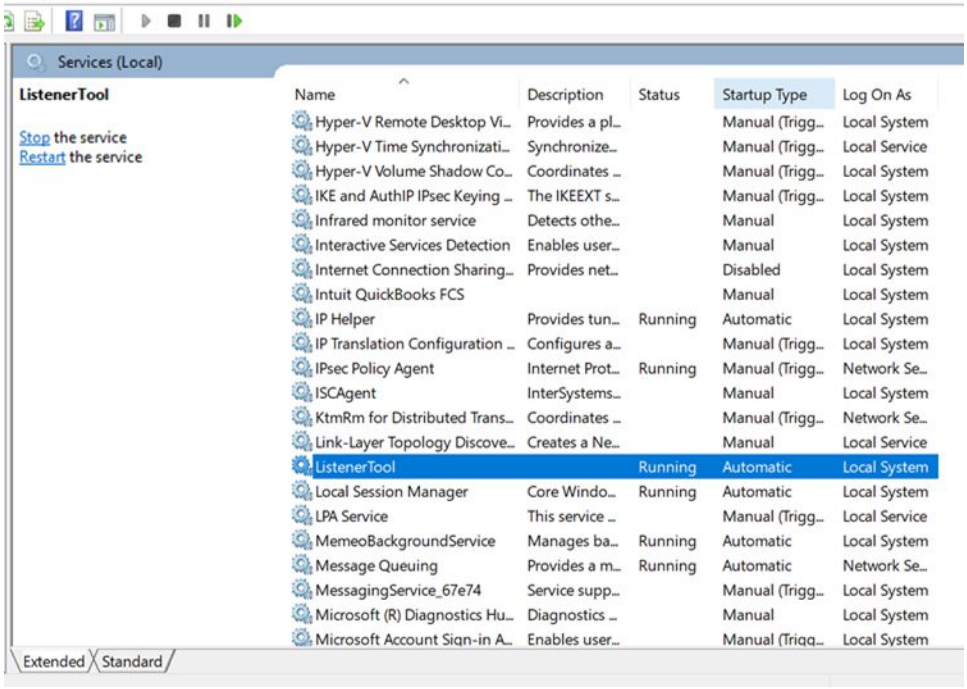
3. Verify VIX Viewer and VIX Render services are running (Figure 64).

Figure 64: VIX Viewer and Render Services Running



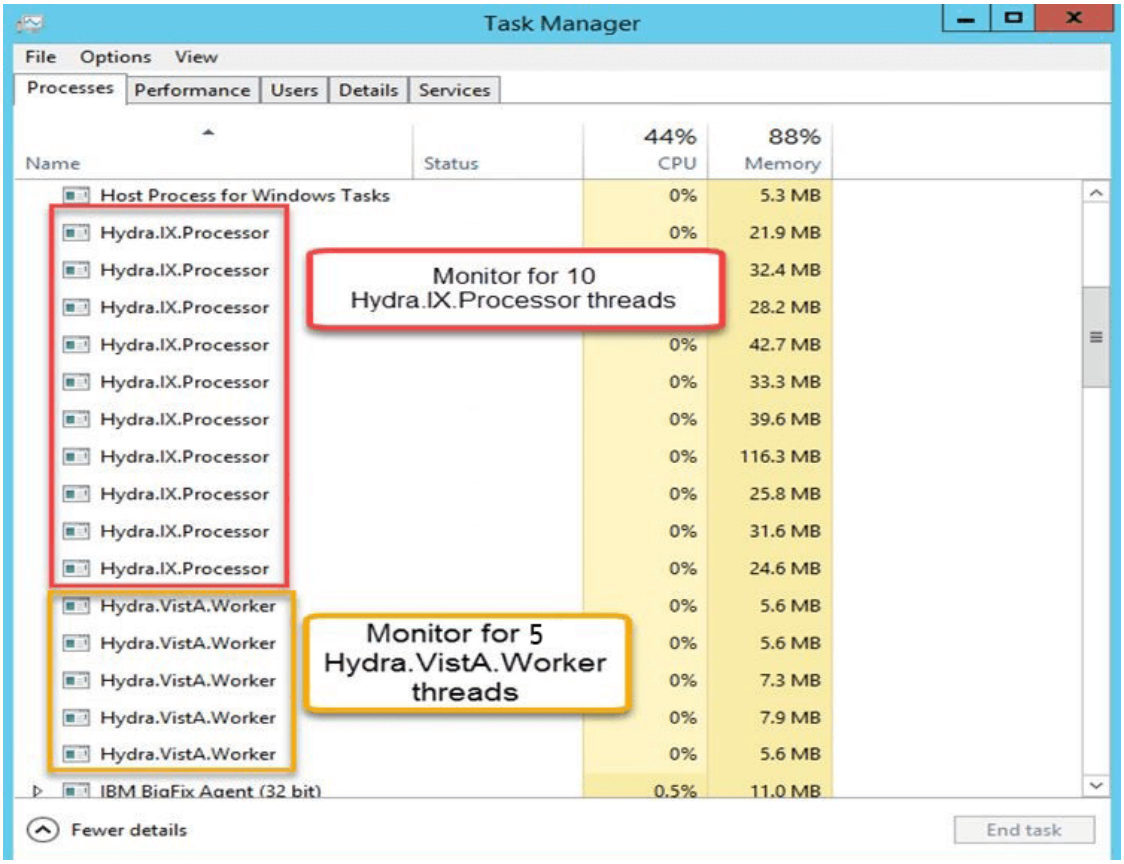
4. Verify the ListenerTool is running (Figure 65).

Figure 65: Listener Running



5. Verify that you have 10 Hydra IX Processor and 5 Hydra VistA Worker processes running (Figure 66):

Figure 66: 10 Hydra IX Processor and 5 Hydra VistA Worker Processes Running



4.5. Verifying VIX Operations

After a VIX is installed and is registered with the Image Exchange Service (not needed if VIX is only being updated), Clinical Display (MAG*3.0*258 or later) and VistARad (MAG*3.0*199 or later) workstations automatically start using the VIX.

- Clinical Display begins sending requests for remote data to the VIX immediately. No configuration changes are required for Clinical Display to start using the VIX.
- VistARad needs some local configuration changes to enable some of its VIX-supported capabilities; refer to the VistARad documentation for details.
- Joint Legacy Viewer (JLV) Image Viewing does not require any additional configuration changes. The Image Viewer should launch without issue and be able to display MUSE images.

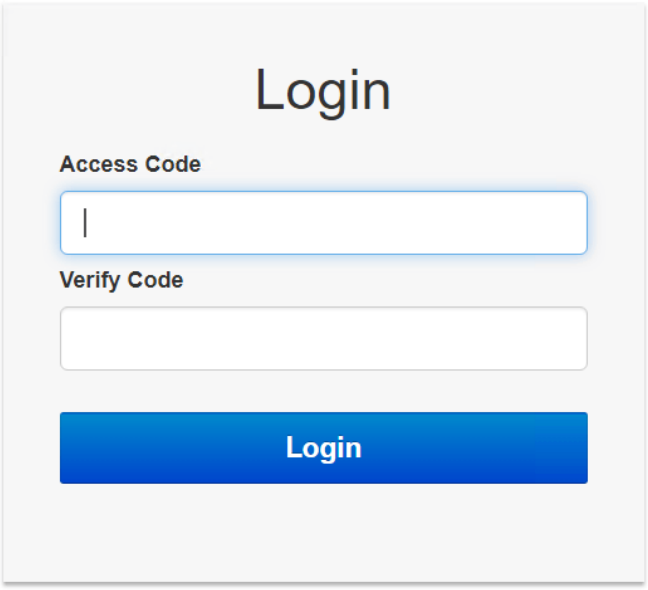
New with MAG*3.0*269: The VA and Microsoft no longer support Internet Explorer (IE) as of June 15, 2022. MAG*3.0*269 officially deprecates support for IE. Please use either Google Chrome or Microsoft Edge on your Government Furnished Equipment (GFE) or VIX server to verify and perform VIX Operations. If necessary and able install Chrome or Edge if not already present.

4.5.1. Verifying Access to the VIX Tools and VIX Transaction Log

VIX administrators can use the VIX Tools as described in the *VIX Administrator's Guide* with a listing of available tools in Appendix B: VIX Tools of the VIX Administrator's Guide.

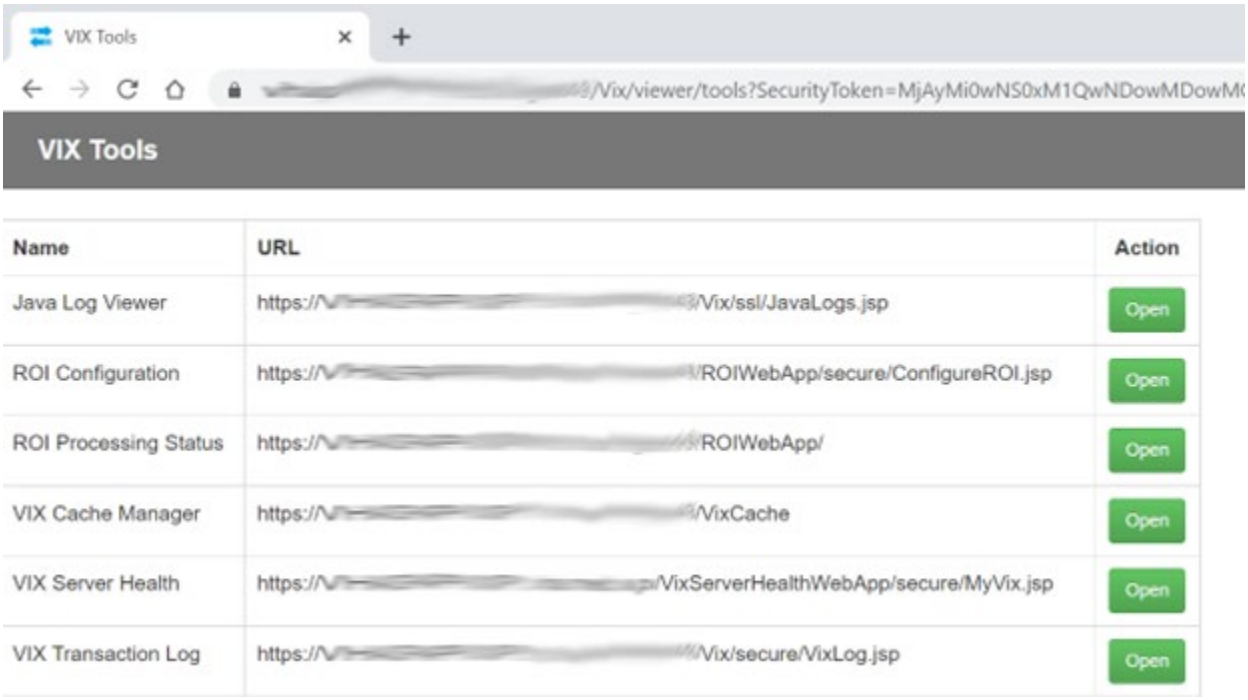
New with MAG*3.0*269: To access the VIX Tools, navigate to REDACTED/vix/viewer/tools to be prompted to login (Figure 67). Use a VistA account with the MAG VIX ADMIN security key and INITIAL to log in.

Figure 67: Login Page



The VIX transaction log can be used to monitor VIX activities. Once logged in to the VIX Tools page, access to the transaction log at **http://*FQDN*:REDACTED/Vix/secure/VixLog.jsp** is available
(where *FQDN* is the fully qualified domain name of the VIX server) (Figure 68).

Figure 68: VIX Tools Page



If you cannot access the transaction log, verify that the VIX service is running.

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

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

4.5.2. Spot-Checking VIX Image Delivery

This section shows different ways you can spot-check displaying remote images.

1. Using JLV:
    a. Select an image with a camera icon, and launch the Image Viewer to display the selected image.
    b. Select the "Cardiology Studies VA MUSE Only" widget, and view a MUSE EKG image by selecting the camera icon. This launches the Image Viewer to display the selected MUSE EKG image.
    c. Turn on the Display DOD Image User Preference in JLV. View a DoD image by selecting the camera icon. This launches the Image Viewer to display the selected DoD image.
2. On the Clinical Display workstation:
    a. Select a patient with remote images.
    b. If it is not visible already, display the Abstracts area to display an abstract for one of the remote images.

c. Right-click the abstract for the remote image, and open the Image Information window.
d. In the Image Information window, check the IEN (Internal Entry Number) value or Image Number. If the value starts with "urn", the remote image was retrieved by the VIX.

4.6. DICOM SCP Configuration

Please refer to *Appendix B: DICOM SCP Configuration* to configure the DICOM Service Class Provider (SCP).

4.7. Using the VIX Service Installation Wizard to Reconfigure the VIX

You must re-execute the VIX Service 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 hostname or port number.

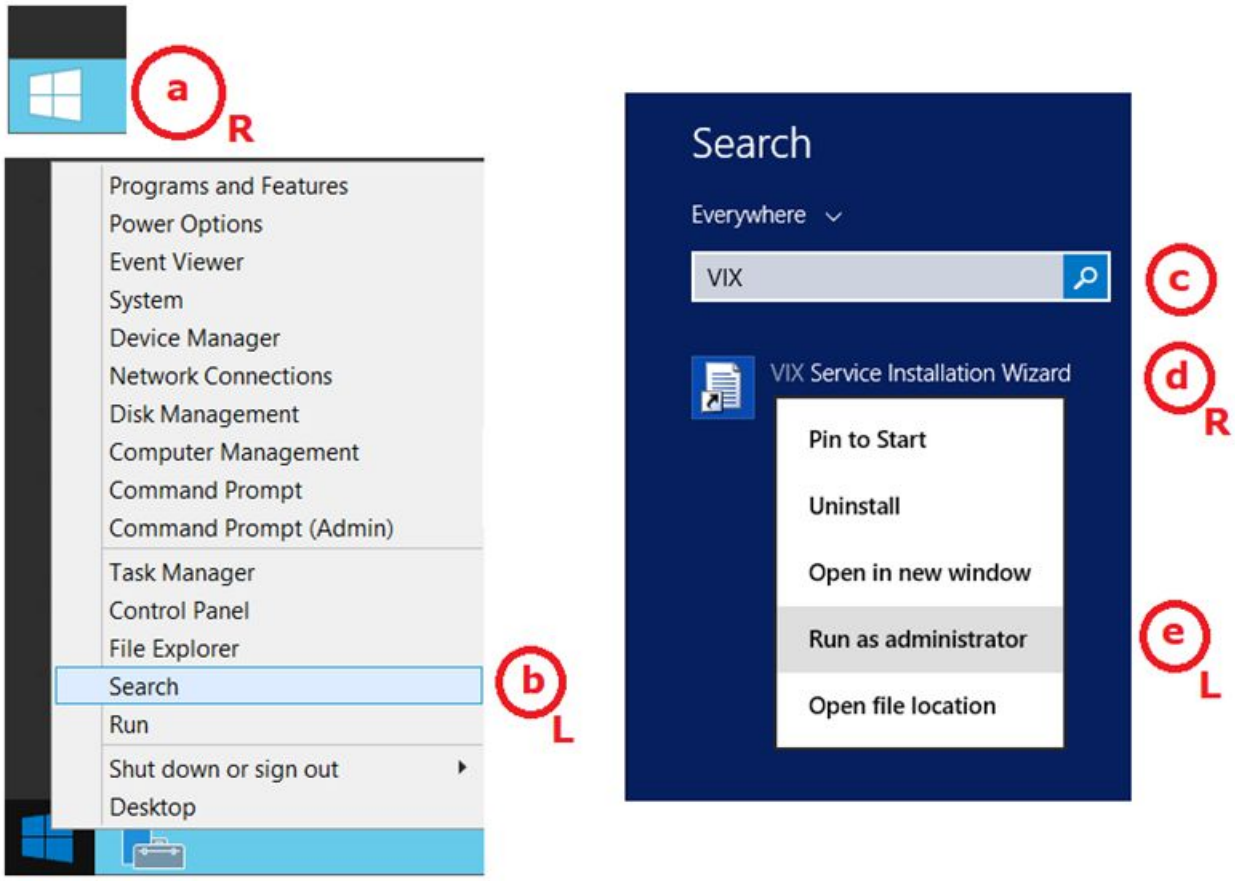
Using the VIX Service Installation Wizard to reconfigure VIX is like the steps for updating a VIX, except the process is much faster since no actual software is being installed.

TIP: Changing a VIX cache location or local connection information should take about 5 minutes.

4.7.1. Reconfiguring a VIX Server

1. Review the information in the *Scheduling Downtown and Impact of a VIX Update* section, and schedule downtime and notify appropriate groups of the downtime.
2. Run the VIX Service Installation Wizard as an administrator (Figure 69).
   a. **R**ight-click **Start**.
   b. **L**eft-click **Search**.
   c. Type **VIX**.
   d. **R**ight-click VIX Service Installation Wizard.
   e. **L**eft-click Run as administrator.

Figure 69: Run the VIX Service Installation Wizard



3. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes**.
4. Click **Next** until the Specify the VA Site... page displays.
5. On this page, verify that the **Site Number** box shows your STATION NUMBER (field (#99) in the INSTITUTION file (#4) of your site, the information is in FileMan in VistA). Then, click the **Lookup Server Address**.
6. Verify the correct hostname and port number for the local VistA system displays. Then, click **Next**.
    a. When the Install the VIX Prerequisites page displays, click **Next**. (All prerequisites are installed already.)
7. When the Install the VIX Prerequisites page displays, click **Next**. (All prerequisites are installed already.)
8. On the "Specify the VA Site the VIX will service" page, do one of the following:
    a. If you are changing the location of the VIX cache and configuration files, select the new drive for each. Click **Create**. Then, click **Next**.
    b. If you are NOT changing the location of the VIX cache and configuration files, click **Next**.
9. In the Specify the VistA and email Configuration, do the following:

a. Enter the access and verify codes. If you are changing the email address or addresses enter them. Click **Validate**.
b. Click **Next**.

10. In the Configure local DoD connection page, click **Next**.
11. In the Install the VIX page, click **Install**.
12. Wait until the installation is complete and click **Finish**. The VIX restarts automatically.

5. Troubleshooting

5.1. Resuming an Interrupted VIX Installation

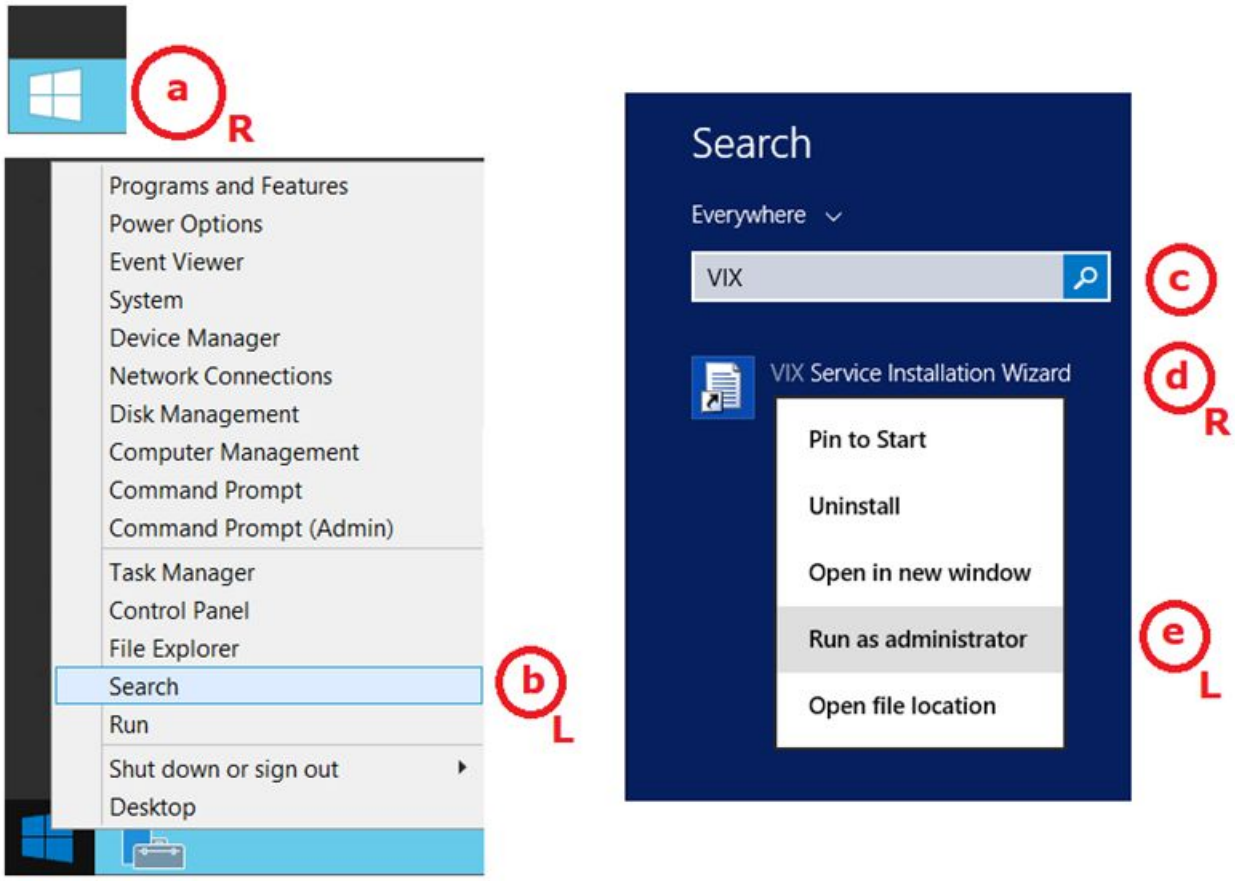
If you have had to interrupt or cancel an in-progress VIX installation, you can resume the installation.

NOTE: If you re-run MAG3_0P<number>_VIX_SETUP.msi, you are repeating the installation of the VIX Service 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 following the steps below.

5.1.1. Resuming Installation (single server VIX)

1. Log onto the VIX server as an administrator.
2. Run the VIX Service Installation Wizard as an administrator (Figure 70).
   a. **R**ight-click **Start**.
   b. **L**eft-click **Search**.
   c. Type **VIX**.
   d. **R**ight-click VIX Service Installation Wizard.
   e. **L**eft-click Run as administrator.

Figure 70: Run the VIX Service Installation Wizard



3. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes.**
4. Follow the steps for a first-time VIX installation or for updating a VIX.

5.2. Tomcat Permissions

Please refer to *Appendix D: Tomcat Permissions* if encountering file system access errors, i.e.: ...error denying access to apachetomcat account, after VIX Installation.

5.3. VIX Support

If you encounter problems installing the VIX, please call the Enterprise Service Desk at REDACTED.

6. Back Out/Uninstall

6.1. Stopping the VIX Services

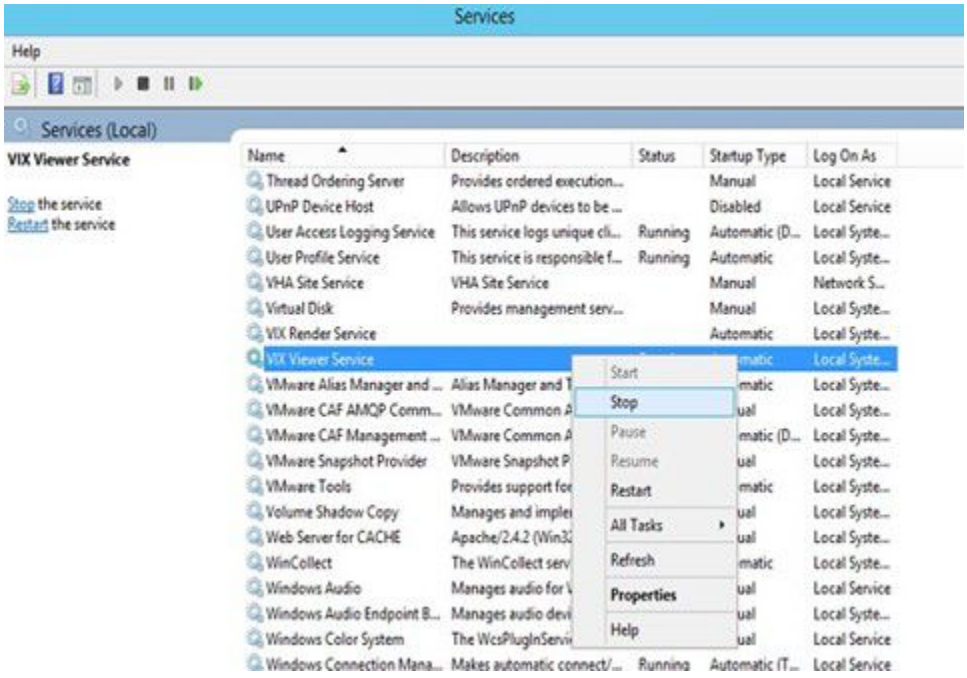
To minimize downtime and speed up the MAG*3.0*269 VIX back out/uninstall, stop the following services first:

For Server 2012 R2 or 2016 (Server Manager | Tools | Component Services | Services (Local), or Task Manager | Services | Open Services), sort the Name column, and stop each VIX service shown below by selecting **Stop** (Figure 71).

- ListenerTool
- Tomcat9
- VIX Render Service
- VIX Viewer Service

Always use the Window 'Task Manager' to monitor the processing tasks as needed.

Figure 71: Stopping VIX Viewer Service



6.2. 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.

6.2.1. 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 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 REDACTED when the VIX was set up.

   NOTE: You need to re-enter this serial number as a part of the VIX installation process.
2. Run the VIX Service Installation Wizard as an administrator.
   a. **R**ight-click **Start**.
   b. **L**eft-click **Search**.
   c. Type **VIX**.
   d. **R**ight-click VIX Service Installation Wizard.
   e. **L**eft-click Run as administrator.
3. When the Welcome page displays, verify that the screen displays "This wizard will guide you through the installation of the Vista Imaging Patch MAG*3.0*269 VIX" and click **Next**.
4. Then, when prompted to do so, click **Uninstall version 30.269.xxx**. (The wizard gracefully stops the VIX service before performing the uninstall.)
5. When the Uninstall completes, "Press Next to continue" displays in the VIX Service Installation Wizard, click **Cancel**. Click **Yes** in the dialog box that displays "Do you really want to quit the VIX Service Installation Wizard?"
6. Go to the Control Panel, choose **Add/Remove Programs**, and remove the MAG*3.0*269 VIX Service Installation Wizard.
7. Re-execute the VIX installation as if for a new VIX, see *New VIX Server Installation* section.
8. Re-execute the Post-Installation instructions, see *Post-Installation for New VIX Installations and Updating Existing VIX Installations* section.

6.2.2. 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 need to do the following:

1. Contact the REDACTED mail group and arrange to have the existing Laurel Bridge DCF toolkit licenses transferred to a new server.
2. Validate the new VIX server 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, see *New VIX Server Installation* section.

6.2.3. Decommissioning a VIX

If you need to completely decommission a VIX and not replace it by another VIX, do the following:

1. Notify the REDACTED mail group that the Laurel Bridge license seats used by your site are no longer being used.
2. Contact REDACTED 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.

6.3. 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 remove the VIX and permanently delete the VIX cache.

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

1. Stop the VIX service. See Section 6.1.
2. Remove VIX-related applications, accounts, directories, and variables.

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

6.3.1. Remove VIX related applications, accounts, directories, and variables

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

These steps presume you are already logged in as an administrator on the 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 VIXCache is located, and delete the following folders:

   <shared drive letter>:\VixCache
2. Delete the VixRenderCache folder, which is usually on that same drive.
3. Use Windows Explorer to delete the following directories:

   C:\DCF_RunTime
   C:\Program Files\Java\jre1.8.0_291
4. 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 need to recreate the VIX configuration and request new VIX security certificates.

C:\VixBackup

C:\VixConfig
C:\VixCertStore

5. Open the window used to remove programs.
   a. On Windows, click **Start | Control Panel**. Under the Programs item, click Uninstall a program.
   b. Remove these four programs (no reboot required):
      - Apache Tomcat 9.0.40
      - Java (TM) 1.8.0. Update 291
      - LibreOffice 7.0.6
      - VIX Service Installation Wizard
6. In Windows Explorer, navigate to C:\Program Files and delete the LibreOffice folder (C:\Program Files\LibreOffice).
7. In Windows Explorer, right-click the Local Disk (C:) folder, select Properties. Then, select the **Security** tab.
8. Select the apachetomcat user and click **Remove**.
9. Click **OK** to close the Properties dialog box and click **Yes** when asked if you want to continue.

   NOTE: If one or more "Error applying security" messages display, click Continue until they are all closed.
10. Open the Computer Management/Server Manager window.
    a. On Windows, right-click **Computer** on the desktop. Then, click **Manage**.
11. In the tree on the left side of the window, navigate to Users.
    a. On Windows, go to Server Manager/Configuration/ Local Users and Groups/Users.
12. On the right side of the window, right-click the apachetomcat user, click **Delete**, and click **Yes** when you are asked for confirmation.
13. Open the System Properties dialog box.
    a. On Windows, *right-click* **Computer** on the desktop. Then, click **Properties**. Then on the left side of the System window, click **Advanced system setting.**
14. In the Advanced tab, click **Environment Variables**.
15. 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
DCF_ROOT
DCF_TMP
DCF_USER_BIN
OMNI_ROOT
vixcache
vixconfig

16. In the System variables list, select the Path system variable. Then, click **Edit**.
    a. In the Variable value box, delete the following substrings:
    b. C:\DCF (if present)
       C:\DCF_Runtime\bin
       C:\DCF_Runtime\lib
       C:\Program Files\Java\jre1.8.0_291\bin
    c. NOTE: It is recommended that after deleting each substring you delete any extra semicolon characters.
    d. After removing the substrings, click **OK**. Then click **OK** twice more to close the Environment Variables and System Properties dialog boxes.
17. VIX removal is complete.

6.4. Rollback and Back Out of MAG*3.0*269

If it is necessary to uninstall the MAG*3.0*269 VIX and back out the VIX to a prior version perform the following steps:

1. Run the MAG*3.0*269 VIX Service Installation Wizard as an administrator.
    a. **R**ight-click **Start**.
    b. **L**eft-click **Search**.
    c. Type **VIX**.
    d. **R**ight-click VIX Service Installation Wizard.
    e. **L**eft-click Run as administrator.

NOTE: If the VIX Service Installation Wizard does not appear in the Search bar, open Windows Explorer and navigate to the **C:\Program Files (x86)\Vista\Imaging\VixInstaller** folder, **r**ight-click **VixInstaller.exe** and **l**eft-click **Run as administrator**.

2. When the Welcome page displays, verify that the screen displays “This wizard will guide you through the installation of the Vista Imaging Patch MAG*3.0*269 VIX” and click **Next**.
3. Then, when prompted to do so, click **Uninstall version 30.269.xxx**. (The wizard gracefully stops the VIX service before performing the uninstall.)
4. When the Uninstall completes, "Press Next to continue" displays in the VIX Service Installation Wizard, click **Cancel**. Click **Yes** in the dialog box that displays "Do you really want to quit the VIX Service Installation Wizard?"
5. Go to the Control Panel, choose **Add/Remove Programs**, and remove the MAG*3.0*269 VIX Service Installation Wizard.
6. Verify backup copies of critical configuration file folders exist within C:\VIXBackup\P284\YYYYMMDDHHMMSS. Where YYYYMMDDHHMMSS is the latest version of the folder that contains the backups (most current date).

   NOTE: Backups exist of the following:

- C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf
- C:\VixConfig
- C:\VixCertStore
- C:\Program Files\VistA\Imaging\VIX.Config

7. Stop each VIX service: ListenerTool, Tomcat9, VIX Render Service, and VIX Viewer Service by opening Windows Services and then selecting **Stop** for each service (Figure 71) as described in Section 6.1.
8. Copy the file ROIPeriodicCommandConfiguration.config in C:\VIXBackup\P284\YYYYMMDDHHMMSS\VixConfig to C:\VixConfig and replace over the existing ROIPeriodicCommandConfiguration.config file. Where YYYYMMDDHHMMSS is the latest version of the folder that contains the backups (most current date).
9. Install the previous version of VIX, which was included in MAG*3.0*284 (find it on the VA SFTP site or from a local backup folder). Do the following to prepare the VIX Service Installation Wizard:
   a. Right-click the MAG3_0P284_VIX_SETUP.msi file and click on Install.
   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**.
10. Run the MAG*3.0*284 VIX Service Installation Wizard as an administrator.
    a. **R**ight-click **Start**.
    b. **L**eft-click **Search**.
    c. Type **VIX**.
    d. **R**ight-click **VIX Service Installation Wizard**.
    e. **L**eft-click **Run as administrator**.

NOTE: If the VIX Service Installation Wizard does not appear in the Search bar, open Windows Explorer and navigate to the **C:\Program Files (x86)\Vista\Imaging\VixInstaller** folder, **r**ight-click **VixInstaller.exe** and **l**eft-click **Run as administrator**.

11. Once the MAG*3.0*284 VIX Service Installation Wizard is running, click **Next** and continue with the installation steps described in detail in the *MAG*3.0*284 VIX Installation Guide* as if it is an upgrade MAG*3.0*284 install.
12. Upon completion of the installation, if necessary, configuration files in C:\VIXBackup\P284\YYYYMMDDHHMMSS\VixConfig can be copied to C:\VixConfig as needed (e.g. MuseDataSource-1.0.Config) to restore the prior version. Where YYYYMMDDHHMMSS is the latest version of the folder that contains the backups (most current date). If configuration files are to be restored, first stop each VIX service: ListenerTool, Tomcat9, VIX Render Service, and VIX Viewer Service by opening Windows Services and then selecting **Stop** for each service (Figure 71) as described in Section 6.1.
13. Uninstall Java 8.0.291 manually using the Control Panel (Figure 13).

14. Apply the McAfee Exclusions after MAG*3.0*284 install as discussed in the *MAG*3.0*284 VIX Installation Guide*.

NOTE: Make sure the subfolder C:\Program Files\Java**jre1.8.0_251\lib** is excluded.

15. Install MAG*3.0*326 to apply the log4j fixes.
16. Reboot your server.

6.4.1. Rollback Verification Procedure

1. Verify the version of Java after reinstalling MAG*3.0*284 by running Windows 'Programs and Feature', is Java 8.0.251
2. Verify the version of Tomcat after reinstalling MAG*3.0*284 by running Windows 'Programs and Features', is Tomcat 9.0.34
3. Verify the version of the VIX by going to the VIX homepage **http://*FQDN of VIX server*:REDACTED/** using a browser e.g.: Edge or Chrome.

7. Appendix A: Enable MUSE Functionality

NOTE: Perform this step as part of the *Post-Installation for New VIX Installations and Updating Existing VIX Installations.*

Enabling the MUSE functionality is only needed to be performed if this is a new installation, or in the case of an upgrade installation, it is determined it is not enabled by following *Has the MUSE functionality already been configured to be enabled?*

Has the MUSE functionality already been configured to be enabled?

- To determine if MUSE functionality is already configured to be enabled, open the MuseDataSource-1.0.Config file located in C:\VixConfig. Run Notepad, Notepad++, or WordPad as an administrator and then open the file.
    - **No, it is not enabled**. If the MuseDataSource-1.0.Config file located in C:\VixConfig is like the template displayed in Figure 72, continue with this Appendix to perform the steps to enable MUSE functionality.
    - **Yes, it is enabled.** If the MuseDataSource-1.0.Config file located in C:\VixConfig is not like the template displayed in Figure 72 (i.e. a real MUSE site number, host, username, and password are present), the MUSE functionality is already enabled. There is no reason to perform the steps in this Appendix unless reconfiguring.

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

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

To enable the MUSE configuration, the site administrator is expected to know the `museSiteNumber`, `host`, `username`, and `password` and replace the default values with those for the site:

1. Set the entries for the MUSE config in the MuseDataSource-1.0.Config file.
2. Set the value for the MUSE site number of the MUSE server that contains EKGs for your facility.
   `<museSiteNumber>**MUSE SITE NUMBER HERE**</museSiteNumber>`
3. Insert the value of the host.
   `<host>**MUSE HOST HERE**</host>`
4. Insert the value of the MUSE username.
   `<username>**MUSE USER HERE**</username>`

5. **Insert the password obtained from existing site VistA Imaging documentation (if not available, please contact the local BioMed team or MUSE administrator for the password).**
   `<password>**MUSE PWD HERE**</password>`
6. Verify museDisabled is set to false.
   `<museDisabled>false</museDisabled>`

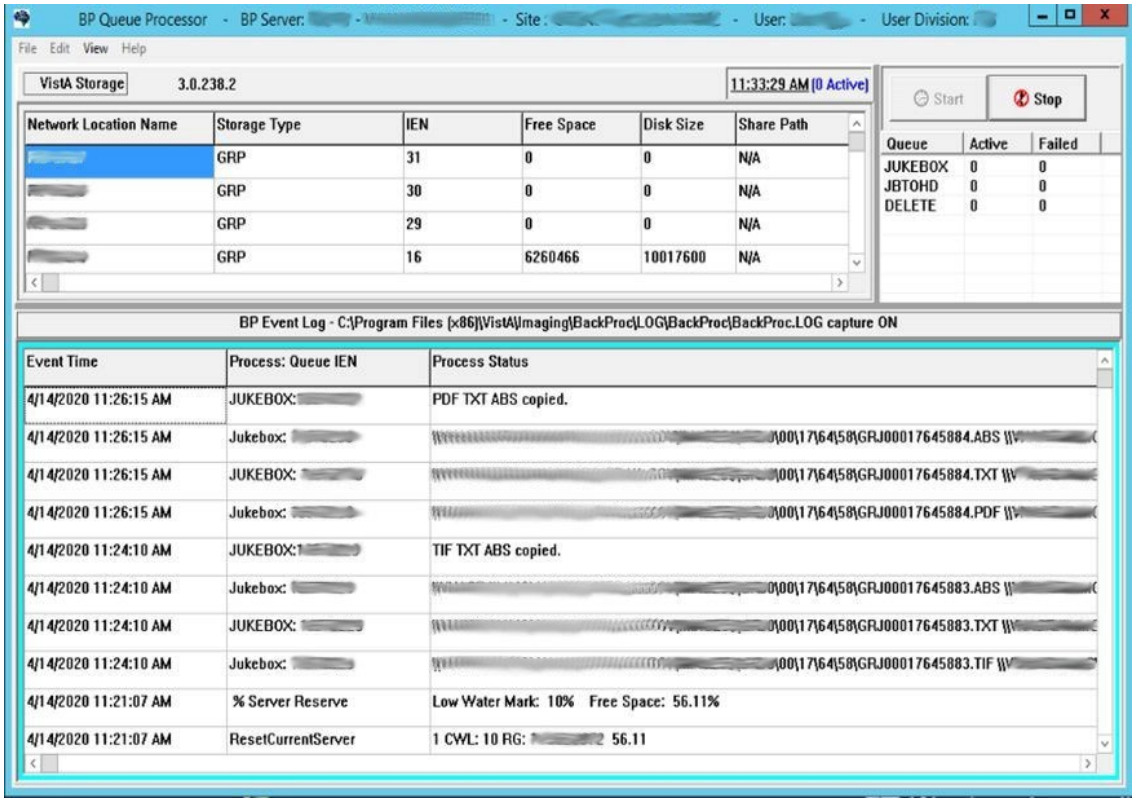
Save the MuseDataSource-1.0.Config file after updating the entries. After updating the MUSE config file, the MuseDataSource-1.0.Config looks like (Figure 72):

Figure 72: Sample MuseDataSource-1.0.Config File for One Server (MUSE ENABLED FOR JLV VIX Image Viewer)

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

1. From the Background Processor Queue Processor (Figure 73) menu bar, select **Edit** > **Network Location Manager** to open the Network Location Manager window.

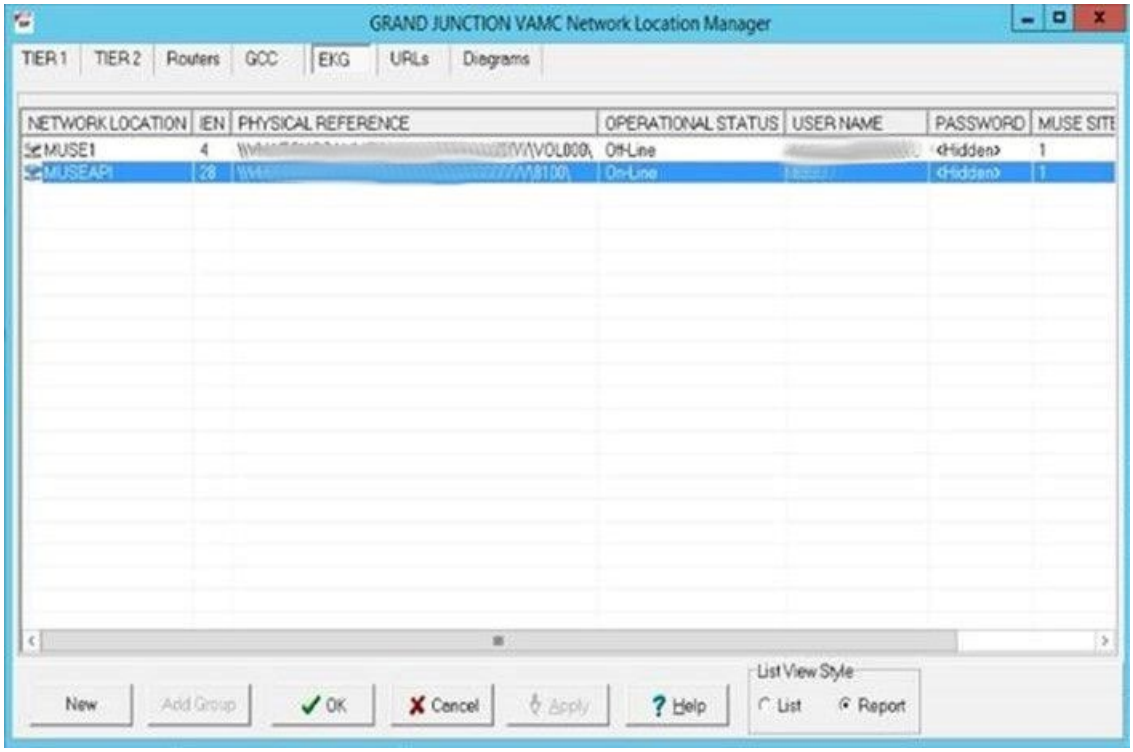
Figure 73: Background Processor Queue Processor



2. Click on the EKG tab in the Network Location Manager window. A listing of the network location of available MUSE servers appears (Figure 74).

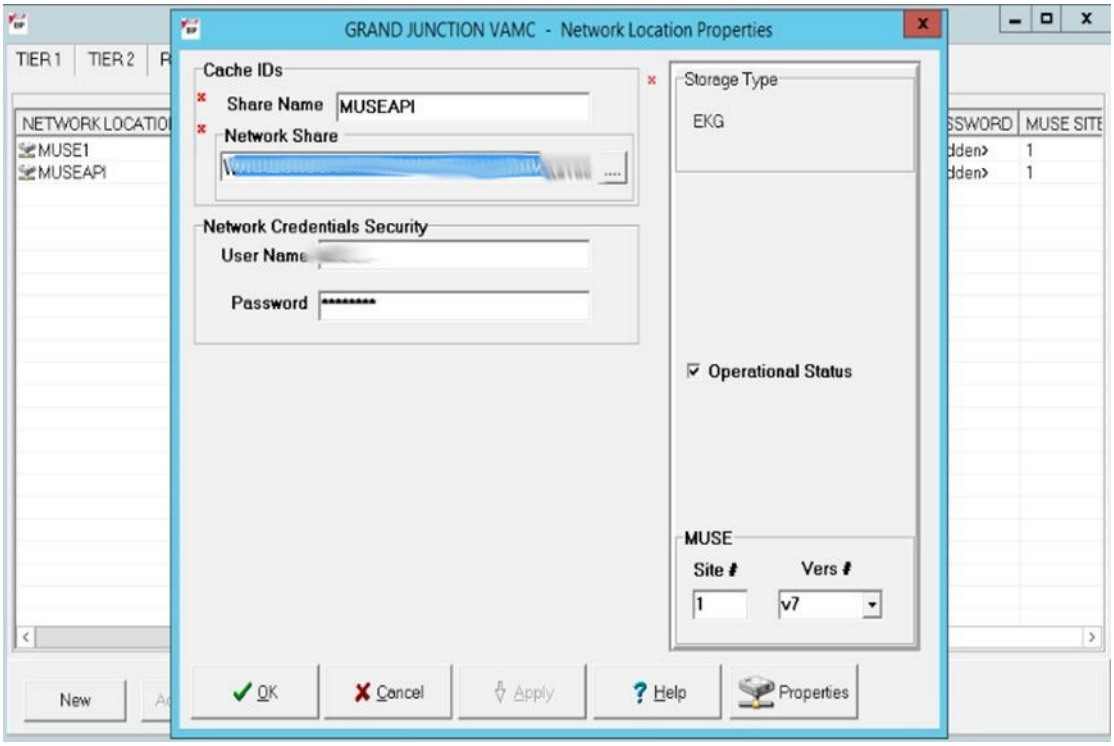
   NOTE: Pay attention to the Operational Status of available MUSE servers. Only add the MUSE server that is **On-Line and contains EKGs of the local site.**

Figure 74: EKG Tab in Network Location Manager in Background Processor Queue Processor



3. To obtain details for a MUSE server, right-click on the server and run **Properties** to launch Network Location Properties. The network share and username for that MUSE server displays (Figure 75).
4. Use the details from the Network Location Properties for the MUSE server that is On-Line to obtain the `<museSiteNumber>`, `<host>`, and `<username>` entries for the MuseDataSource-1.0.Config file. The MUSE Site Number for the `<museSiteNumber>` entry is listed under "Site Number" under "MUSE". The Fully Qualified Domain Name of the Server for the `<host>` entry is listed under "Network Share" between \\ and \ (Figure 75). The MUSE Site Username for the `<username>` entry displays under "User Name" under "Network Credentials Security"

Figure 75: Network Location Properties in Background Processor Queue Processor



Once inside the file, MuseDataSource-1.0.Config, find entries for the `<museSiteNumber>`, `<host>` and `<username>` and update them with the information for the MUSE server that is On-Line. This is obtained from the Network Location Manager Properties tab in the Background Processor Queue Processor. The parameter line for `<password>` with the MUSE site password must be manually added. This password can be obtained from the existing site VistA Imaging documentation (if not available, obtain your MUSE site password from the local BioMed team or MUSE administrator).

After updating the MUSE config file, MuseDataSource-1.0.Config, as described above, execute the restart script (Restart_VIX_Services.ps1) to restart the Apache Tomcat service, VIX Viewer and VIX Render services, and Listener Tool, see *Appendix C: Restart Script*.

Continue to the *McAfee Exclusions* step in the Post-Installation Instructions.

8. Appendix B: DICOM SCP Configuration

NOTE: Perform this step as part of the *Post-Installation for New VIX Installations and Updating Existing VIX Installations.*

The DICOM Service Class Provider (SCP) enables Commercial Picture Archive and Communication System (PACS) and various query retrieve devices at VA facilities to get remote VistA images through the use of DICOM C-FIND and C-MOVE.

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

You need to configure the DICOM SCP if this is a new installation, or in the case of an upgrade installation, you determine it is not yet configured by following *Has the DICOM SCP functionality already been configured?*

Has the DICOM SCP functionality already been configured?

- To determine if DICOM SCP functionality is already configured, open the ae_title_mappings file located in the folder cfg\dicom within the Laurel Bridge installation directory (C:\DCF_RunTime_x64\cfg\dicom by default). Run, Notepad, Notepad++ or WordPad as an administrator and then open the file.
    - **No, it is not configured**. If the ae_title_mappings file located in the folder cfg\dicom within the Laurel Bridge installation directory (C:\DCF_RunTime_x64\cfg\dicom by default) is like the template displayed in Figure 76, continue with this Appendix to perform the steps to configure DICOM SCP functionality.
    - **Yes, it is configured.** If the ae_title_mappings file located in in the folder cfg\dicom within the Laurel Bridge installation directory (C:\DCF_RunTime_x64\cfg\dicom by default) is not like the template displayed in Figure 76 (i.e. a real DICOM SCP host IP, port, and AE Title are present), the DICOM SCP functionality is already configured. There is no reason to perform the steps in this Appendix unless reconfiguring.

Additional details on the DICOM SCP Configuration are provided in the "*Configure DICOM SCP Functionality*" section in the *VIX Administrator's Guide*.

8.1. AE Titles Configuration

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

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

8.1.1. Laurel Bridge AE Titles Configuration on VIX/CVIX

This section describes how to configure the AE Titles configuration file ae_title_mappings located in the folders cfg\dicom within the Laurel Bridge installation directory

(C:\DCF_RunTime_x64\cfg\dicom by default). Open the ae_title_mappings file to perform edits. Run, Notepad, Notepad++, or WordPad as an administrator and then open the file.

For each DICOM SCP client, the AE Title name and its host/port attributes must be set. For each DICOM SCP client, update the following entries for the AE Titles configuration file (refer to Figure 76 for line numbers):

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

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

Figure 76: Sample AE Titles Configuration File

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

An example of the ae_title_mappings file updated for one DICOM SCP client is shown in Figure 77.

NOTE: The example in Figure 77 for configuration of one DICOM SCP client is not how an actual VIX site's ae_title_mappings file is to be configured. This example is for illustrative purposes only.

Figure 77: Example AE Titles Configuration File

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

For each additional DICOM SCP client, similarly add lines for the host, port, and ae_title with the correct values as new lines below the prior lines for the prior DICOM SCP client (Figure 78). Save the ae_title_mappings file after updating the entries.

Figure 78: Sample AE Titles configuration File with Multiple DICOM SCP Clients

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

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

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

```

After updating the ae_title_mappings file, as described above, execute the restart script (Restart_VIX_Services.ps1) to restart the Apache Tomcat service, VIX Viewer and VIX Render services, and Listener Tool, see *Appendix C: Restart Script*.

8.1.2. AE Titles Configuration on DICOM SCU

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

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

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

8.2. Tomcat/ Laurel Bridge DICOM SCP Configuration

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

Update the following entries for the DICOM SCP functionality (refer to Figure 79 for line numbers):

1. Set the DICOM SCU calling AE title, inside opening and closing aeTitle tags (inside <aeTitle> </aeTitle> - line 18 in Figure 79). Change the value from the default setting of ALL.
2. Set the DICOM SCU IP address inside the opening and closing callingAeIp tags (inside < callingAeIp> </callingAeIp> - line 19 in Figure 79). Change the value from the default setting of 0.0.0.0.

Figure 79: Sample DICOM SCP Configuration File

```
<gov.va.med.imaging.facade.configuration.ScpConfiguration>
  <dirty>false</dirty>
  <accessCode>[redacted]</accessCode>
  <verifyCode>[redacted]</verifyCode>
  <cachedir>C:\VixCache</cachedir>
  <studytype>radiology</studytype>
  <siteFetchTPoolMax>20</siteFetchTPoolMax>
  <siteFetchTimeLimit>45</siteFetchTimeLimit>
  <imageFetchTPoolMax>4</imageFetchTPoolMax>
  <imageFetchTimeLimit>600</imageFetchTimeLimit>
  <cacheLifespan>1</cacheLifespan>
  <fetchLocalVix>false</fetchLocalVix>
  <preFetchSeries>true</preFetchSeries>
  <preFetchImages>false</preFetchImages>
  <calledAETitle>ANY_0.0.0.0</calledAETitle>
  <callingAEConfigs>
    <gov.va.med.imaging.facade.configuration.ScpCallingAE>
      <aeTitle>ALL</aeTitle>
      <callingAeIp>0.0.0.0</callingAeIp>
      <buildImageSR>true</buildImageSR>
      <fetchVAOnly>false</fetchVAOnly>
      <modalityBlockList>
        <gov.va.med.imaging.facade.configuration.ScpModalityList>
          <dataSource>ALL</dataSource>
          <addImageLevelFilter>false</addImageLevelFilter>
          <modalities>
            <string>none</string>
          </modalities>
        </gov.va.med.imaging.facade.configuration.ScpModalityList>
      </modalityBlockList>
    </gov.va.med.imaging.facade.configuration.ScpCallingAE>
  </callingAEConfigs>
</gov.va.med.imaging.facade.configuration.ScpConfiguration>
```

An example of the ScpConfiguration.Config file updated for one DICOM SCP client is shown in Figure 80.

NOTE: The example in Figure 80 for configuration of the aeTitle and callingAeIp is not how an actual VIX site's ScpConfiguration.Config file is to be configured. This example is for illustrative purposes only.

Figure 80: Example ScpConfiguration Configuration File

```
1  <gov.va.med.imaging.facade.configuration.ScpConfiguration>
2    <dirty>false</dirty>
3    <accessCode>C[redacted]</accessCode>
4    <verifyCode>1[redacted]</verifyCode>
5    <cachedir>C:\VixCache</cachedir>
6    <studytype>radiology</studytype>
7    <siteFetchTPoolMax>20</siteFetchTPoolMax>
8    <siteFetchTimeLimit>45</siteFetchTimeLimit>
9    <imageFetchTPoolMax>100</imageFetchTPoolMax>
10   <imageFetchTimeLimit>600</imageFetchTimeLimit>
11   <cacheLifespan>1</cacheLifespan>
12   <fetchLocalVix>false</fetchLocalVix>
13   <preFetchSeries>true</preFetchSeries>
14   <preFetchImages>false</preFetchImages>
15   <calledAETitle>ANY_0.0.0.0</calledAETitle>
16   <callingAEConfigs>
17     <gov.va.med.imaging.facade.configuration.ScpCallingAE>
18       <aeTitle>AE_SCP_HOST</aeTitle>
19       <callingAeIp>1[redacted]</callingAeIp>
20       <buildImageSR>true</buildImageSR>
21       <fetchVAOnly>false</fetchVAOnly>
22       <modalityBlockList>
23         <gov.va.med.imaging.facade.configuration.ScpModalityList>
24           <dataSource>ALL</dataSource>
25           <addImageLevelFilter>false</addImageLevelFilter>
26           <modalities>
27             <string>none</string>
28           </modalities>
29         </gov.va.med.imaging.facade.configuration.ScpModalityList>
30       </modalityBlockList>
31     </gov.va.med.imaging.facade.configuration.ScpCallingAE>
32   </callingAEConfigs>
33 </gov.va.med.imaging.facade.configuration.ScpConfiguration>
```

If additional changes to the defaults for the Tomcat DICOM SCP Configuration and/or Laurel Bridge DICOM SCP Configuration are desired, see the *VIX Administrator's Guide* for details.

NOTE: If desired to see only VA studies (currently VA Cerner Images - 200CRNR - are not being retrieved and are scheduled for the next release) and prevent DoD studies from being retrieved, set fetchVAOnly to true inside the opening and closing fetchVAOnly tags, otherwise set false (inside <fetchVAOnly> </fetchVAOnly> - line 21)

NOTE: For each additional DICOM SCP client, insert an additional block of code containing the elements from lines 17 to 31 before current line 32 (Figure 80), as described in the *VIX Administrator's Guide*.

If additional updates are needed to the access and verify codes for the account with VistA credentials see the section "Modifying the ROI Processing and DICOM Query/Retrieve Parameters of the VIX" in the *VIX Administrator's Guide* to update (preferred) or see the section "*Reconfiguring a VIX Server*," in this VIX Installation Guide to perform a reconfigure installation.

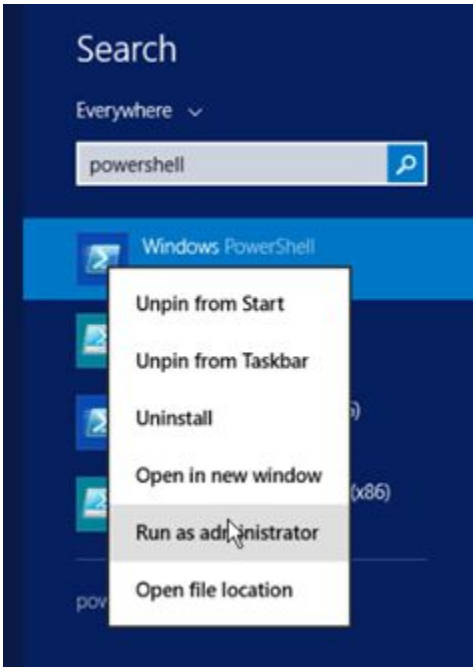
9. Appendix C: Restart Script

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

Perform the following:

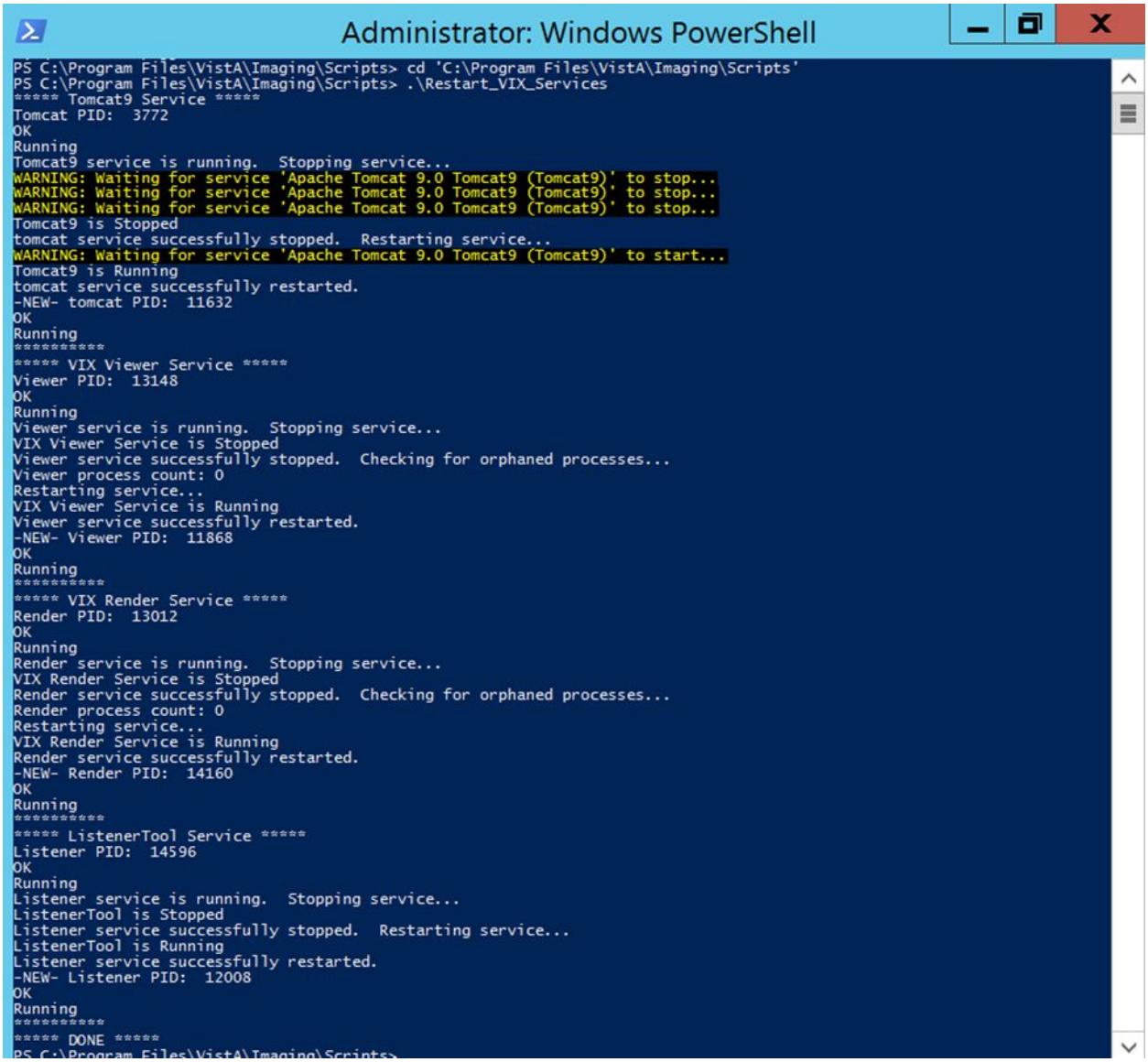
1. Run PowerShell as an administrator (Figure 81).
    a. Right-click **Start**.
    b. Left-click **Search**.
    c. Type **powershell**.
    d. Right-click **Windows PowerShell**.
    e. Left-click Run as administrator.

Figure 81: Execute Windows PowerShell



2. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes**.
3. Once PowerShell launches, **type** the command:
   `cd "C:\Program Files\VistA\Imaging\Scripts"`
   Then press **[ENTER]** to change the working directory to the Scripts folder.
4. Then **type** the command:
   `.\Restart_VIX_Services.ps1`
   And press **[ENTER]** to execute the restart script. Wait for the script to complete (Figure 82).

Figure 82: Windows PowerShell Restart Script



5. Close PowerShell.

10. Appendix D: Tomcat Permissions

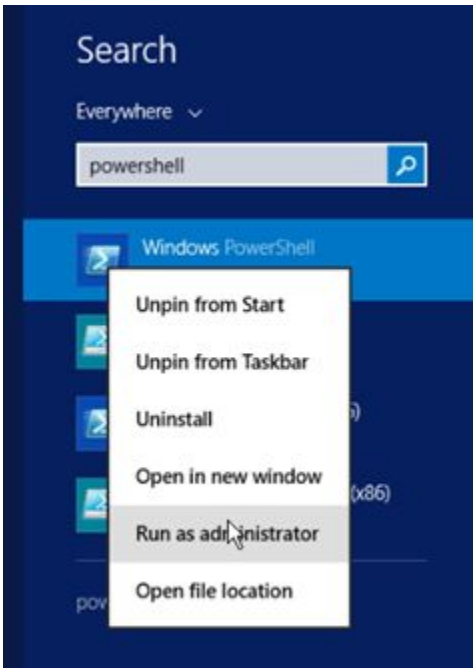
Due to the VA group policy restriction or rules, there may be an issue found while the VIX installer wizard is setting file system access rules - i.e.: ...error denying access to apachetomcat account to c:\...

To resolve this, after the VIX Installation, run the tomcat permissions script (permission_fixer.ps1).

Perform the following:

1. Run PowerShell as an administrator (Figure 83).
    a. Right-click **Start**.
    b. Left-click **Search**.
    c. Type **powershell**.
    d. Right-click **Windows PowerShell**.
    e. Left-click Run as administrator.

Figure 83: Execute Windows PowerShell



2. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes**.
3. Once PowerShell launches, **type** the command:
   `cd "C:\Program Files\VistA\Imaging\Scripts"`
   Then press **[ENTER]** to change the working directory to the Scripts folder.
4. Then **type** the command:
   `.\permission_fixer.ps1`
   And press **[ENTER]** to execute the permission fixer script. Wait for the script to complete.

5. Close PowerShell.
6. Follow the steps in *Appendix C: Restart Script* to execute the restart script.

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

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

NOTE: In the event the installation is unable to set the permissions for YOUR_DRIVE_LETTER:\VixCache (stops or is hung) the contents of the YOUR_DRIVE_LETTER:\VixCache folder and the existing subfolders: va-metadata-region, va-image-region, dod-metadata-region, and dod-image-region, in the YOUR_DRIVE_LETTER:\VixCache folder can be deleted.

If the installation is unable to set the permissions for YOUR_DRIVE_LETTER:\VixCache, perform the following before re-attempting installation:

1. Run PowerShell as an administrator (Figure 83).
    a. Right-click **Start**.
    b. Left-click **Search**.
    c. Type **powershell**.
    d. Right-click **Windows PowerShell**.
    e. Left-click Run as administrator.
2. If prompted with "Do you want to allow the following program from an unknown publisher to make changes to this computer?", click **Yes**.
3. Once PowerShell launches, **type** the command:

    ```
    $vixLocalCachePath =
    [System.Environment]::GetEnvironmentVariable('vixcache') -
    replace "/", "\"
    ```

    Then press **[ENTER]** to set the path of YOUR_DRIVE_LETTER:\VixCache.

    NOTE: If the system variable for the vixcache is not set, use the below command instead and replace YOUR_DRIVE_LETTER with your drive letter of the VixCache folder.

    ```
    $vixLocalCachePath = "YOUR_DRIVE_LETTER:\VixCache"
    ```

4. Now **type** the command:

    ```
    Get-ChildItem -Path "\\?\$($vixLocalCachePath)" -Recurse |
    Foreach-object {Remove-item -Recurse -Force -path
    $_.FullName}
    ```

Then press **[ENTER]** to delete the sub-folders in YOUR_DRIVE_LETTER:\VixCache.

5. Once the command completes, **type** the command:
   ```
   cd "C:\Program Files\VistA\Imaging\Scripts"
   ```
   Then press **[ENTER]** to change the working directory to the Scripts folder.
6. Then **type** the command:
   ```
   .\permission_fixer.ps1
   ```
   And press **[ENTER]** to execute the permission fixer script. Wait for the script to complete.
7. Close PowerShell.

11. Appendix E: Service Account Settings

The VIX uses a service account on the local VistA for periodic processing of ROI disclosure requests and DICOM query retrieve SCP requests. The service account may be the same one used by the DICOM Gateway and the Hybrid DICOM Gateway (HDIG). You may also use it to log into the new VIX Tools page described in the *Verifying Access to the VIX Tools and VIX Transaction Log* section.

Table 2 lists each VIX site's current and suggested local VistA service account. The Designated User (DUZ) identifies the service account on the local VistA. The suggested service account enables each site to have a unique name.

The VIX's service account on its local VistA must have the following SSN format, security keys, secondary menus, a value for the INITIAL field, RAD/NUC med classification, CPRS TAB, and authorized to write med orders. If any setting is missing, update the service account.

NOTE: If unable to update the service account on the local VistA yourself, please create a ticket assigned to the ESD Tier 1 group to update the service account on the local VistA. Example text for the ticket appears after the table.

Set the SSN of the service account on the local VistA as specified in Table 2 if not already set. All SSNs begin with 9 to avoid possible collisions with a real SSN issued by the Social Security Administration.

Verify the service account on the local VistA has the following security keys:

- MAG SYSTEM
- MAG VIX ADMIN
- MAG DOD FIX
- RA MGR
- RA VERIFY
- RA ALLOC

Verify the service account on the local VistA has the following secondary menus:

- MAG WINDOWS (All MAG* RPC's)
- MAG DICOM VISA (DICOM VISA)
- OR CPRS GUI CHART (CPRSChart version x.xx.xxx.x)
- MAG DICOM GATEWAY FULL
- MAG DICOM QUERY RETRIEVE

Verify the service account on the local VistA has a value for the INITIAL field.

Verify the service account on the local VistA has the following RAD/NUC med classification:

- 1 staff
- 4 technologist

Verify the service account on the local VistA has the following CPRS TAB:

- CPRS TAB: COR

- EFFECTIVE DATE: <TODAY

Verify the service account on the local VistA has the following authorized to write med orders:

- YES

NOTE: To verify the service account on the local VistA has a value for the INITIAL field perform the following:

1. Access VA FileMan [DIUSER] in your VistA instance.
2. Select Inquire to File Entries [DIINQUIRE], then choose the NEW PERSON file (#200).
3. When prompted "Select NEW PERSON NAME", select your VistA Imaging service account.
4. Either answer Yes to Standard Captioned Output (followed by No in "Include COMPUTED fields"), or answer No, and then choose the INITIAL field (#1).
5. The latter just shows the INITIAL field, the former shows all fields. Either way, verify that the results include a value for the account's initials.

If the service account on the local VistA does not have a value for the INITIAL field set one:

1. Access VA FileMan [DIUSER] in your VistA instance.
2. Select Enter or Edit File Entries [DIEDIT], then choose the New Person file (#200). When prompted "EDIT WHICH FIELD", choose INITIAL (#1).
3. When prompted "Select NEW PERSON NAME", choose your VistA Imaging service account.
4. Finally, when you see the "INITIAL" prompt, enter the initials for the user. Enter any appropriate value, such as VSA.

Table 2: VIX Site's User Profile SSN, Service Account on Local VistA, and Suggested Service Account on Local VistA

Site Name	Site Number	VIX User Profile SSN	VIX's Service Account on Local VistA	Suggested VIX's Service Account on Local VistA
Manila, PI	358	REDACTED		REDACTED
Togus, ME	402	REDACTED	REDACTED	REDACTED
White River Junction, VT	405	REDACTED	REDACTED	REDACTED
Montana HCS	436	REDACTED	REDACTED	REDACTED
Fargo, ND	437	REDACTED	REDACTED	REDACTED
Sioux Falls, SD	438	REDACTED	REDACTED	REDACTED
Cheyenne, WY	442	REDACTED	REDACTED	REDACTED
Honolulu, HI	459	REDACTED	REDACTED	REDACTED
Wilmington, DE	460	REDACTED	REDACTED	REDACTED
Anchorage, AK	463	REDACTED	REDACTED	REDACTED
Albuquerque, NM	501	REDACTED	REDACTED	REDACTED
Alexandria, LA	502	REDACTED	REDACTED	REDACTED
Altoona, PA	503	REDACTED	REDACTED	REDACTED
Amarillo, TX	504	REDACTED	REDACTED	REDACTED
Ann Arbor, MI	506	REDACTED	REDACTED	REDACTED
Atlanta, GA	508	REDACTED	REDACTED	REDACTED
Augusta, GA	509	REDACTED	REDACTED	REDACTED
Maryland HCS	512	REDACTED	REDACTED	REDACTED
Battle Creek, MI	515	REDACTED	REDACTED	REDACTED

Bay Pines, FL	516	REDACTED	REDACTED	REDACTED
Beckley, WV	517	REDACTED	REDACTED	REDACTED
Bedford, MA	518	REDACTED	REDACTED	REDACTED
Big Spring, TX	519	REDACTED	REDACTED	REDACTED
Biloxi, MS	520	REDACTED	REDACTED	REDACTED
Birmingham, AL	521	REDACTED	REDACTED	REDACTED
Boston HCS	523	REDACTED	REDACTED	REDACTED
Bronx, NY	526	REDACTED	REDACTED	REDACTED
Upstate NY HCS	528	REDACTED	REDACTED	REDACTED
Butler, PA	529	REDACTED	REDACTED	REDACTED
Boise, ID	531	REDACTED	REDACTED	REDACTED
Charleston, SC	534	REDACTED	REDACTED	REDACTED
Chicago, IL (Westside)	537	REDACTED	REDACTED	REDACTED
Chillicothe, OH	538	REDACTED	REDACTED	REDACTED
Cincinnati, OH	539	REDACTED	REDACTED	REDACTED
Clarksburg, WV	540	REDACTED	REDACTED	REDACTED
Cleveland, OH	541	REDACTED	REDACTED	REDACTED
Coatesville, PA	542	REDACTED	REDACTED	REDACTED
Columbia, SC	544	REDACTED	REDACTED	REDACTED
Miami, FL	546	REDACTED	REDACTED	REDACTED
West Palm Beach, FL	548	REDACTED	REDACTED	REDACTED
North Texas HCS	549	REDACTED	REDACTED	REDACTED
Danville, IL	550	REDACTED	REDACTED	REDACTED

Dayton, OH	552	REDACTED	REDACTED	REDACTED
Detroit, MI	553	REDACTED	REDACTED	REDACTED
Eastern Colorado HCS	554	REDACTED	REDACTED	REDACTED
North Chicago, IL	556	REDACTED	REDACTED	REDACTED
Dublin, GA	557	REDACTED	REDACTED	REDACTED
Durham, NC	558	REDACTED	REDACTED	REDACTED
New Jersey HCS	561	REDACTED	REDACTED	REDACTED
Erie, PA	562	REDACTED	REDACTED	REDACTED
Fayetteville, AR	564	REDACTED	REDACTED	REDACTED
Fayetteville, NC	565	REDACTED	REDACTED	REDACTED
Black Hills HCS	568	REDACTED	REDACTED	REDACTED
Fresno, CA	570	REDACTED	REDACTED	REDACTED
N. Florida/S. Georgia HCS	573	REDACTED	REDACTED	REDACTED
Grand Junction, CO	575	REDACTED	REDACTED	REDACTED
Hines, IL	578	REDACTED	REDACTED	REDACTED
Houston, TX	580	REDACTED	REDACTED	REDACTED
Huntington, WV	581	REDACTED	REDACTED	REDACTED
Indianapolis, IN	583	REDACTED	REDACTED	REDACTED
Iron Mountain, MI	585	REDACTED	REDACTED	REDACTED
Jackson, MS	586	REDACTED	REDACTED	REDACTED
Kansas City, MO	589	REDACTED	REDACTED	REDACTED
Hampton, VA	590	REDACTED	REDACTED	REDACTED
Las Vegas, NV	593	REDACTED	REDACTED	REDACTED

Lebanon, PA	595	REDACTED	REDACTED	REDACTED
Lexington, KY	596	REDACTED	REDACTED	REDACTED
Little Rock, AR	598	REDACTED	REDACTED	REDACTED
Long Beach, CA	600	REDACTED	REDACTED	REDACTED
Louisville, KY	603	REDACTED	REDACTED	REDACTED
Loma Linda, CA	605	REDACTED	REDACTED	REDACTED
Madison, WI	607	REDACTED	REDACTED	REDACTED
Manchester, NH	608	REDACTED	REDACTED	REDACTED
Northern Indiana HCS	610	REDACTED	REDACTED	REDACTED
Northern California HCS	612	REDACTED	REDACTED	REDACTED
Martinsburg, WV	613	REDACTED	REDACTED	REDACTED
Memphis, TN	614	REDACTED	REDACTED	REDACTED
Minneapolis, MN	618	REDACTED	REDACTED	REDACTED
Central Alabama HCS	619	REDACTED	REDACTED	REDACTED
Hudson Valley HCS	620	REDACTED	REDACTED	REDACTED
Mountain Home, TN	621	REDACTED	REDACTED	REDACTED
Muskogee, OK	623	REDACTED	REDACTED	REDACTED
Tennessee Valley HCS	626	REDACTED	REDACTED	REDACTED
New Orleans, LA	629	REDACTED	REDACTED	REDACTED
NY HCS	630	REDACTED	REDACTED	REDACTED
Northampton, MA	631	REDACTED	REDACTED	REDACTED
Northport, NY	632	REDACTED	REDACTED	REDACTED
Oklahoma City, OK	635	REDACTED	REDACTED	REDACTED

Central Plains HCS	636	REDACTED	REDACTED	REDACTED
Asheville, NC	637	REDACTED	REDACTED	REDACTED
Palo Alto HCS	640	REDACTED		REDACTED
Philadelphia, PA	642	REDACTED	REDACTED	REDACTED
Phoenix, AZ	644	REDACTED	REDACTED	REDACTED
Pittsburgh HCS	646	REDACTED	REDACTED	REDACTED
Portland, OR	648	REDACTED	REDACTED	REDACTED
Prescott, AZ	649	REDACTED	REDACTED	REDACTED
Providence, RI	650	REDACTED	REDACTED	REDACTED
Richmond, VA	652	REDACTED	REDACTED	REDACTED
Roseburg, OR	653	REDACTED	REDACTED	REDACTED
Reno, NV	654	REDACTED	REDACTED	REDACTED
Saginaw, MI	655	REDACTED	REDACTED	REDACTED
St. Cloud, MN	656	REDACTED	REDACTED	REDACTED
St. Louis, MO	657	REDACTED	REDACTED	REDACTED
Salem, VA	658	REDACTED	REDACTED	REDACTED
Salisbury, NC	659	REDACTED		REDACTED
Salt Lake City, UT	660	REDACTED	REDACTED	REDACTED
San Francisco, CA	662	REDACTED		REDACTED
Puget Sound HCS	663	REDACTED	REDACTED	REDACTED
San Diego, CA	664	REDACTED	REDACTED	REDACTED
Sheridan, WY	666	REDACTED	REDACTED	REDACTED
Shreveport, LA	667	REDACTED	REDACTED	REDACTED

Spokane, WA	668	REDACTED	REDACTED	REDACTED
South Texas HCS	671	REDACTED	REDACTED	REDACTED
San Juan, PR	672	REDACTED	REDACTED	REDACTED
Tampa, FL	673	REDACTED	REDACTED	REDACTED
Central Texas HCS	674	REDACTED	REDACTED	REDACTED
Orlando, FL	675	REDACTED	REDACTED	REDACTED
Tomah, WI	676	REDACTED	REDACTED	REDACTED
Tucson, AZ	678	REDACTED	REDACTED	REDACTED
Tuscaloosa, AL	679	REDACTED	REDACTED	REDACTED
Walla Walla, WA	687	REDACTED	REDACTED	REDACTED
Washington, DC	688	REDACTED	REDACTED	REDACTED
Connecticut HCS	689	REDACTED	REDACTED	REDACTED
West Los Angeles, CA	691	REDACTED	REDACTED	REDACTED
White City OR	692	REDACTED	REDACTED	REDACTED
Wilkes Barre, PA	693	REDACTED	REDACTED	REDACTED
Milwaukee, WI	695	REDACTED		REDACTED
Valley Coastal Bend HCS	740	REDACTED	REDACTED	REDACTED
El Paso, TX	756	REDACTED	REDACTED	REDACTED
Columbus, OH	757	REDACTED	REDACTED	REDACTED
Billings, MT CBOC	436GH	REDACTED	REDACTED	REDACTED
Pensacola, FL	520BZ	REDACTED	REDACTED	REDACTED
Canandaigua, NY	528A5	REDACTED	REDACTED	REDACTED
Bath, NY	528A6	REDACTED	REDACTED	REDACTED

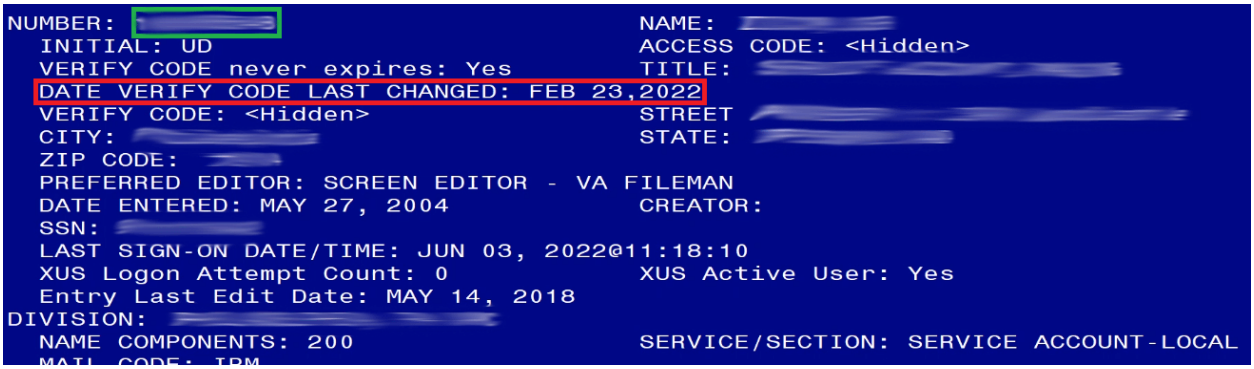
Syracuse, NY	528A7	REDACTED	REDACTED	REDACTED
Albany, NY	528A8	REDACTED	REDACTED	REDACTED
Lake City VA Medical Center	573A4	REDACTED	REDACTED	REDACTED
Columbia, MO	589A4	REDACTED	REDACTED	REDACTED
Topeka, KS	589A5	REDACTED	REDACTED	REDACTED
Leavenworth, KS	589A6	REDACTED	REDACTED	REDACTED
Wichita, KS	589A7	REDACTED	REDACTED	REDACTED
Lexington, KY -CDD	596A4	REDACTED	REDACTED	REDACTED
Grand Island, NE	636A4	REDACTED	REDACTED	REDACTED
Lincoln, NE	636A5	REDACTED	REDACTED	REDACTED
Central Iowa HCS	636A6	REDACTED	REDACTED	REDACTED
Iowa City, IA	636A8	REDACTED	REDACTED	REDACTED
Poplar Bluff, MO	657A4	REDACTED	REDACTED	REDACTED
Marion, IL	657A5	REDACTED	REDACTED	REDACTED

NOTE: For several sites, the VIX service accounts in Table 2 are missing because they expired at the time of this publication.

NOTE: Sites can find the DUZ corresponding to their VIX service account on the local VistA by following the steps below:

1. In FileMan, choose the option to Inquire to File Entries, choose the New Person file (#200), and then enter the name of your VIX's service account on its local VistA.
2. Accept the defaults for Standard Captioned Output, when asked "Include COMPUTED fields", answer either B or R, as you need to view the record number.
3. If multiple results are returned based on the name you entered, you will need to view each of them to determine which is your local service account and which are visitor accounts. Select one of the accounts.
4. In the data listed for each account, check for the presence of the DATE VERIFY CODE LAST CHANGED field (refer to the red highlighted field in Figure 84). If the DATE VERIFY CODE LAST CHANGED field is not present return to step 2 and select a different account upon reaching step 4, otherwise continue to the next step.

Figure 84: FileMan File Entry 200



5. If the field is present, it is the VIX's service account on the local VistA. If it is not, it is a visitor account and should not be edited. The number printed in the NUMBER field is the DUZ of the VIX's service account on the local VistA (refer to the green highlighted field in Figure 84). Record the DUZ of the VIX's service account on the local VistA. (Consider documenting the DUZ of the service account on the local VistA in your Master Site Profile.)

NOTE: Once the DUZ is obtained, follow the steps below to update the corresponding VIX's service account on the local VistA:

1. To view a record once you have its DUZ value, access VA FileMan [DIUSER] and select Inquire to File Entries [DIINQUIRE].
2. When prompted "Output from what File", select NEW PERSON (#200).
3. When asked to "Select NEW PERSON NAME", enter a back-tick (`) followed by the DUZ for the account. Select whichever view options you want (the defaults are fine), and then view the account's record to determine the details and make any necessary adjustments.

NOTE: If you are unable to perform the above steps, please create a support ticket with VistA Apps for assistance.

Below is an example of the information to provide in a ticket to update the VIX's service account on the local VistA. The example shows specifying the access code of the VIX's service

account on the local VistA, the name of the VIX's service account on the local VistA, the suggested name of the VIX's service account on the local VistA, the SSN of the VIX's service account on the local VistA, and any missing VistA menus, keys, and other settings to add to the VIX's service account on the local VistA. Be sure to copy and paste the security keys, secondary menus, INITIAL, and RAD/NUC information shown before Table 2 into the ticket as needed.

```
Assignment group: ESD Tier 1
Category: Service
Subcategory: Access

Please use the SITE_SERVICE_ACCOUNT_ACCESS_CODE_HERE to look up the
DUZ for the SITE_SERVICE_ACCOUNT_NAME_HERE service account in
SITE_VISTA_NAME_HERE VistA and then update the service account with
the following:
Change service account name to: IMAGINGSVC,SITE_ABBREVIATION_HERE
Add SSN: SITE_SERVICE_ACCOUNT_SSN_HERE
Add keys: MAG DOD FIX, RA ALLOC
Add secondary menus: MAG WINDOWS, MAG DICOM QUERY RETRIEVE
Add INITIAL field: VSA

Add RAD/NUC med classification: RAD/NUC MED CLASSIFICATION
                                1      staff
                                4      technologist
Add CPRS TAB: CPRS TAB: COR
              EFFECTIVE DATE: <TODAY
Add AUTHORIZED TO WRITE MED ORDERS: YES

NOTE: This is a false SSN, which was not generated by, and will not
conflict with, a real SSN issued by the Social Security
Administration, but meets the requirements for VistA Broker Security
Exchange (BSE) authentication between sites. These changes are
required for Enterprise DICOM query retrieve with MAG*3.0*269.
```

12. Appendix F: VIX Install Checklist

Table 3 summarizes the VIX installation process.

12.1. VIX Install Checklist

Table 3: VIX Install Checklist

	Requirement	Location in VIX Installation Guide	Action
☐	Install patch MAG*3.0*269 KIDS in VistA	See Installation Prerequisites	Perform steps in MAG*3.0*269 Patch Description Document
☐	Verify VIX server meets minimum hardware specifications	See *Hardware Requirements*	Allocate more CPU cores/RAM as needed to meet the minimum or recommended specifications
☐	Verify Microsoft Visual C++ 2010 Redistributable Package (x64) is installed	See *Operating System and Environment Requirements*	If required, download and install Microsoft Visual C++ 2010 Redistributable Package (x64)
☐	Verify .NET 3.5 is installed and enabled	See *Operating System and Environment Requirements*	Install and enable .NET 3.5 if required
☐	Verify .NET 4.7.2 or 4.8 is installed and enabled	See *Operating System and Environment Requirements*	If required, download and install .NET 4.7.2 or 4.8
☐	Verify PowerShell 5.1 is installed	See *PowerShell Version Verification*	If required, download and install PowerShell 5.1
☐	Verify MUSE configuration information needed for installation, if any	See *Appendix A: Enable MUSE Functionality*	Verify MUSE site number, MUSE server name, MUSE username, and MUSE password
☐	Verify you have SQL 2017 Express zip file SQLExpress_x64-14.0.1000.169	See Installation Instructions	Download from SFTP site, if required, but do not install since the VIX Service Installation Wizard does it
☐	Initiate the installation of the VIX MAG3_0P269_VIX_SETUP.msi	See Installation Instructions	Perform steps in Installation Instructions
☐	Verify that McAfee Exclusions are updated	See *McAfee Exclusions*	Perform steps in McAfee Exclusions

	Requirement	Location in VIX Installation Guide	Action
☐	Verify VIX install is complete	See *Verifying Installation/Upgrade is Complete*	Perform steps in Verifying Installation/Upgrade is Complete
☐	Verify that VIX is running	See *Verifying Installation/Upgrade is Complete*	Verify VIX is running
☐	Verify that VIX Viewer and VIX Render services running	See *Verifying Installation/Upgrade is Complete*	Verify VIX Viewer and VIX Render services are running
☐	Verify ListenerTool service is running	See *Verifying Installation/Upgrade is Complete*	Verify ListenerTool service is running
☐	Request Site Service update to your facility if needed	See *To Register the VIX*	Create a national ticket requesting CLIN3 to update your site service entry to include the new viewer (Port REDACTED for HTTPS)
☐	Verify that images, including MUSE EKGs and DoD images, can be viewed via zero-footprint Image Viewer.	See *Spot-Checking VIX Image Delivery*	Verify JLV utilizing zero-footprint viewer. If unable to view an image including MUSE EKGs and DoD images, enter a support ticket for assistance