



VistA Imaging Hybrid DICOM Image Gateway

Installation Guide

July 2019 – Revision 3.2

Department of Veterans Affairs
Product Development
Health Provider Systems

Hybrid DICOM Image Gateway Installation Guide VistA July 2019

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: <http://www.va.gov/imaging>
VA intranet: <http://vaww.va.gov/imaging>

Revision History

Date	Rev	Notes
Sep 13 2011	1	Initial draft for end of contract date 9/13/2013. M. Mitchell (Rev 1)
May 9 2016	2	Updates for MAG*3.0*162. L. Shope, J. Lin, N. Nguyen, S. Marner
May 31 2019	3	Updates for MAG*3.0*204. C. Andersen, D. Siddabathula
July 17 2019	3.2	Updates for MAG*3.0*204. C. Andersen, D. Siddabathula

Contents

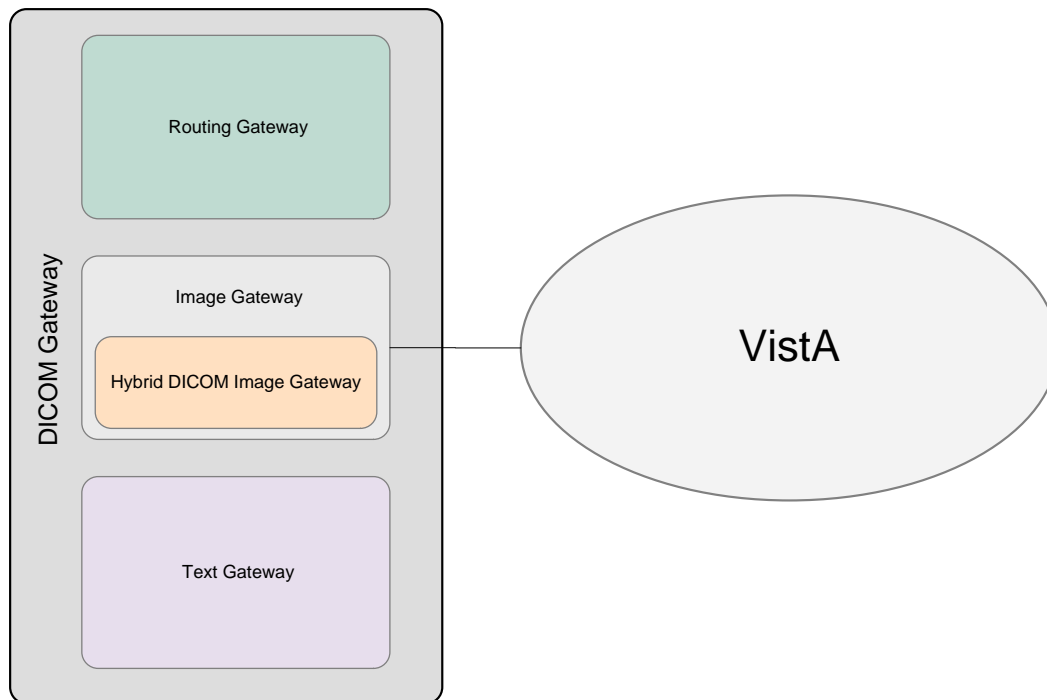
Introduction	1
The Hybrid DICOM Image Gateway	1
Intended Audience	2
Terms of Use	2
Terms and Abbreviations	2
Document Conventions	5
Installing a New HDIG	6
Preparing for a New HDIG Installation	6
Setting up VistA	6
FDA Requirements	6
Requirements for the HDIG Host	6
Site Information	8
Apache Tomcat Application Password	8
Laurel Bridge License	8
VistA Site Service	9
Java Version	9
Additional Considerations	9
New HDIG Installation	9
Running the HDIG Installer	10
Updating an Existing HDIG	25
Preparing for an HDIG	25
.NET Version Update	25
Java Version	29
Updating the HDIG	29
HDIG Post-Installation	35
Configuring the HDIG	35
Verify Antivirus Scanning Exclusions	35
Increasing the Memory Allocated to the HDIG	35
Email Notifications	39
Error Messages and Email Handling	39
Warning Message Bundling for Email Handling	39
Warning Email Handling Configuration Guidelines	39
Configure the HDIG for Each Image Processing Server	40
Verify the HDIG Service Account Credentials	40
Updating the HDIG Administrator Email Address(es)	41
Save the HDIG Stat Page as the Home page	41
Save the HDIG Logs Page as a favorite	42
Testing the HDIG Operation	42
Review the HDIG Stats Page for Each Image Gateway Server	42
Test and Review HDIG and Legacy Image Processing	42
Post Installation	45
Complete Appendix D – Post-Install Checklist	45

Appendix A Activating the DCF Toolkit Product Serial Number ...	46
Network Activation	46
Manual Activation	48
Appendix B The DICOM AE Security Matrix	50
Overview - Configuring the DICOM AE Security Matrix	52
Entries for Storage Functionality.....	52
Entries for Query/Retrieve Functionality.....	52
Entries for Import Functionality - Media	52
Entries for Import Functionality – Network Import	53
Fields in the DICOM AE SECURITY MATRIX	53
Example DICOM AE SECURITY MATRIX Values (partial).....	61
Adding Devices to the DICOM AE SECURITY MATRIX	62
Entries for Storage Commitment Requests	66
Appendix C Pre-Install Checklist	77
Appendix D Post-Install Checklist	79
Appendix E DCF Toolkit Enterprise License Request Form	81

Introduction

The Hybrid DICOM Image Gateway

The Hybrid Digital Imaging and Communications in Medicine (DICOM) Image Gateway (HDIG) is a new component of the DICOM Gateway, introduced in MAG*3.0*34 to enable the storage of the newly supported Service Object Pair (SOP) classes.



When you install the HDIG, you can select these components:

- **DICOM Listener.** The DICOM Listener listens on a specific port for incoming DICOM objects from pre-defined DICOM devices (Application Entities). It validates all newly supported SOP classes and stores the DICOM objects that pass the various validation checks in the new database structure. It forwards the previously supported SOP classes to the legacy gateway application for processing and storage in the old database.
- **Archiver.** The Archiver archives the newly supported SOP classes.
- **New Abstract Maker.** The new Abstract Maker creates abstracts (thumbnail icons) for the newly supported SOP classes.

In the course of installing the HDIG, you are prompted to select the components you want to enable on the specific gateway. You can enable all components on

one gateway. You must have at least one instance of each component enabled at your site.

Intended Audience

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

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

Terms of Use

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



Caution: Federal law restricts this device to use by or on the order of either a licensed practitioner or persons lawfully engaged in the manufacture or distribution of the product.



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



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

Terms and Abbreviations

The following terms are used in this document.

Term	Definition
ACL	Access Control List
AE	Application Entity: An end point of a DICOM information exchange, including the DICOM network or media interface software; that is, the software that sends or receives DICOM information objects or messages. A single device may have multiple Application Entities.
AESM	DICOM AE SECURITY MATRIX – a file in VistA for defining DICOM modality roles and service privileges

AE_Title	The unique name assigned to a DICOM application to identify the application to other DICOM applications on the network.
Application log	The primary log on the HDIG to which it writes application-level events.
Codec	Encoding/Decoding of digital information
cPACS	Commercial PACS
CPU	Central Processing Unit
CVIX	Centralized Vista Imaging eXchange
DCF	DICOM Connectivity Framework
DICOM	Digital Imaging and Communication in Medicine
DICOM Correct	The name assigned to the process used to correct DICOM Objects that fail processing on the DICOM Gateway.
DICOM Importer	Refers to the application that performs the automated DICOM import process from outside facilities.
DICOM Role	Defines how a DICOM Service will perform the role as either a SCP or a SCU.
DICOM Service	Consists of many different services, most of which involve transmission of data over a network

Term	Definition
DoD	Department of Defense
DVD	Digital Versatile Disc
HDIG	Hybrid DICOM Image Gateway: An image gateway that combines the legacy DICOM Gateway and the new VISA Gateway. It implements DICOM services.
IHS	Indian Health Services
JRE	Java Runtime Environment
KIDS	Kernel Installation and Distribution System
Modality Device	The type of DICOM device being used to generate or utilize DICOM objects.
Outside Facility	External to the local facility. It can be another VA facility, a DoD facility, or another institution.
PACS	Picture Archiving and Communications System
PSN	Product Serial Number
Q/R	Query/Retrieve
RPC	Remote Procedure Call
SCP	Service Class Provider
SCU	Service Class User
SOP	Service Object Pair
SOP Class	Unique identifier assigned by the DICOM Standard to identify DICOM objects.
Staging	<p>Copying study data from either media or an authorized network location into temporary persistent storage for later reconciliation. There are two types of staging (controlled by Security Keys):</p> <p><i>Basic Staging:</i> An authorized user copies all study data from an authorized source to Importer Persistent Storage.</p> <p><i>Advanced Staging:</i> An authorized user can view source data by study and copy data by study to Importer Persistent Storage.</p>
Supported SOP Class	A DICOM Object that can be processed by the DICOM Gateway and delivered to other VistA Imaging applications for use within VistA Imaging.

Term	Definition
UID	Unique identifier
VA	US Department of Veterans Affairs
VISA	VistA Imaging Services Architecture
VistA	Veterans Health Information Systems and Technology Architecture
VIX	VistA Imaging eXchange

Document Conventions

The following typographic conventions are used in this document.

Symbol/Typeface	Meaning/Use	Example
Bold	User input, selection, GUI element (menu item, button, field)	Click Finish . Choose Open from the File menu. Type the user account name in the Name field.
Monospaced font (typically, in a box) (Bo ld indicates user input or selection).	Command-line sample or output (such as character-based screen captures and computer source code), menus, file names	Navigate to the \\Docs\\Imaging_Docs_Latest folder.
<i>Italics</i>	Emphasis, reference to section in the document or another document, or a variable	For more information, see the <i>VistA Imaging DICOM Gateway Installation Guide</i> .
Square brackets, monospace or italics	Variable, placeholder, VistA menu	Access the Kernel Installation and Distribution System Menu [XPD MAIN]. ;;3.0;IMAGING;*[Patch List]**;Mar 19, 2002;Build 1989;Feb 21, 2011 MAG*3.0*<PatchNumber>.KID
<Enter> in character-based screen captures	Indicates that the user should press the Enter or Return key.	THEN PRINT FIELD: <Enter>

Symbol/Typeface	Meaning/Use	Example
UPPERCASE	M code, variable names, or the formal name of options, field/file names, and security keys.	The XUPROGMODE key

Installing a New HDIG

This section explains how to implement a new HDIG.

Tip: If you are updating an existing HDIG, refer to section Updating an Existing HDIG.

Preparing for a New HDIG Installation

Before starting the HDIG installation, do the following:

Setting up VistA

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

FDA Requirements

The HDIG is a component of VistA Imaging and is therefore regulated as a medical device by the FDA.

Requirements for the HDIG Host

A VistA Imaging Exchange (VIX) is required for the HDIG software and the VIX must be running latest version. If you do not have a VIX or the latest version installed, please refer to the [VIX Installation Guide](#).

Important: The VIX server and the HDIG must be on different computers.

You must install the HDIG on all DICOM Image Gateways. Do not install the HDIG on dedicated TEXT or ROUTING gateways that do not process images.

Installing the HDIG updates the Query/Retrieve service and the server side of the DICOM Importer III application. You must enable the DICOM Listener on all DICOM Gateways on which you want to have any of the following:

- DICOM Listener to receive and process incoming images
- DICOM Importer III server to process imported images and DICOM Correct to correct patient or study lookup errors
- Query/Retrieve service

Hardware Requirements

Minimum hardware requirements for installing the HDIG:

- Eight gigabytes of RAM are recommended.
- A dedicated local drive for the HDIG with at least 75 gigabytes of disk space. A larger drive may be desirable based on usage.

Network Requirements

- The HDIG cannot be installed on the same server as the VIX.
- Ports 443, 8080 and 8443 must be accessible to VA wide area network IP addresses/FQDN from the HDIG server.
- The VistA Site Service must be accessible from the HDIG computer. The VistA Site Service is a central repository of information used by Imaging components to connect to other sites. For more information about it, see the *VistA Imaging System Technical Manual*.

Operating System and Environment Requirements

The HDIG can only run on a computer with the following infrastructure elements installed:

- Windows Server 2012 Standard or Enterprise Edition

Note: Use Windows Updater to install any security updates available for .NET 4.6.2 and above. If there are issues installing the .NET framework, please reach out to the Helpdesk or CLIN3.

Note: More recent .NET updates can be installed but be certain that .NET 4.6.2 and above are included in the installation.

Note: If the Tier 1 equipment vendor (i.e., HP) template is used to create the virtual machine, then the appropriate .NET version may be included.

Older Modalities and DICOM Modality Worklist Support

If you are a site that has any older modalities installed, then verify that the modality is able to fully support the DICOM Modality Worklist function – Query

by Accession Number. Some of the older devices only support query by case numbers.

Site Information

Make sure you have the following information about your site and VistA installation, which you must supply when you install the HDIG:

- Division and/or site code: the value of the field STATION NUMBER as defined in the INSTITUTION file (#4)
- Name of the VistA host and the domain
- Name of the DICOM Gateway host
- DICOM Gateway service account details:
 - ✦ DICOM Gateway Service Account logon
 - Access code
 - Verify code

Apache Tomcat Application Password

1. Prepare a password to be used for the Apache Tomcat administrator account that will be created as part of the HDIG installation process.
 - This account will be rarely used; it only needs to be secured properly.
 - The password is case-sensitive and only alphanumeric characters are allowed.
2. Prepare a password to be used for the Apache Tomcat application account that will be created as part of the HDIG installation process.
 - This Windows account, which will be named “apachetomcat” when it is created by the HDIG installer, is used to run the HDIG in the Tomcat environment. This account is limited to only the functions it needs to run the HDIG.
 - The password is case sensitive, must contain at least eight characters, and must contain at least one capital letter and one number.

Laurel Bridge License

Installation requires an upgrade to the Laurel Bridge DCF license for each gateway that performs DICOM image processing. Time required to complete this task will vary depending on the number of DICOM Gateways.

Request the product serial numbers from Laurel Bridge. See Appendix A, Appendix A Activating the DCF Toolkit Product Serial Number.

Note: The DICOM Listener, which is included as part of the Query/Retrieve application, requires an upgrade of the existing Laurel Bridge DCF License to version 3.3.x.

Upgrading the license keys is a two-part process. As part of the planning process, required information is submitted to Laurel Bridge to request Product Serial Numbers for each gateway server that will have an HDIG installed.

During the installation of the HDIG, the Product Serial Numbers will be used to activate the new licenses on the HDIGs.

VistA Site Service

The VistA Site Service resides on the Centralized VistA Imaging eXchange (CVIX) host. Make sure that you have the location (URL) of the VistA Site Service and that the service is accessible from the computer on which you are installing the HDIG.

To find out if the VistA Site Service is accessible, try to access the VistA Site Service location (URL) from a browser on the computer on which you plan to install the HDIG:

<http://siteserver.vista.med.va.gov/VistaWebSvcs/ExchangeSiteService>

Java Version

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

Additional Considerations

- Verify that the DICOM Correct queue is empty (#2006.575).
- If you are using the Importer, verify that all studies have been reconciled and that the Importer queue is empty (#2006.5752).
- MAG*3.0*118 introduced a new file called the DICOM AE SECURITY MATRIX file (#2006.9192). The time it takes to configure this file will depend on the number of modality devices being configured. Estimate approximately one minute per device. **Note:** This should be configured after installing the KIDS but prior to performing the Gateway installations.

New HDIG Installation

This section explains how to install a new installation of the Hybrid DICOM Image Gateway (HDIG).

Note: The screenshots are provided as a representation and the actual screenshots may show different patch numbers, path locations and other details.

Running the HDIG Installer

The HDIG installer runs two consecutive installation processes. The first is very short; it installs the HDIG installation wizard. The second installs and configures the HDIG.

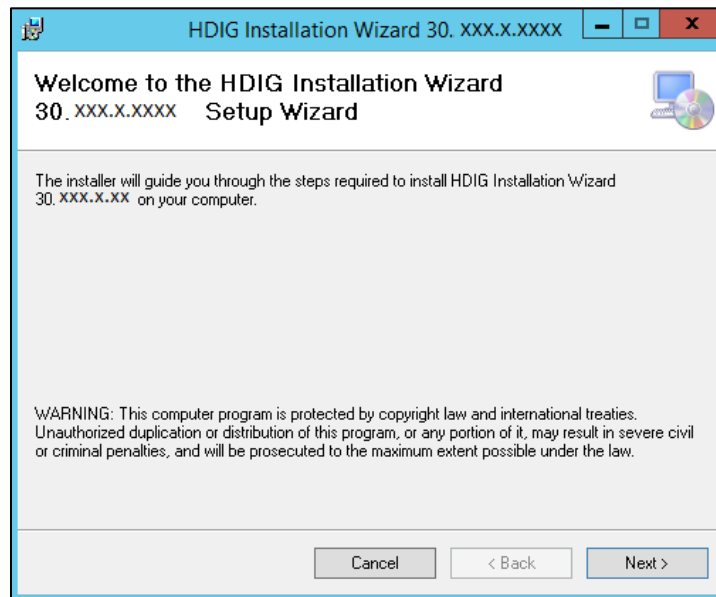
Step 1 - Install the HDIG Installer

1. Log into the computer on which the HDIG will be installed using the administrator account you used to install the DICOM Gateway portion of the patch.
2. Copy the HDIG installation file (MAG3_0P<patch #>_HDIG_Setup.msi) to a local folder on the server.

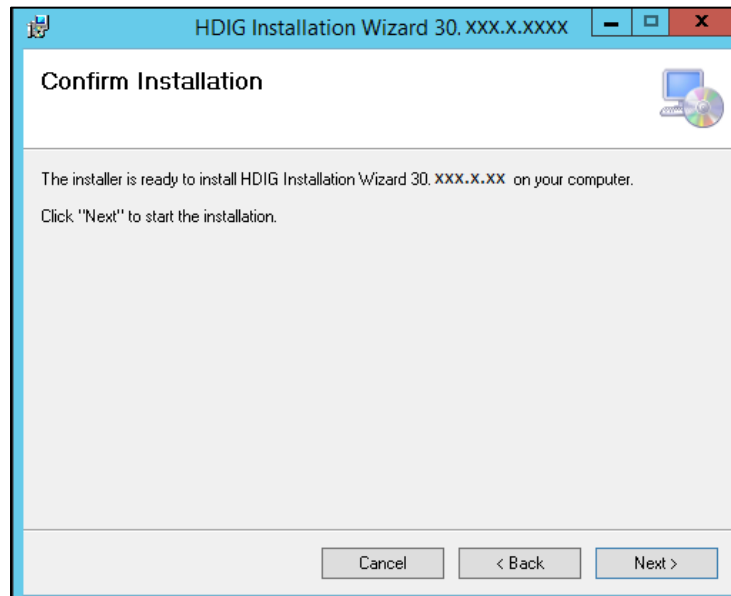
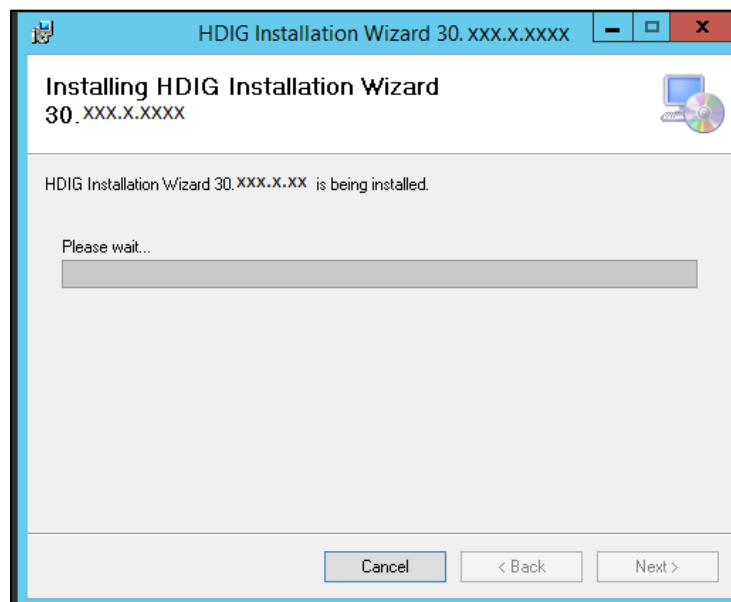
Note: When you run the HDIG installer, make sure that all other applications are closed and that the focus is left on the installer. If you have other applications running, including other instances of the installer, you may get an error message.

3. Do the following to prepare the HDIG Installation Wizard:
 - a. Double-click the HDIG installation file.

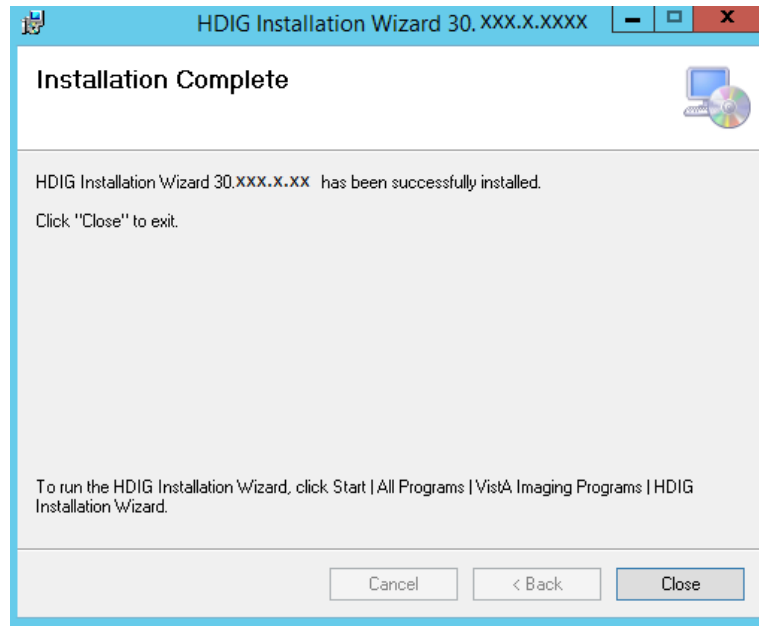
Figure 1: HDIG Installation Wizard Welcome Page



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

Figure 2: HDIG Installation Wizard Confirmation Page**Figure 3: HDIG Installation Wizard Installation Page**

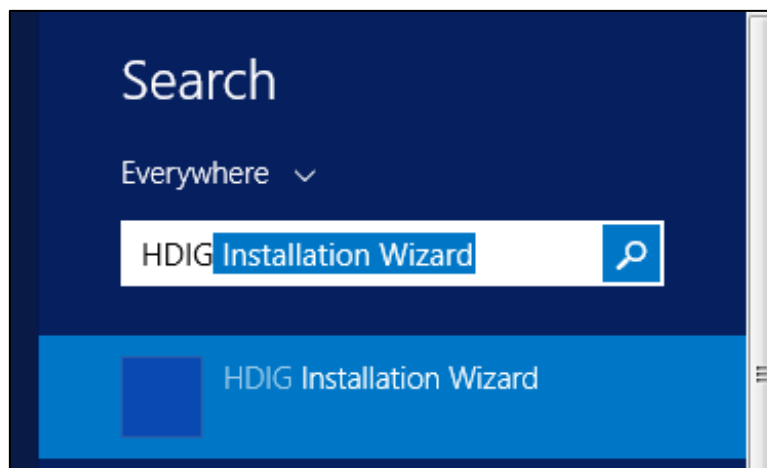
The following screen appears:

Figure 4: HDIG Installation Wizard Installation Complete Page

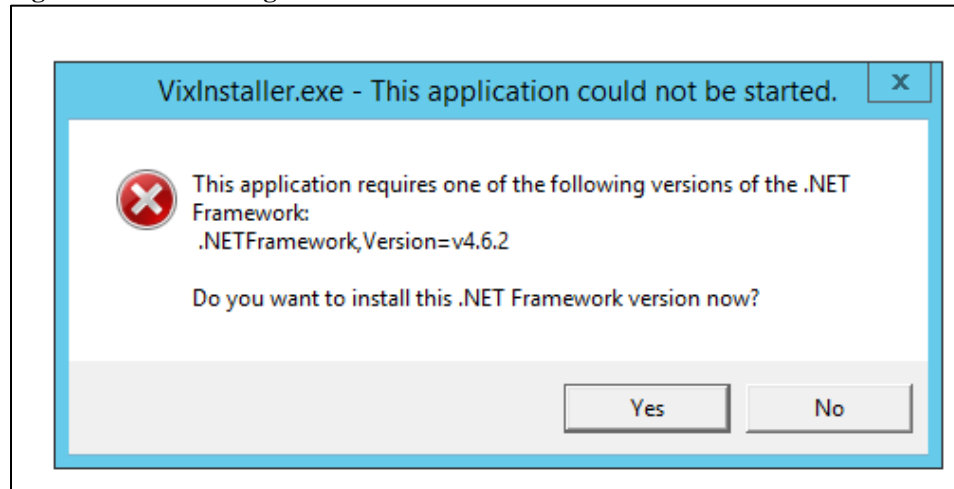
- d. When the Installation Complete screen displays, click **Close**.

Step 2 - Running the HDIG Installer

1. Choose Start | All Programs | Vista Imaging Programs | HDIG Installation Wizard to start the HDIG Installation Wizard.

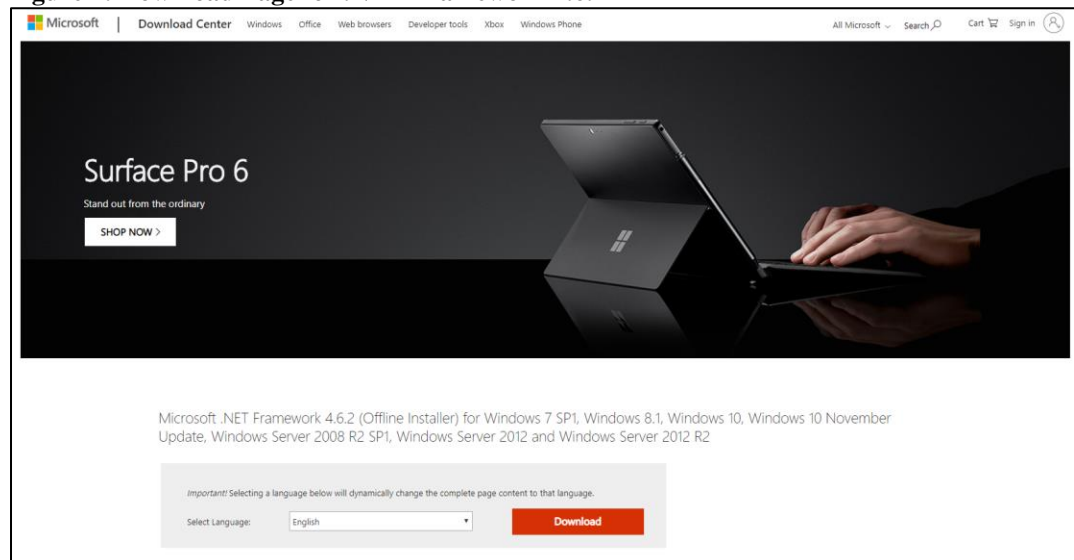
Figure 5: Manual Search Field

- a. When attempting to run the HDIG Installation Wizard you may receive the following error:

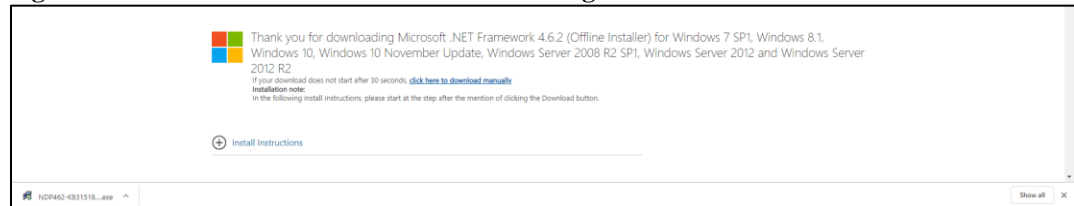
Figure 6: Error Message

Note: You must have an active internet connection to click “Yes” and follow the next steps. If you do not have an active internet connection, STOP HERE and please contact your Help Desk/CLIN3 for assistance.

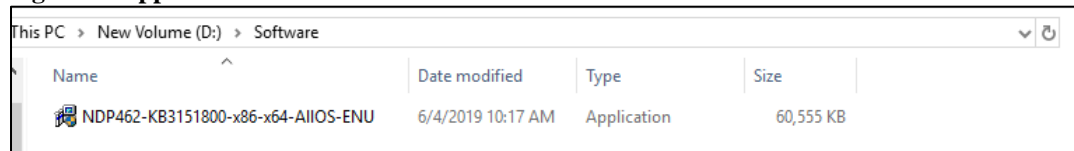
- b. Clicking Yes will bring you to the download page for .NET Framework 4.6.2, or click on the following [link](#) to access the offline installer.

Figure 7: Download Page for .NET Framework 4.6.2

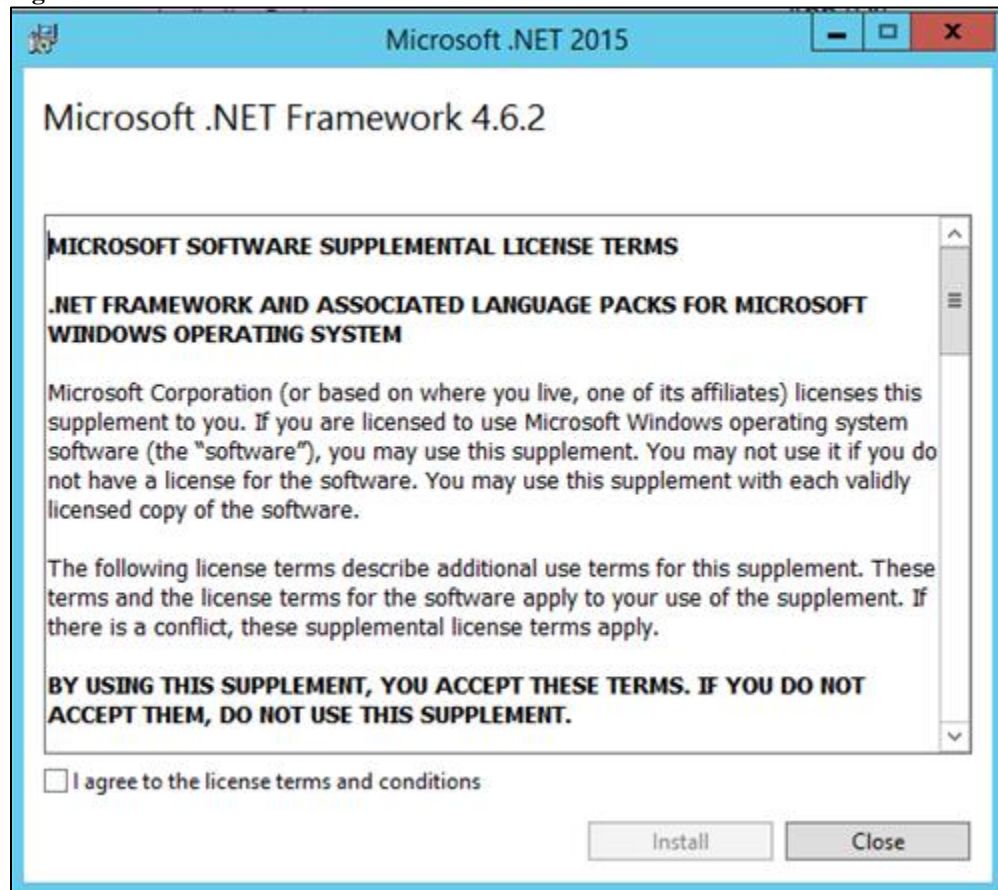
- c. Click the **DOWNLOAD** button to download the **.NET Framework 4.6.2 (NOT Developer Pack)** and save it to your hard drive.

Figure 8: .NET Framework 4.6.2 Download Message

- d. Find the application file and run it to begin the install.

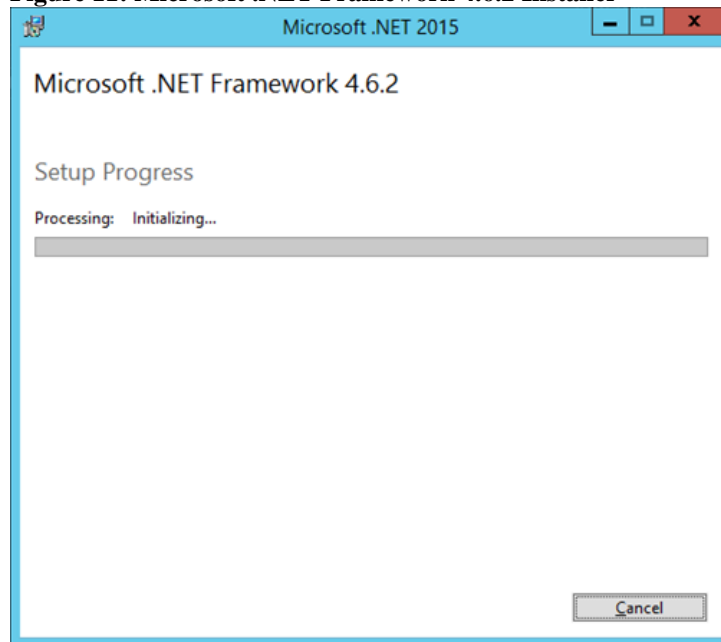
Figure 9: Application File

- e. Agree to the License terms and conditions and click Install.

Figure 10: Microsoft .NET Framework 4.6.2 License Terms

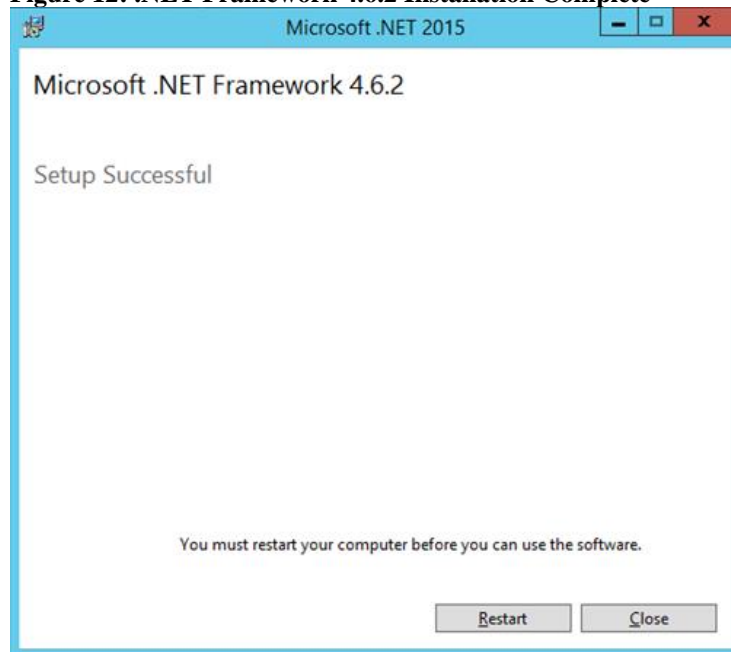
- f. The update will begin installation

Figure 11: Microsoft .NET Framework 4.6.2 Installer



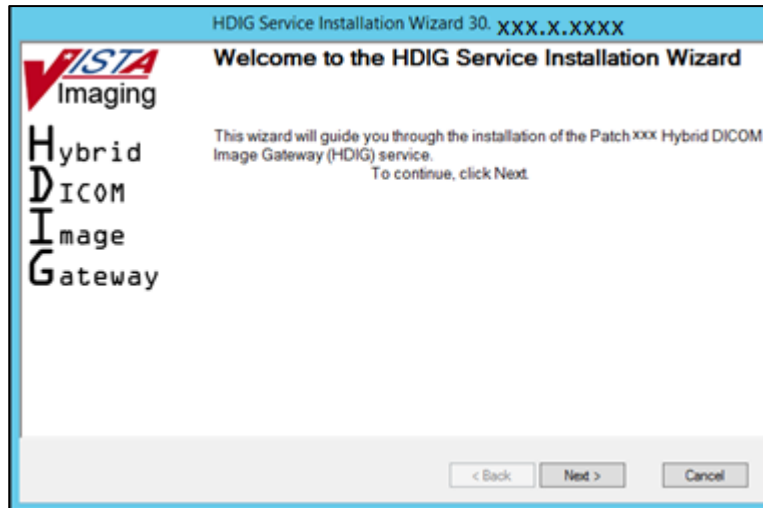
- g. Once installation is complete, you must click **Restart**

Figure 12: .NET Framework 4.6.2 Installation Complete



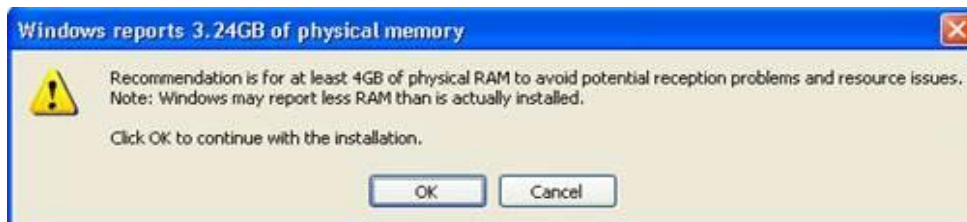
2. After successfully restarting, re-run the HDIG Service Installation Wizard. When the **Welcome to the HDIG Service Installation Wizard** dialog box displays, click Next.

Figure 13: HDIG Service Installation Wizard Welcome Page



3. If the installer detects that the Gateway server has less than 3.5 GBs of memory, the following dialog box appears.

Figure 14: Less than 3.5 GBs of Memory Detection Message



4. In the **Specify the VA site the HDIG will service** dialog box, enter the **Site Number** of the site where the HDIG service is installed, then click **Lookup Server Addresses**.

Figure 15: Specify the VA Site the HDIG Will Service Dialog Box

HDIG Service Installation Wizard 30. xxx.x.xxxx

Specify the VA site the HDIG will service.

Specify the VA site number for this HDIG then click the Lookup Server Addresses button.

Site Service URL:

Site Number:

VistA Server Name:

VistA Server Port:

< Back Next > Cancel

5. Verify that the information the lookup retrieved is correct, then click Next.
6. In the **Specify the DICOM Configuration** dialog box, enter the required information.
 - a. **DICOM Image Gateway properties** – The properties of the computer on which the DICOM Image Gateway resides:
 - **Server** – The name of the host on which the DICOM Gateway has been installed (the host on which you are installing the HDIG).
 - **Designated Port** – The number of the TCP port that the DICOM Gateway uses to communicate with the other VistA components. The port is 60001. You cannot modify this port.

Figure 16: Specifying the DICOM Image Gateway

Specify the DICOM Image Gateway

Server: Designated Port:

- b. **DICOM Image Gateway service account properties** – The properties of the service account the HDIG uses to access the VistA menu options. You can get the account properties from the VistA administrator at your site.
 - **Access** – The access code for accessing VistA

- **Verify** – The verify code for accessing VistA
- **Confirm Verify** – A field in which you type the verify code for accessing VistA again.

Figure 17: Specifying the DICOM Configuration

- c. DICOM Image Gateway services – The components (services) that the HDIG provides. You can enable all components on one computer. At least one component must be selected. By default, all components are selected. If you do not want to enable all components, clear the ones that you do not want to be enabled.
 - **DICOM Listener Enabled** – This checkbox must be selected, if you plan to activate the DICOM Listener, enable the Query/Retrieve application, or enable the DICOM Importer on this gateway.
 - **Archive Enabled** – This checkbox must be selected to activate the Archiver on this computer. Activating the Archiver enables archiving of the newly supported SOP classes for the site.
 - **Thumbnail Processing Enabled** – This checkbox must be selected to enable the new Abstract Maker on this gateway.

Figure 18: Configure Services Section of Figure 17

- d. **Send email notifications to:** – This field specifies the email address or addresses to which the HDIG sends notifications when the HDIG detects invalid service account credentials. You must enter at least one email address in the field. If you want to enter more than one address, use a comma to separate the addresses.

Figure 19: Send Email Notification to Section of Figure 17



Note: This email address does not configure the email address used for queuing email messages.

7. Click **Validate**. The 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.
8. Click **Next** to continue. When the **Install the HDIG Prerequisites** dialog box displays, review the list of required prerequisites.

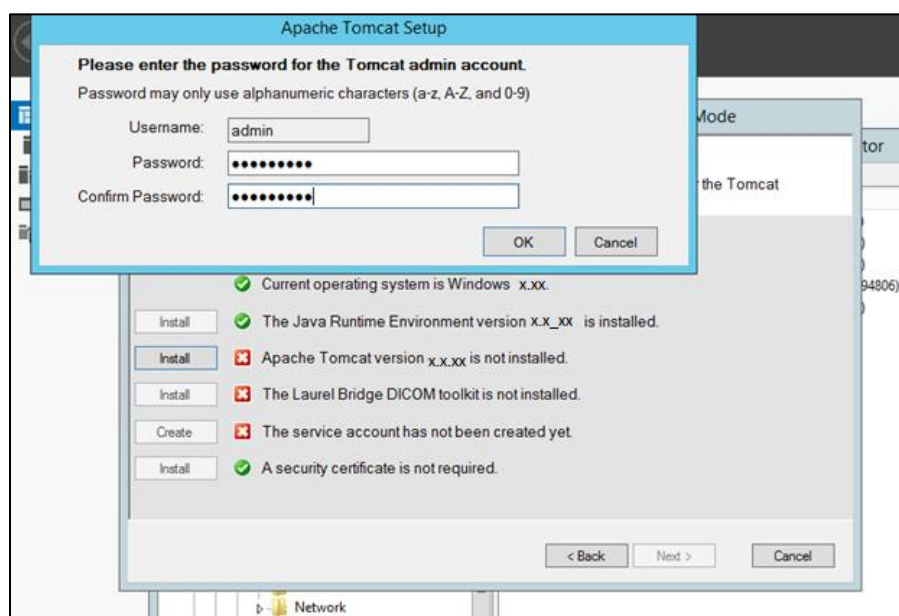
Figure 20: Required HDIG Prerequisites



For any items flagged with , see the following notes.

- a. **<account> has Administrator role** – This check verifies that an administrator account is being used. If not, cancel the installation and restart it using a Windows administrator account.
- b. **Current operating system is <OperatingSystem>** – This check verifies that the proper operating system is present. If a different operating system is used, the installation cannot continue.
- c. **The Java Runtime Environment <Version> is installed.** – Click Install if this component has not been installed already.
- d. **Apache Tomcat** – Click Install to create the Apache Tomcat administrator account. Provide the password defined in the Apache Tomcat Application Password section above. Type the password again in the Confirm Password field and click OK.

Figure 21: Apache Tomcat Setup



The Laurel Bridge DCF Toolkit

1. If you enabled the DICOM Listener and the Laurel Bridge DCF Toolkit is not installed, click **Install** next to The Laurel Bridge DCF Toolkit prerequisite. If the HDIG host can connect to the Internet, an Activate DCF License dialog box opens. The **Network Activation** tab in the dialog box is already selected and some fields are pre-populated.
2. Enter all of the following information in the **Network Activation** tab:
 - **Product Serial Number** – The new Laurel Bridge DCF toolkit serial number (include dashes).
 - **Site** – The name of your site.

- **Host** – The name of the Server.
- **Number of CPUs** – The number of CPUs on the server hosting the HDIG.
- **Contact name and Contact email** – The administrator of your local Vista Imaging system.

Figure 22: Activate DCF License Dialog Box

3. Click **Activate**. After a brief delay, the Status field will display a green **Success** message.

Figure 23: Status Field Success Message

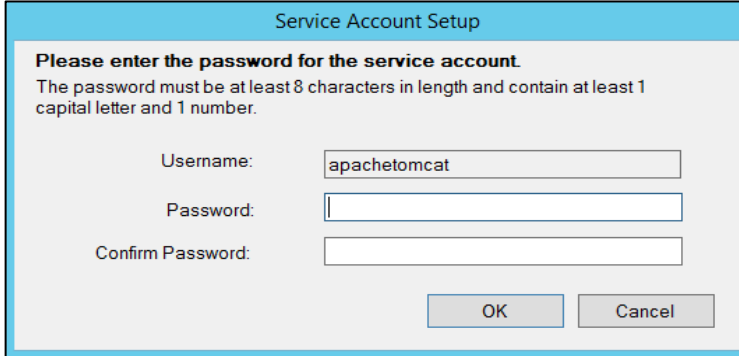
4. Click **Exit with success**. The Activate DCF License window will close and the updated Laurel Bridge toolkit will be installed (installation will only take a second or two).

Figure 24: Exit with Success Option

5. If the HDIG host *cannot* connect to the Internet and can access the Laurel Bridge Web site, activate the license manually, as instructed in Appendix A Manual Activation of the SUPPLY.
6. If you did not enable the DICOM Listener, the **Install** button is grayed out and the text next to it reads **The Laurel Bridge DCF toolkit is not required**.

7. If the required version of the Laurel Bridge DCF toolkit is installed, there is a green check mark next to the text **The Laurel Bridge DCF Toolkit is installed.**
8. **Service Account** – Click **Create** to create the HDIG service account. Provide the password if requested. Type the password again in the Confirm Password field and click **OK**

Figure 25: Service Account Setup Page



The image shows a 'Service Account Setup' dialog box. It has a title bar with the text 'Service Account Setup'. Inside, it says 'Please enter the password for the service account.' followed by a note: 'The password must be at least 8 characters in length and contain at least 1 capital letter and 1 number.' There are three input fields: 'Username:' with the text 'apachetomcat', 'Password:', and 'Confirm Password:'. At the bottom right are 'OK' and 'Cancel' buttons.


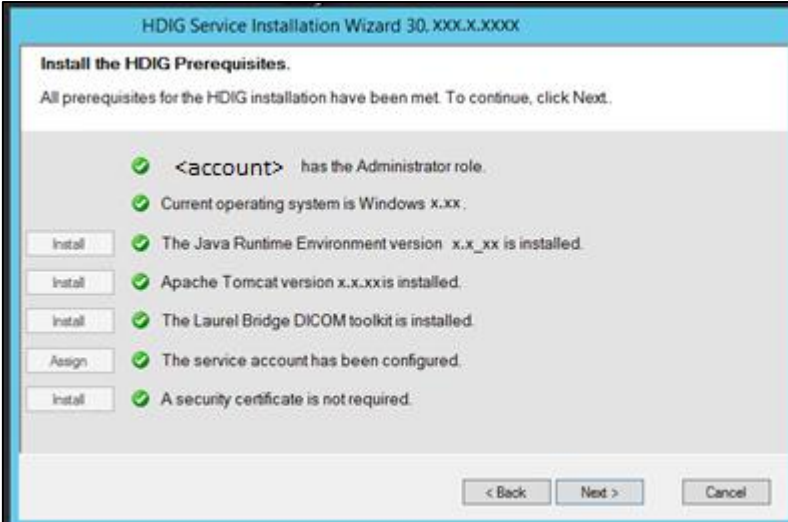
9. When all items in the Prerequisites dialog have an  icon next to them, click **Next**.

Figure 26: Completed Install the HDIG Prerequisites Page



The image shows the 'HDIG Service Installation Wizard' window, titled 'HDIG Service Installation Wizard 30, XXX.X.XXXX'. The main heading is 'Install the HDIG Prerequisites.' Below it, it says 'All prerequisites for the HDIG installation have been met. To continue, click Next.' There is a list of six prerequisites, each with a green checkmark icon and an 'Install' button to its left:

- <account> has the Administrator role.
- Current operating system is Windows x.xx.
- The Java Runtime Environment version x.x_xx is installed.
- Apache Tomcat version x.x.xx is installed.
- The Laurel Bridge DICOM toolkit is installed.
- The service account has been configured.
- A security certificate is not required.

 At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

Note: The HDIG installer was built using the same VISA foundation as the VIX, including the same installer program. There may be some references to the VIX directories even though an HDIG is being installed.

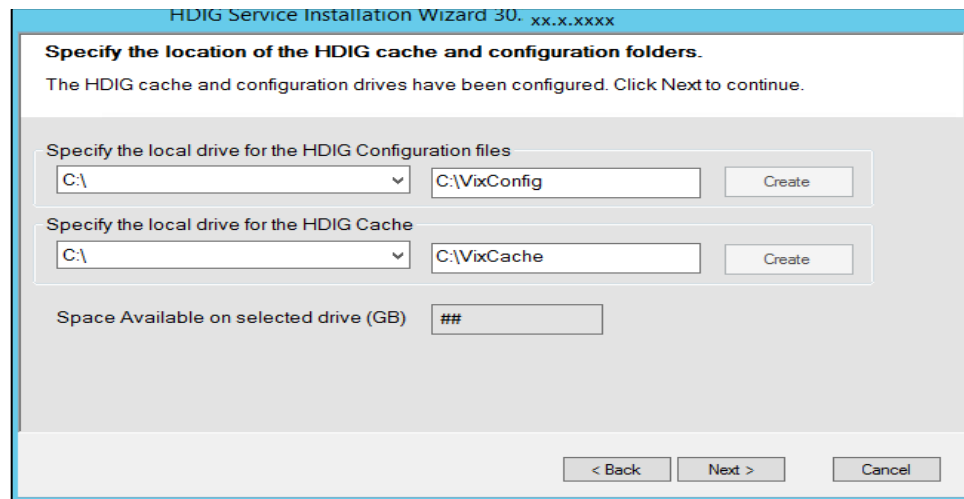
10. In the **Specify the location of the HDIG cache and configuration folders** dialog box, select the drive where you want the HDIG configuration files to reside, then click **Create**.

Note: The HDIG configuration files must be on the local system drive (the drive on which the operating system is installed, which is typically C:\).

11. Select the drive where the cache will be located, then click **Create**.

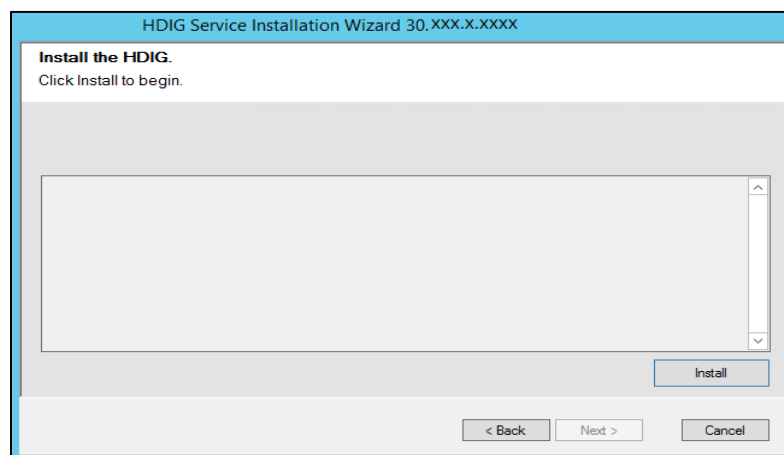
Tip: We recommend using a different physical drive for the HDIG cache, if the computer on which you are installing the HDIG has another physical drive.

Figure 27: Specify the Location of the HDIG Page



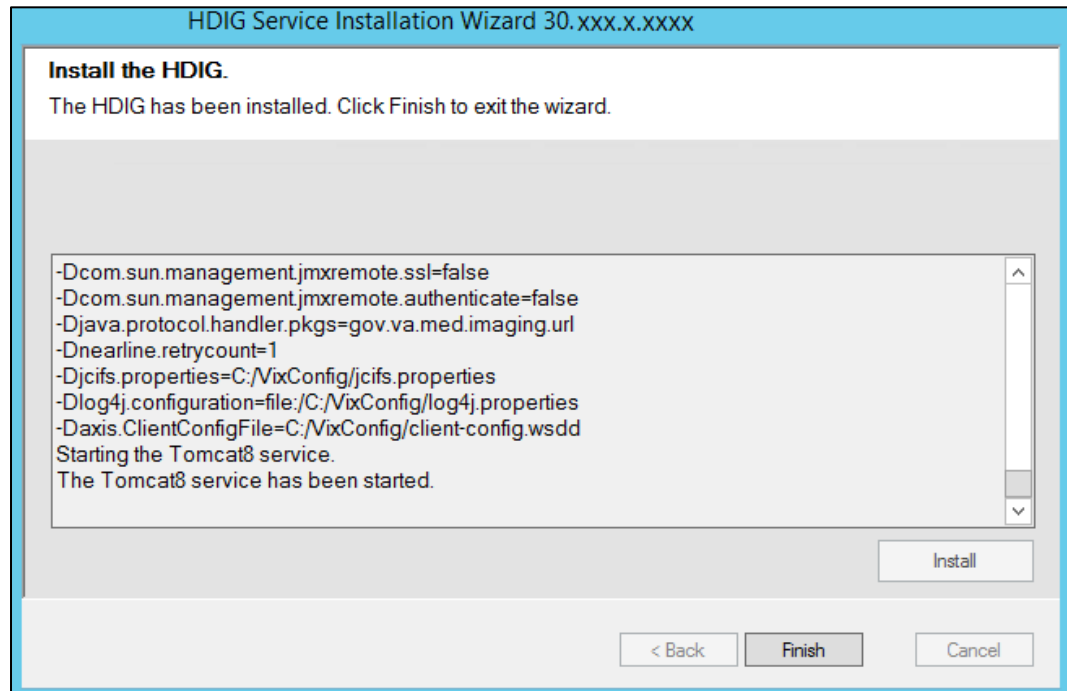
12. Click **Next**.
13. In the Install the HDIG dialog box, click **Install**.

Figure 28: Install the HDIG Page



14. When installation completes, click **Finish** to exit the wizard. The HDIG service starts automatically after it is installed.

Figure 29: HDIG Installation Complete



Updating an Existing HDIG

Preparing for an HDIG

.NET Version Update

Note: Use Windows Updater to install any security updates available for .NET 4.6.2 and above. If there are issues installing the .NET framework, please reach out to the Helpdesk or Clin3.

Note: More recent .NET updates can be installed but make sure that .NET 4.6.2 and above are included in the installation.

To verify your version of .NET:

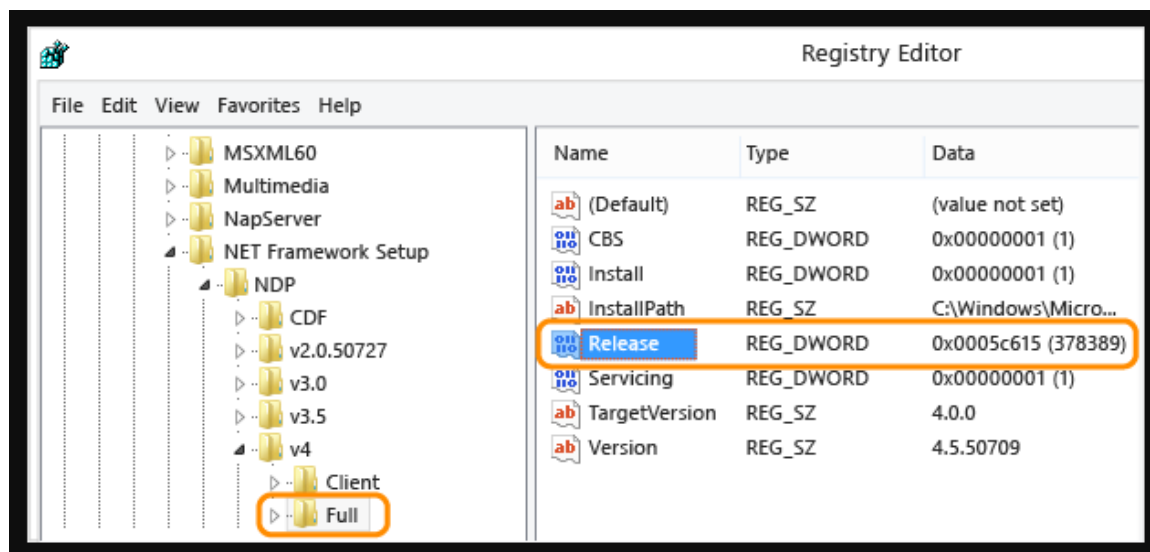
1. From the **Start** menu, choose **Run**, enter *regedit*, and then select **OK**.

Note: You must have administrative credentials to run regedit.

2. In the Registry Editor, open the following subkey: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full**. If the **Full** subkey isn't present, then you don't have the .NET Framework 4.5 or later installed.

Note: The **NET Framework Setup** folder in the registry does *not* begin with a period.

3. Check for a DWORD entry named **Release**. If it exists, then you have .NET Framework 4.5 or later versions installed. Its value is a release key that corresponds to a particular version of the .NET Framework. In the following figure, for example, the value of the **Release** entry is 378389, which is the release key for .NET Framework 4.5.

Figure 30: DWORD Release Entry Name Example**Figure 31: .NET Framework Release Keys**

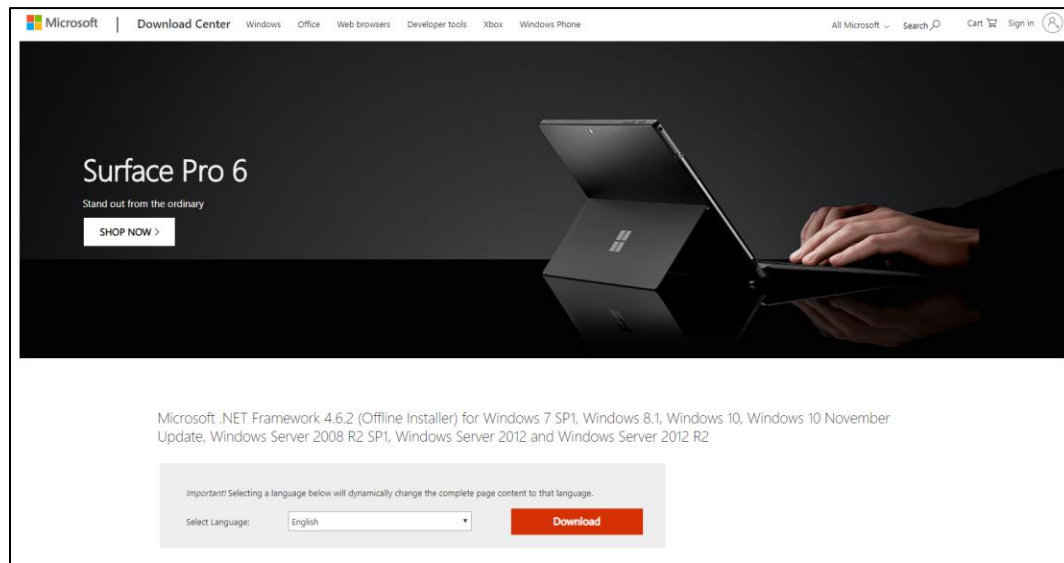
.NET Framework version	Value of the Release DWORD
.NET Framework 4.5	All Windows operating systems: 378389
.NET Framework 4.5.1	On Windows 8.1 and Windows Server 2012 R2: 378675 On all other Windows operating systems: 378758
.NET Framework 4.5.2	All Windows operating systems: 379893
.NET Framework 4.6	On Windows 10: 393295 On all other Windows operating systems: 393297
.NET Framework 4.6.1	On Windows 10 November Update systems: 394254 On all other Windows operating systems (including Windows 10): 394271
.NET Framework 4.6.2	On Windows 10 Anniversary Update and Windows Server 2016: 394802 On all other Windows operating systems (including other Windows 10 operating systems): 394806
.NET Framework 4.7	On Windows 10 Creators Update: 460798 On all other Windows operating systems (including other Windows 10 operating systems): 460805
.NET Framework 4.7.1	On Windows 10 Fall Creators Update and Windows Server, version 1709: 461308 On all other Windows operating systems (including other Windows 10 operating systems): 461310
.NET Framework 4.7.2	On Windows 10 April 2018 Update and Windows Server, version 1803: 461808 On all Windows operating systems other than Windows 10 April 2018 Update and Windows Server, version 1803: 461814
.NET Framework 4.8	On Windows 10 May 2019 Update: 528040 On all others Windows operating systems (including other Windows 10 operating systems): 528049

4. Check to make sure .NET 4.6.2 and above is installed installing the HDIG Installer.

If your .NET version is not 4.6.2 or later:

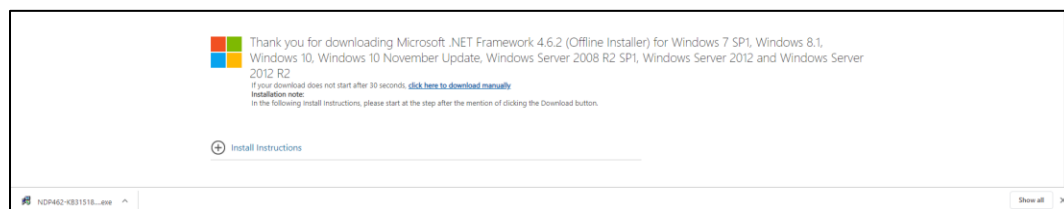
1. click on the following [link](#) to access the offline installer.

Figure 32: Download Page for .NET Framework 4.6.2



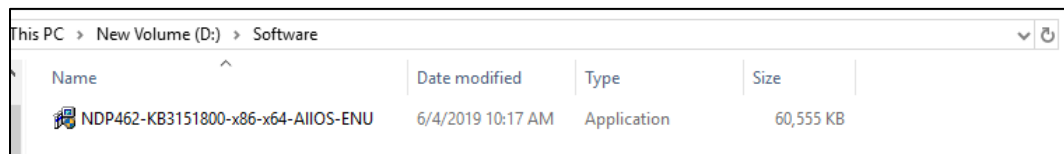
2. Click the **DOWNLOAD** button to download the **.NET Framework 4.6.2 (NOT Developer Pack)** and save to your hard drive

Figure 33: .NET Framework 4.6.2 Download Message



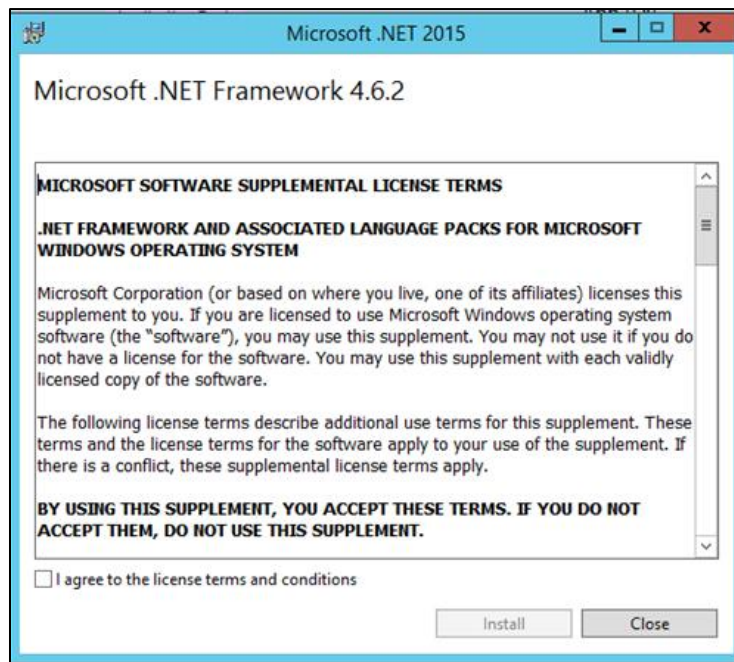
3. Find the application file and run it to begin the install

Figure 34: Application File



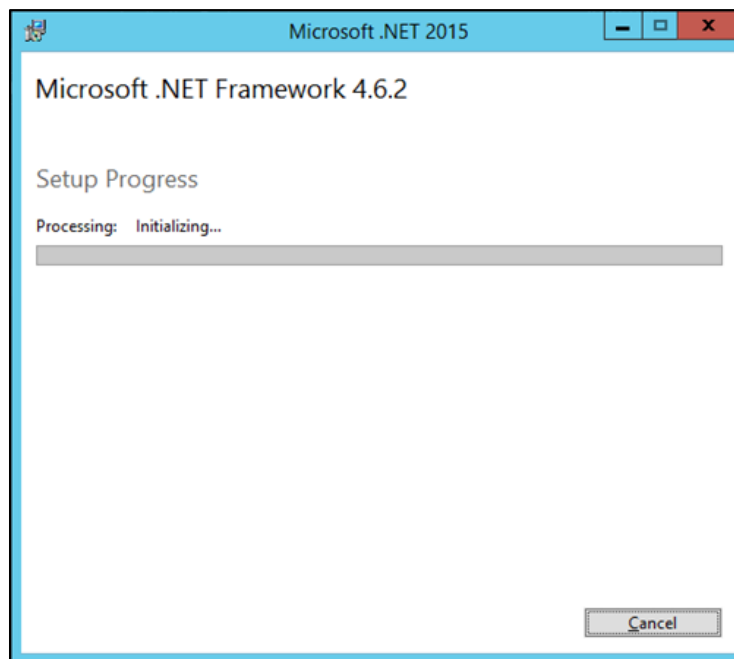
4. Agree to the License terms and conditions and click Install

Figure 35: Microsoft .NET Framework 4.6.2 License Terms



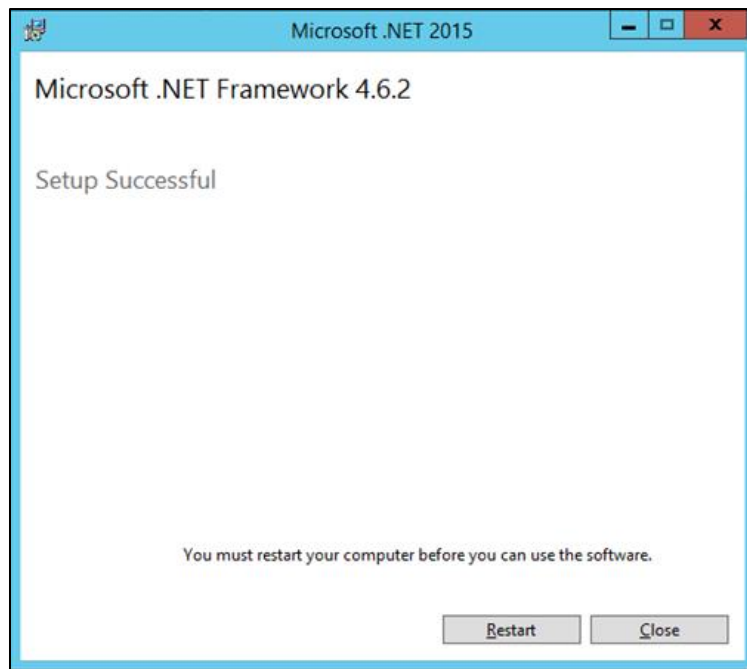
5. The update will begin installation

Figure 36: Microsoft .NET Framework 4.6.2 Installer



6. Once installation is complete, you must click **Restart**

Figure 37: .NET Framework 4.6.2 Installation Complete

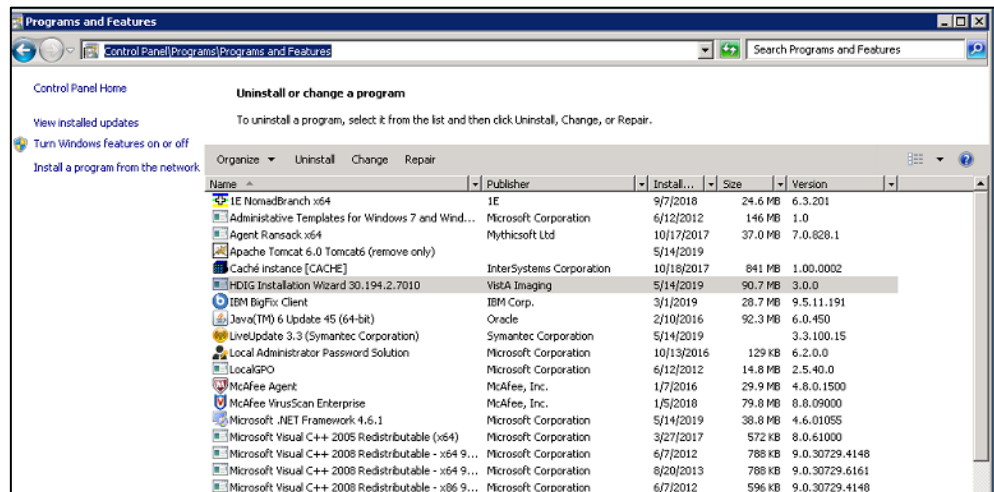


Java Version

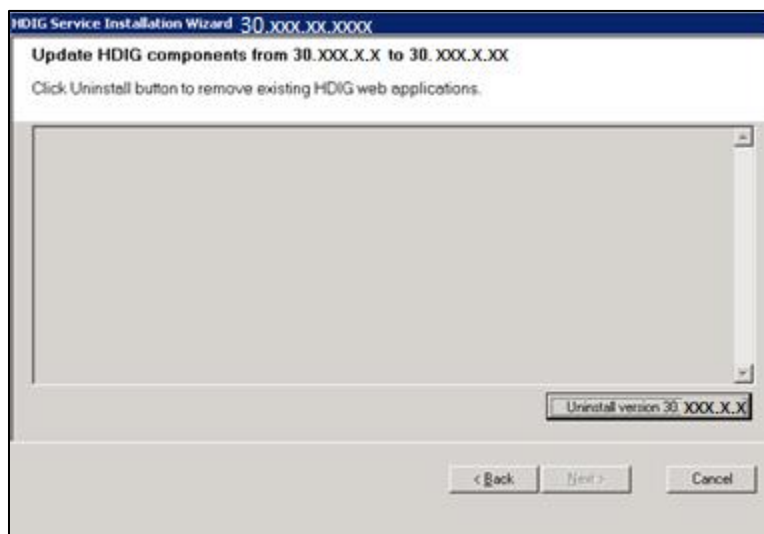
Validate the specific patch description document for the current version of Java. If the server has a different version of Java than the required version specified in patch description, the wizard will install/uninstall the Java version.

Updating the HDIG

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

Figure 38: Uninstall Programs in the Control Panel (Windows 2012 R2)

- 2 At the Update HDIG Components screen, click the **Uninstall version 30.XXX.X.X** button to remove the previous version of the HDIG.

Figure 39: Uninstall Confirmation

- 3 At the **Specify the VA site that the HDIG will service** screen, enter the **Site Number** of the site where the HDIG service is installed, then click **Lookup Server Addresses**.

Figure 40: Specify the VA Site the HDIG Will Service Dialog Box

- 4 Click **Next**. The DICOM Configuration screen opens.

Figure 41: Specifying the DICOM Configuration

- 5 Click **Next**. The Install the HDIG Prerequisites screen opens. Items with a green check are successfully installed. Items with a red X require installation. Click the **Install** button next to each one in order. This portion of the installation may

take 15-20 minutes. For more information on prerequisites, refer to the Running the HDIG Installer section above.

Note: After Installing Java and BEFORE Installing Apache:

In some cases, it was observed that old Apache entries were not removed from the Windows Registry Editor (regedit).

BEFORE PROCEEDING TO INSTALL THE NEWEST APACHE TOMCAT VERSION, please **RUN “regedit”** and **“RIGHT-CLICK + DELETE”** the entries for previous versions of Apache under the **HKEY_LOCAL_MACHINE > SOFTWARE > APACHE SOFTWARE FOUNDATION > TOMCAT** folder. For more information please contact the CLIN3 help desk.

Figure 42: Tomcat 6.0

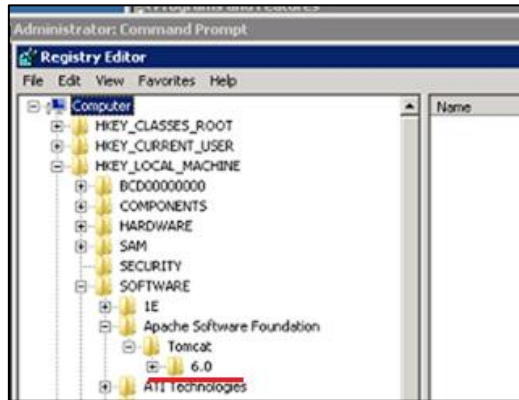


Figure 43: Required HDIG Prerequisites



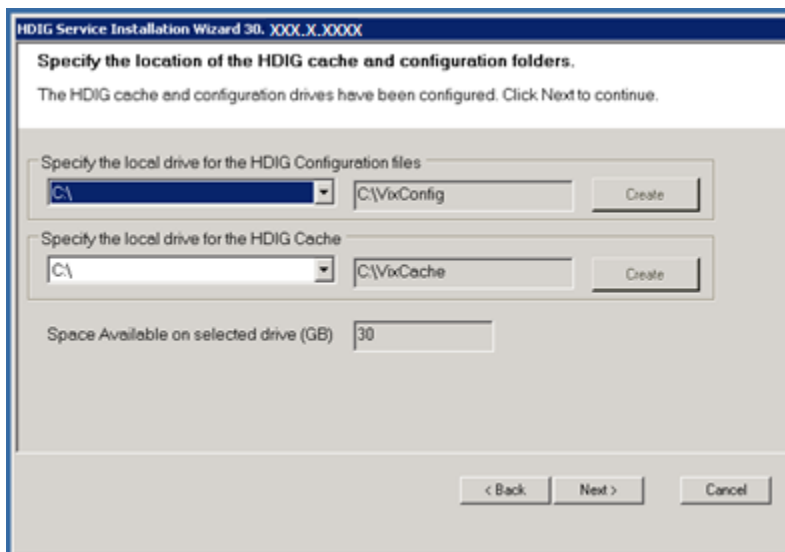
- 6 When all the prerequisite installations have completed, the **Next** button is enabled. Click **Next**.

Figure 44: Completed Install the HDIG Prerequisites Page



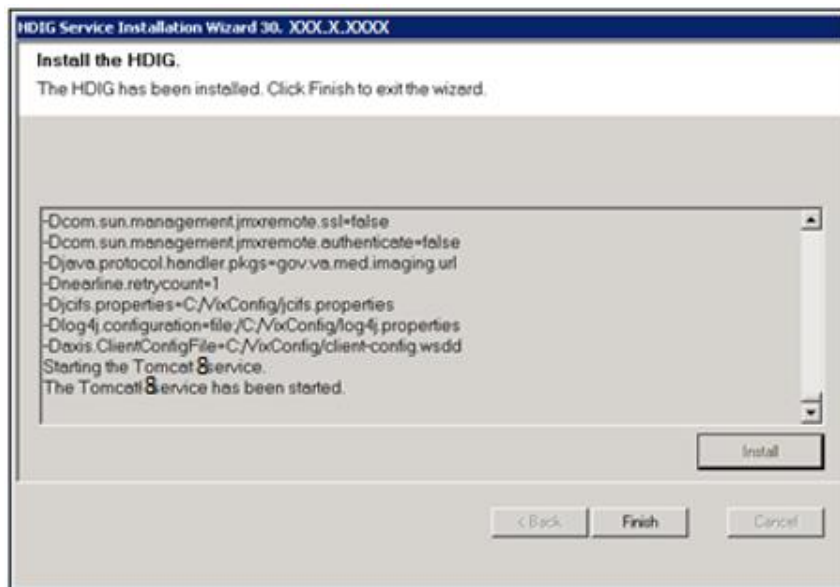
- 7 Specify the location of the HDIG cache and configuration folders. Click **Next**.

Figure 45: Specify the Location of the HDIG Page



- 8 The Install the HDIG screen opens. Click **Install**.

Figure 46: HDIG Installation Complete



HDIG Post-Installation

This section provides information about the additional steps you must perform after installing the software.

After installing the patches, you must perform these steps:

1. Verify antivirus scan exclusions for designated directories.
2. Verify the memory allocated to the HDIG. (For DICOM Gateways with RAM of 2 GB.)
3. Starting image processing on the legacy Image Gateways by running option 2-3.
4. Review the HDIG Stat Page for each image-processing server.
5. Review the HDIG Logs.
6. Check for emails from the server notification service.
7. If you plan to import studies from outside locations over the network, you must configure an Outside Location.

Configuring the HDIG

After installing the HDIG, there are several configuration steps required, to be followed by multiple steps to test and verify the HDIG is working properly.

Verify Antivirus Scanning Exclusions

Verify the following exclusions to the antivirus scanning application definitions:

C:\DICOM\VixCache

C:\DICOM\Image_In

C:\DICOM\Image_Out

Note: if the default drive of C was not used, change the designation of the drive where these directories reside.

The exclusions should also be applied on the root directory of each drive that hosts an image share. For example, G:\.

Increasing the Memory Allocated to the HDIG

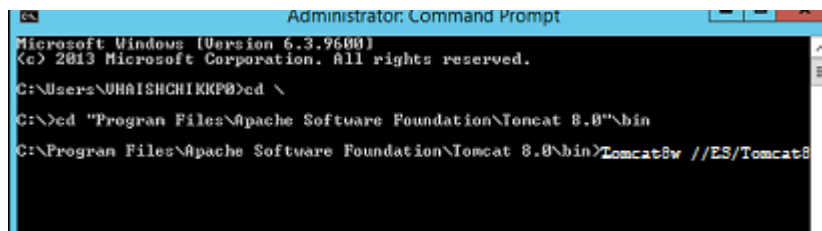
On DICOM Gateways with RAM of 2 GB or less, you must increase the memory allocated to the HDIG (Apache Tomcat 8) service, because the processing of some DICOM datasets (mostly of new SOP Classes or new modality devices) requires a lot of memory. Increasing the memory may have a slight impact on the HDIG performance, but it will reduce the risk of failure due to insufficient memory (not having enough Java Heap Space).

To Upgrade the Memory on the Tomcat Application Server:

1. Check the total memory allocated to the server by going to “Control Panel” > “System”.
2. Stop the Apache Tomcat server by selecting “Services”.

Name	Description	Status	Startup Type	Log
1E Client Health	Runs health...	Running	Automatic (D...	Loc
1E Nomad Branch	Nomad Bra...	Running	Automatic (D...	Loc
Apache Tomcat 8.0 Tomcat8	Apache To...	Running	Manual	.\ap
App Readiness	Gets apps re...		Manual	Loc
Application Experience	Processes a...	Running	Automatic (T...	Loc

3. Open the command prompt “as Administrator”.
4. If Tomcat’s version is 8.0, execute the following steps:
 - a) Run the following command within the command prompt window



```

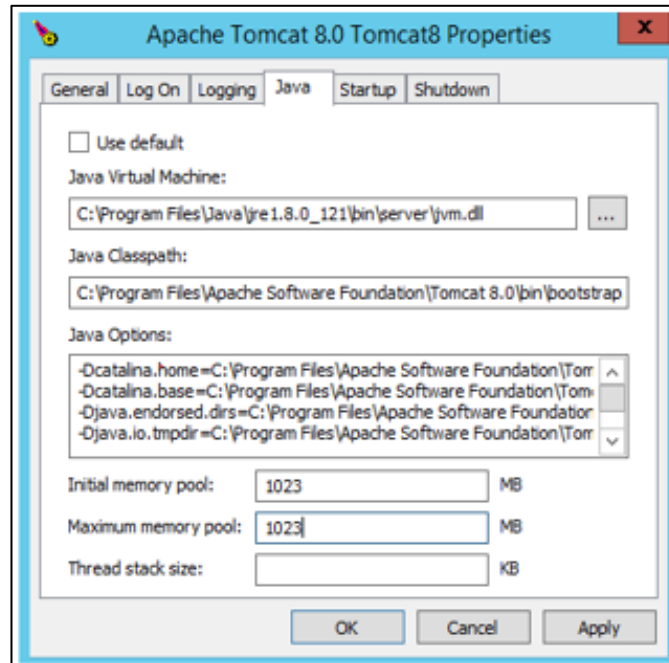
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\UHAISHCHIKKP>cd \
C:\>cd "Program Files\Apache Software Foundation\Tomcat 8.0\bin"
C:\Program Files\Apache Software Foundation\Tomcat 8.0\bin>Tomcat8w //ES/Tomcat8
  
```

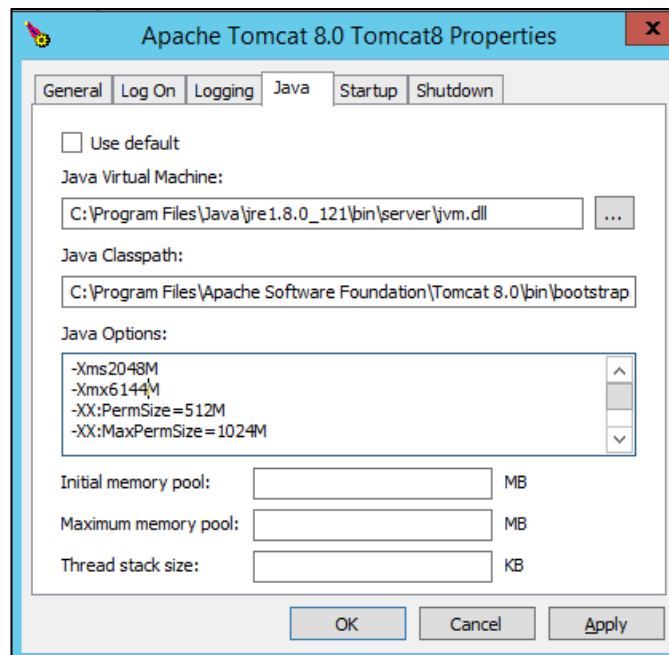
Tomcat8w //ES/Tomcat8

- b) Once the popup has opened, click on “Java”
- c) If the total memory or RAM on the server is 8GB, please add the following parameters under the existing parameters in the popup window (Maximum size allowed for a transfer file has been tested at 750MB).

From:



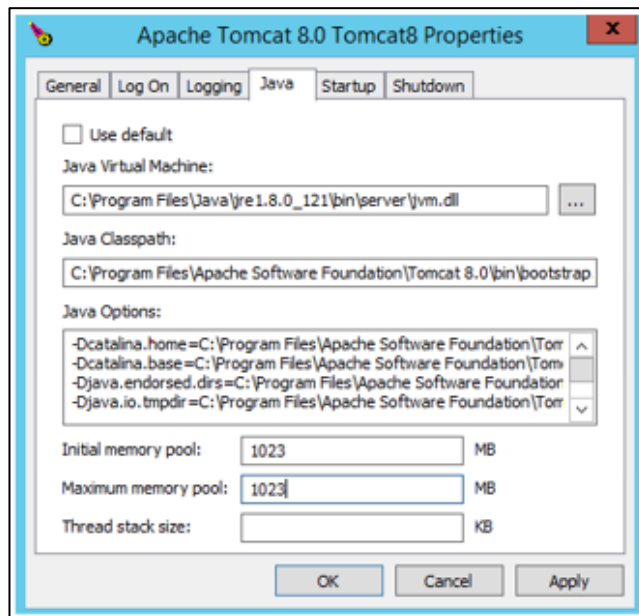
To:



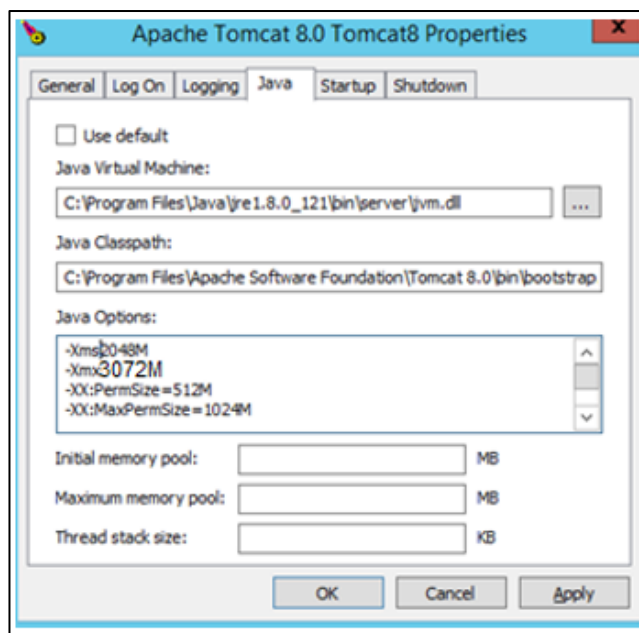
-Xms2048M
 -Xmx6144M
 -XX:PermSize=512M
 -XX:MaxPermSize=1024M

- d) If the total memory or RAM on the server is 4GB, add the following parameters under existing parameters within the popup window (Maximum size allowed for a transfer file has been tested at 500MB).

From:



To:



-Xms2048M
 -Xmx3072M
 -XX:PermSize=512M
 -XX:MaxPermSize=1024M

- e) Click **Apply** and **OK**.
- f) Start the Apache Tomcat server

Email Notifications

There are two types of email notifications sent by the HDIG: ERROR email notifications and WARNING email notifications. The HDIG handles the two notifications differently.

Error Messages and Email Handling

The system has a pre-configured time period for checking to see if there are any error messages to be sent (The system default is 60 seconds.). At the end of the specified time period, if there are any error messages to be sent, they are bundled and sent as one email.

Warning Message Bundling for Email Handling

There are two thresholds that are checked when determining when to send a warning email bundle. These two thresholds are email count and email bundle size. Whichever of the two conditions are satisfied first, triggers the sending of an email.

The email count threshold has a system default of 100. Warning messages are bundled into groups of 100 email messages. Each time the configured threshold is met, an email is sent to the email address configured in the legacy gateway with all of the warnings.

A second threshold, the email bundle size is also checked. The system default is that the email bundle should not exceed 5MB in size. If there are large warning email messages and this 5MB threshold is reached before the email bundle reaches the email count threshold, the email bundle will be sent.

Warning Email Handling Configuration Guidelines

The proper settings will make sure, that generated emails are not too frequent for the recipient(s) and not too large for the mail server in use. The recommendation is that you use the system defined defaults. However, you can adjust the default settings by editing

the NotificationEmailConfiguration.config XML file in the C:\VixConfig folder. (For assistance editing this XML file, please request assistance from the CLIN 3 team.) Guidelines for settings and behavior:

- If you want more warning messages bundled (less frequent emails), set xxx higher (default is 100).

- If your email server cannot handle 5MB emails, lower it to the accepted value (example; 1MB is $1 \times 1024 \times 1024 = 1048576$). Lowering the bundle size will result in more frequent emails.

Configure the HDIG for Each Image Processing Server

Verify the HDIG Service Account Credentials

- 1 Access the HDIG Stats Page; `http://<HDIG Hostname.Domain>:8080/HDIGManagementWebApp/ViewHDIGStats.jsp`
Note: URLs are case sensitive

For first time installs, the screen will appear as follows:

- 2 Click Update the HDIG service account credentials.



- 3 Enter the Access Code of the DICOM Gateway Service Account.
- 4 Enter the Verify Code of the DICOM Gateway Service Account.



After the credentials have been validated, the page will appear as follows:

Basic Information

[Access Java Logs Viewer](#)
[Update the HDIG service account credentials](#)
[Update the Administrator email address\(es\)](#)

Hostname:	vhaiswingvms711
Site Number:	660
Site Name:	SALT LAKE CITY
Version:	xx.xxx.xx.xxxx
JVM Start Time:	Jul 24, 2013 10:46:06 AM
JVM Up Time:	1 hours, 21 minutes, 53 seconds

Updating the HDIG Administrator Email Address(es)

- 1 Review the HDIG email address used to alert for invalid service account credentials by clicking on **Update the Administrator email address(es)** update if needed.
Note: You must enter at least one email address in the field. If you want to enter more than one address, use a comma to separate the addresses.
- 2 Verify the email address(es) by performing the following steps.
- 3 Use **CTRL^C** to copy the email address from the HDIG page.
- 4 Open your email client and initiate a new email.
- 5 Use **CTRL^V** to paste the email address into the TO box of the email message.
- 6 Type MAG*3.0*xxx Install Test email in the subject line.
- 7 Send the email.
- 8 Check your email inbox to verify you received the email.

Save the HDIG Stat Page as the Home page

- 1 Set the View HDIG Statistics page as the Windows Internet Explorer Home page.
- 2 Click **Tools**, then **Internet Options**.
- 3 Under the Home page section, choose **Use current**, click **Apply** and then **OK**.

Save the HDIG Logs Page as a favorite

- 1 Access the HDIG Logs page; <https://<HDIG Hostname.Domain>/Vix/ssl/JavaLogs.jsp> **Note:** The HDIG logs are secured, to open the logs page enter the access and verify codes of a Vista account that holds the security key MAG VIX ADMIN.
- 2 Click **Favorites**, then **Add to Favorites**.
- 3 Name as <server name> HDIG Logs, click **Add**.

Testing the HDIG Operation

Review the HDIG Stats Page for Each Image Gateway Server

- 1 If not opened already, access the HDIG Stats Home page or <http://<HDIG Hostname.Domain>:8080/HDIGManagementWebApp/ViewHDIGStats.jsp>.
- 2 Check for proper values in the Basic Information fields Hostname, Site Number, Site Name and Version <30.136.35.3>.
- 3 Review the Inbound Activity section of the HDIG Stats Page to ensure all instruments on each specific gateway are listening on the proper ports as indicated in the INSTRUMENT.DIC file.

Inbound Activity	
DICOM Listening Ports:	
Port Number:	60177
Status:	LISTENING
Listening Since:	20130115
Port Number:	60196
Status:	LISTENING
Listening Since:	20130115

Starting image processing on the legacy Image Gateways by running option 2-3 **Process DICOM Images**.

Test and Review HDIG and Legacy Image Processing

Begin a limited transmission of images to one or more image gateway servers.

- 1 If not opened already, access the HDIG Stats Home page or <http://<HDIG Hostname.Domain>:8080/HDIGManagementWebApp/ViewHDIGStats.jsp>.
- 2 Review the section Inbound Associations for processed and rejected data by AE_ Title.

Inbound Associations:

AE Title:	IU22-2
IP Address:	10.XXX.XX.XX
Total Accepted Associations:	42
Total Rejected Associations:	0
Last Access Timestamp:	20130116

- 3 Review the section Inbound DIMSE Messages for processed and rejected data by AE_Title.

Inbound Dimse Messages:

AE Title:	IU22-2
Dimse Service:	C-Store
Total Dimse Messages Processed:	706
Total Dimse Messages Rejected:	0

- 4 Review the section Inbound Objects for processed and rejected data by AE Title.

Inbound Objects:

AE Title:	IU22-2
Total Objects Processed:	706
Total Objects Rejected:	0
Total Objects Passed to Legacy Gateway:	706
Total Objects Passed to HDIG Data Structure:	0
Total Duplicate Objects (RESENDS):	0

- 5 Review the section Inbound Modality Devices for processed and rejected data, duplicate objects, and IOD violations, by modality.

Inbound Modality Devices:

Manufacturer:	Philips Medical Systems
Model:	iU22
Total Objects Processed:	706
Total Objects Rejected:	0
Total Duplicate Objects (RESENDS):	0
Total Objects with a Duplicate Instance UID:	0
Total Objects with IOD Violations:	0

- 6 Review the legacy telnet window running the option 2-3 **Process DICOM Images**
- 7 If not opened already, access the HDIG Logs page; <https://<HDIG Hostname>/Vix/ssl/JavaLogs.jsp> Note - the HDIG logs are secured, to open the logs page enter the access and verify codes of a Vista account that holds the security key
MAG VIX ADMIN.
- 8 Open and review the HDIGSummary.log for each image processing server to ensure there are not AE_Title's incorrectly configured (or missing) in the DICOM AE SECURITY MATRIX.
Example entries indicating configuration problems:
 - a The Remote AE_Title, EYE6, does not have permission to access Vista Imaging. This permission is configurable using DICOM AE SECURITY MATRIX.
 - b The calling AE_Title, OTECH_QR, does not have permission to perform a CStore DIMSE Service. This permission is configurable using DICOM AE SECURITY MATRIX.
- 9 Open and review the ImagingExchangeWebApp.log for ERROR messages.
- 10 Open and review the VistaRealm.log for domain and log-on errors.
- 11 Check other notification services, specifically the email notification account designated as the mail group in the legacy Gateway Configuration Parameters.

Post-Installation

Complete Appendix D – Post-Install Checklist

- 1 Print *Appendix D, Post-Install Checklist*.
- 2 Complete the checklists.
- 3 Document any issues or problems encountered for future installs/upgrades.
- 4 File.

Appendix A Activating the DCF Toolkit Product Serial Number

Product Serial Numbers are required for each DCF toolkit installed at your site. Each product serial number is issued for a specific computer. You must activate each product serial number on each computer for the DICOM Listener instance to work on that computer.

You activate the product serial number when you run the HDIG installer. You activate the product serial number through the Laurel Bridge Web site. There are two types of activation depending on whether the computer can access the Laurel Bridge Web site directly through the Internet or not.

- **Network activation** – If the computer can connect to the Internet, you can activate the license using your network connection to the Internet.
- **Manual activation** – If the computer is not on a network that connects to the Internet, you must activate the license manually.

Network Activation

If the computer on which you are running the installer is connected to the Internet and can access the Laurel Bridge Web site, you activate the DCF toolkit product serial number (license) automatically through the network.

To activate the DCF Toolkit license through the network:

- 1 In the Requirements page of the HDIG installer, click **Install** next to the Laurel Bridge DCF Toolkit requirement to display the Activate DCF License dialog box.
(Skip this step if the dialog box is displayed.)

The screenshot shows the 'Activate DCF License' dialog box. It has a title bar with 'Activate DCF License' and a 'Help' button. Below the title bar are two tabs: 'Network Activation' and 'Manual Activation'. The 'Network Activation' tab is selected. It contains the following fields and controls:

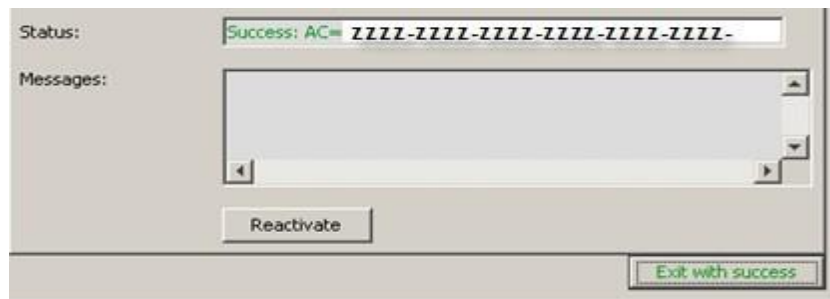
- Platform: Windows_NT_4_x86_VisualStudio8.x
- DCF Version: 3.3.22c
- Product Serial Number: (empty field) Ex: 1111-2222-3333-4444
- Activation Request Code: XXXX-XXXX-XXXX-XXXX
- MAC Address (optional): (empty field)
- Site: (empty field)
- Host: <LocalHost>
- Number of CPUs: (empty field)
- Contact name: (empty field)
- Contact e-mail: (empty field)
- Status: (empty field)
- Messages: (empty text area)
- Buttons: 'Activate' and 'Exit with error'.

- 2 Enter the following information in the **Network Activation** tab of the Activate DCF License dialog box:
 - a **<account> has Administrator role** – This check verifies that an administrator account is being used. If not, cancel the installation and restart it using a Windows administrator account.
 - b **Product Serial Number** – The serial number of the DCF toolkit. c **Site** – The name of your site. d **Host** – The name of the computer on which you are installing the DCF toolkit.
 - e **Number of CPUs** – The number of CPUs on the computer on which you are installing the DCF toolkit. f **Contact name** – Your name.
 - g **Contact e-mail** – Your e-mail address.

The screenshot shows the 'Activate DCF License' dialog box with the 'Network Activation' tab selected. The 'Main' tab is also visible. The 'Platform' is set to 'Windows_NT_4_x86_VisualStudio8.x' and the 'DCF Version' is '3.3.22c'. The 'Product Serial Number' is 'XXXX-XXXX-XXXX-' and the 'Activation Request Code' is 'YYYY-YYYY-YYYY-YYYY'. The 'MAC Address (optional)' field is empty. The 'Site' is 'Site Name', 'Host' is 'localhost', 'Number of CPUs' is '1', 'Contact name' is 'Joe Smith', and 'Contact e-mail' is 'joe.smith@va.gov'. The 'Status' field is empty, and the 'Messages' field is empty. The 'Activate' button is at the bottom, and the 'Exit with error' button is at the bottom right.

3. Click **Activate**.
4. The **Status** field displays a message about the status of the request.
5. If there are errors and the request does not go through, the **Messages** field provides more details about the error.

6. If the request is successful, the **Status** field displays the message **Success** and the activation code.
7. If the request is successful, click the button **Exit with success**.



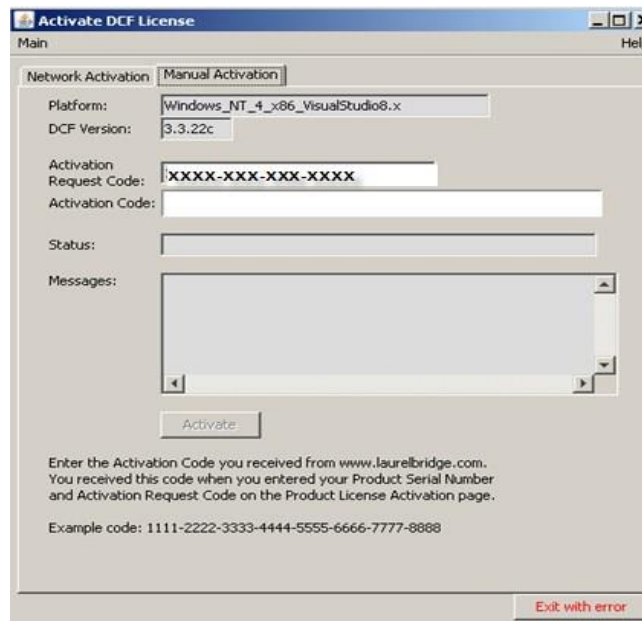
Manual Activation

If the computer on which you are running the HDIG installer is not connected to the Internet, you must activate the DCF toolkit product serial number (license) manually.

To activate the DCF Toolkit license manually:

- 1 In the Requirements page of the HDIG installer, click **Install** next to **the** Laurel Bridge DCF Toolkit requirement to display the Activate DCF License dialog box. (Skip this step if the dialog box is displayed.)

- 2 Click the **Manual Activation** tab.



1. Copy the activation request code displayed in the **Activation Request Code** field.

2. E-mail the activation request code to VHAVILBLicenses@va.gov, the VA License coordinator.
 3. The VA License coordinator will then activate the product serial number through the Laurel Bridge Web site and e-mail you the activation code.
 4. Copy the activation code from the e-mail message and paste it in the **Activation Code** field.
 7. Click the **Activate** button.
 8. The Status field indicates that the activation was successful.
- Click the **Exit with success** button.

Appendix B The DICOM AE Security Matrix

The DICOM AE SECURITY MATRIX file (#2006.9192) includes the configuration settings of all remote devices that use DICOM services to connect to the VistA system. This includes devices that can send data to the VistA system, devices that can query the data stored in the VistA system, and devices that can retrieve images from the VistA system. The remote devices support these DICOM services. The DICOM services at each local site are identified with unique 16-character strings called Application Entities (AE).

A remote device can have more than one DICOM service. For example, when a remote device stores images in VistA, the service associated with it is the storage service class (C-STORE). If the same device queries VistA, it uses the query service class (C-FIND). The device has a DICOM role associated with each service class. For example, a remote device that sends data to VistA is a service class user (SCU) of the storage service class (C-STORE). VistA is a service class provider (SCP) of the storage service class (C-STORE). There can be devices at different locations with the same AE title, service, and role. However, the combination of the remote AE Title, the service, role and site (location) number defines a device uniquely. AE Titles, per the DICOM Standard are a maximum of 16-character, unique alphanumeric strings per Application Entity. The DICOM AE SECURITY MATRIX and HDIG implementation for AE titles is not case sensitive.

MAG*3.0*79 introduced changes to the AE Security Matrix, which allows remote SCUs to issue Storage Commitment requests and also provide the information that the local SCP needs to return the response to the requesting SCU.

After installing the patch software, you must add an entry to the DICOM AE SECURITY MATRIX with the appropriate DICOM services and roles for each device at your site from which you want the DICOM Listener to receive data. If a device is not defined in the DICOM AE SECURITY MATRIX, it will not be able to send images or other data to the DICOM Listener and the data from the device will not be stored in the VistA system.

If you are using the Query/Retrieve application, you must also define all remote devices that can query and retrieve data from the VistA system in the DICOM AE SECURITY MATRIX.

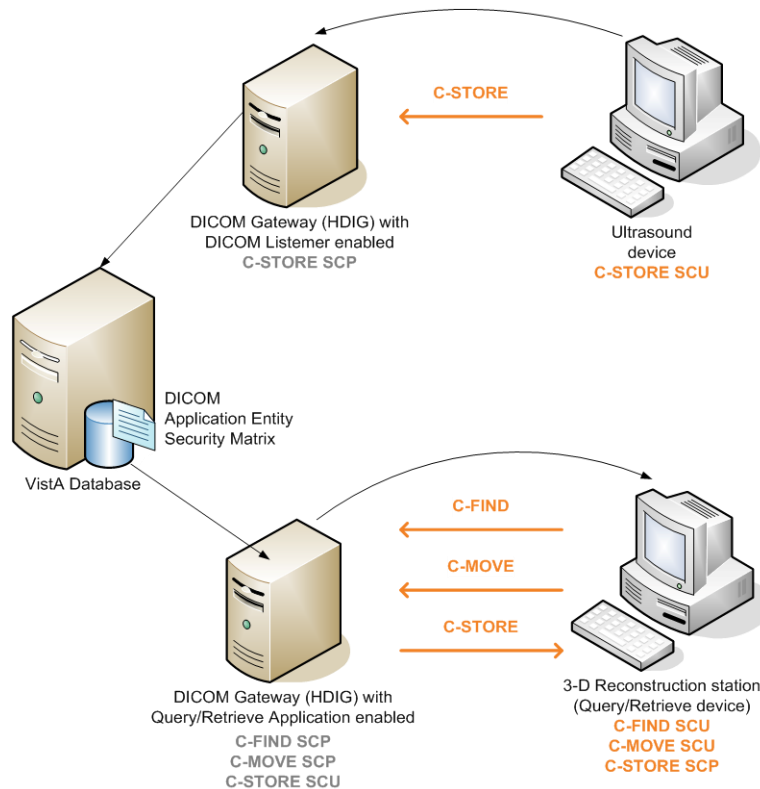
The following figure illustrates the logical relationships of the DICOM services and roles. The image shows two devices that are configured to connect to the VistA system through the DICOM Gateways (Hybrid DICOM Image Gateways).

- An ultrasound device sending DICOM objects to the VistA system. The device is configured as a Service Class User of the C-STORE service (C-STORE SCU), which can send images to the DICOM Gateway (which is the C-STORE SCP for this device). The DICOM Listener on the DICOM Gateway is enabled.

The DICOM Listener listens on a specific port for incoming DICOM objects from the ultrasound device, it processes the images and sends them to the VistA system. The DICOM Gateway is the Service Class Provider of the C-STORE service (C-STORE SCP).

- A 3-D reconstruction station is configured to query the VistA system through the Query/Retrieve application on the DICOM Gateway. The Query/Retrieve application is installed on the DICOM Gateway together with the DICOM Listener (which is a component of the HDIG). The 3-D reconstruction station is configured as a Service Class User of the C-FIND and the C-MOVE services (C-FIND SCU and C-MOVE SCU). The DICOM Gateway acts as the Service Class Provider of these services (CFIND SCP and C-MOVE SCP). Because the retrieved images are stored on the local disk, the 3-D reconstruction station is also defined as a Service Class Provider of the C-STORE service (C-STORE SCP). The DICOM Gateway acts as the Service Class User of the C-STORE service (C-STORE SCU).

Note: Only the remote devices (the ultrasound device and the 3-D reconstruction station) are defined as entries in the DICOM AE SECURITY MATRIX. The local AE titles (the DICOM Listener and the Query/Retrieve application) are not separate entries in the DICOM AE SECURITY MATRIX, but part of the remote entry for each DICOM AE definition.



DICOM Services and Roles

The DICOM AE SECURITY MATRIX contains an entry for importing studies from media using the DICOM Importer. If you plan to import studies from remote locations using a network connection or network drive, you must configure additional entries.

Overview - Configuring the DICOM AE Security Matrix

Entries for Storage Functionality

You must add an entry for each device at your site from which you want the DICOM Listener to receive data. If a device is not defined in the DICOM AE SECURITY MATRIX, it will not be able to send images or other data to the HDIG and the data from the device will not be stored in the VistA system. Each device is a service class user (SCU) of the Storage service class (C-STORE). The DICOM Listener (which runs on the DICOM Gateway), is a service class provider (SCP) of the Storage service class (C-STORE).

Entries for Query/Retrieve Functionality

If you are using the Query/Retrieve application, you must also configure the remote devices that can query and retrieve images from the VistA database. The configuration of the devices that use Query/Retrieve to get information from VistA Imaging database is stored in the DICOM AE SECURITY MATRIX

- Each device is a service class user (SCU) of the C-MOVE and of the C-FIND service classes. The Query/Retrieve application (which runs on the DICOM Gateway) is the service class provider (SCP) of the C-MOVE and of the C-FIND service classes.
- Each device that stores the images it retrieves from the VistA database is also a service class provider (SCP) of the Storage service class (C-STORE). The Query/Retrieve application (which runs on the DICOM Gateway) is the service class user (SCU) of the storage service class (C-STORE). Thus, you must define each device that would store the retrieved images as a C-STORE SCP. The same device that is defined as a C-FIND SCU and a C-MOVE SCU, can also be defined as a C-STORE SCP, if the device stores the images it retrieves in a local directory.

Entries for Import Functionality - Media

When the MAG*3.0*118 KIDS package is installed, a default entry is added to the DICOM AE SECURITY MATRIX file (#2006.9192). The entry has a REMOTE AE TITLE (field 1.1) called IMPORTER that is defined as a Service Class User of the C-STORE Service (C-STORE SCU). This entry allows the DICOM Importer to import data from media such as CDs, DVDs, thumb drives

and the like. If you are importing studies from media (such as DVDs, CDs, thumb drives) and you are *not* importing studies over the network from an outside location, you can use the entry that has already been defined. You do not have to define additional entries.

Entries for Import Functionality – Network Import

If you are importing studies data over the network from an outside location, you must define additional entries. You should have an entry for every community-based outpatient clinic (CBOC) that sends studies to your VistA system over the network. If your site gets studies from multiple origins, you can define separate entries for each origin, such as VA, DoD, or commercial-based clinics or use the same entry for studies imported from multiple origins. The DICOM AE SECURITY MATRIX has a field called ORIGIN INDEX whose value indicates the origin of the study. If you choose not to define individual entries for every origin, you can set the value of this field to the most common origin and edit it later.

The DICOM AE SECURITY MATRIX file (#2006.9192) has a field called FORCE RECONCILIATION field(# 1.3). The value indicates whether the imported images are queued in the DICOM Importer queue for reconciliation or not. For devices that send studies through the network from an outside location, such as an ultrasound device in a Community-Based Outpatient Clinic (CBOC), set the value to YES. The images will be queued in the DICOM Importer queue to be reconciled manually. In all other cases, use the default value – **NO**.

Fields in the DICOM AE SECURITY MATRIX

The DICOM AE SECURITY MATRIX file (#2006.9192) includes a listing of all the AE titles that are configured for the site and their configuration parameters. The following table provides information about the fields.

Fields in the DICOM AE SECURITY MATRIX file (#2006.9192)

Field	Description	Possible Values
AE NAME (#2006.9192, .01)	The name of the device. This is a unique descriptive name that allows you to identify the device. Example: CT 3rd Floor.	This is a free text field 1-30 characters long.

Field	Description	Possible Values
LOCAL AE TITLE (#2006.9192, 1)	The AE title of the local application entity that the remote device is accessing (local with respect to the VistA system at your site). For example, VISTA_STORAGE is the AE title of the DICOM Gateway to which remote devices send images to the VistA system.	This is a free text field 1-16 characters long. Use VISTA_STORAGE for devices that store data in the VistA system using the DICOM Gateway. Use DICOM_QR for devices that use Q/R to query the VistA system. Use IMPORTER for devices Import devices that connect to the network.
REMOTE AE TITLE (#2006.9192, 1.1)	The AE title of the remote device (remote with respect to your VistA system). For example a device that sends images to the DICOM Gateway, or a device that queries the VistA database.	This is a free text field 1-16 characters long. The value must be specified and should not contain spaces.
FORCE RECONCILIATION (#2006.9192,1.3)	This field is relevant only for the DICOM Import devices connected to the network. The value indicates whether the imported images are queued in the DICOM Importer queue for reconciliation or not. For all other devices, use the default value – NO.	NO YES

ORIGIN INDEX (#2006.9192,1.4)	This field is relevant only for the DICOM Import devices connected to the network.	V = VA (US Department of Veterans Affairs) D = Department of Defense F = FEE (Commercial institutions) N = NON-VA origin I = IHS Indian Health Services
----------------------------------	---	--

Field	Description	Possible Values
SITE (#2006.9192, 2)	The division or the site (for sites that are not part of a division) in which the device resides.	The name of the division (site) or its number in the INSTITUTION file (#4): the file that contains a listing of VA institutions.
IP ADDRESS (#2006.9192, 3)	The IP address (or host name) of the device (remote AE title). Only required for Q/R devices.	A string 1-30 characters long.
PORT NUMBER (#2006.9192, 4)	The port number used to communicate with the device (remote AE title). Only required for Q/R devices	A number between 199999.
DICOM SERVICE (#2006.919212, .01)	<p>The DICOM Service Class of the device. Each device that sends data to the VistA system should be defined as a Service Class User (SCU) of the Storage Service Class (C-STORE).</p> <p>Each device that queries the VistA system should be defined as a Service Class User (SCU) of the C-FIND and the C-MOVE Service Classes.</p> <p>If new DICOM Objects are sent to VistA Imaging gateway, it should be defined as a Service Class User (SCU) of the Storage Service Class (C-STORE).</p> <p>If the retrieved objects are stored on the devices local drive, it should also be defined as a Service Class Provider (SCP) of the Storage Service Class (C-STORE).</p>	<p>The valid values and their meaning are:</p> <ul style="list-style-type: none"> 1 = C-STORE (Storage) 2 = C-FIND (Query) 3 = C-MOVE (Retrieve) 4 = C-ECHO 5 = STORAGE

Field	Description	Possible Values
DICOM ROLE (#2006.919212, 1)	<p>The DICOM role of the device. Each device is defined as a Service Class User (SCU) or a Service Class Provider (SCP) of a specific DICOM Service Class.</p> <p>An SCU is the user of a DICOM service. For example, a device that sends data to the VistA system is an SCU for the C-STORE service.</p>	<p>The valid values and their meaning are:</p> <p>6 = SCU</p> <p>7 = SCP</p>

Field	Description	Possible Values
SERVICE TYPE (#2006.9192, 11)	The type of service that generated the order with which the object is associated.	RAD = Radiology CON = Consult
RELAX VALIDATION ¹ (#2006.9192, 10)	The value of this flag determines if the HDIG should relax validation for the object or perform full validation. When this field is set to YES, the HDIG does not send error messages to the sending device when an object that passed basic validation fails the full IOD validation. The HDIG processes objects that pass the basic IOD validation, but fail the complete IOD validation and does not report the validation error to the sending device. When the RELAX VALIDATION flag is set to NO, the HDIG rejects the object if the object fails the full IOD validation and reports the validation errors to the sending device.	NO YES
REJECT ¹ (#2006.9192, 6)	When the value is set to YES, the HDIG sends a Reject message to the device that sent the object every time an object is rejected because it failed basic IOD validation. When the flag is set to NO, the HDIG sends an Error message indicating that there is a problem in the processing flow, but without any other details.	NO YES

¹ Indicates a flag relevant only for devices sending data to the DICOM Gateway.

Field	Description	Possible Values
VALIDATE ¹ (#2006.9192, 9)	<p>When the value is set to YES, the DICOM Listener performs full IOD validation. If the object fails full IOD validation, the HDIG checks the setting of the RELAX VALIDATION flag. If the RELAX VALIDATION flag is set to YES, the HDIG processes the object without rejecting it, as explained in the description of the RELAX VALIDATION flag. Otherwise, it rejects the object and sends a message. The setting of the REJECT flag determines the verbosity of the message.</p> <p>If the VALIDATE flag is set to NO, the HDIG does not perform full IOD validation; it performs only basic IOD validation.</p>	NO YES
WARNING ¹ (#2006.9192, 7)	<p>When the value is set to YES, the HDIG sends a message to the device that sent the object, every time the HDIG finds a duplicate or illegal UID. When the flag is set to NO, the HDIG sends a warning message indicating that there is a problem in the processing flow, but without any other details.</p>	NO YES

Field	Description	Possible Values
RESERR ¹ (#2006.9192, 8)	When the RESERR flag is set to YES, the DICOM listener sends a message to the device that sent the object, every time the HDIG cannot store the object because of a problem with the resource (VistA database, RAID disk, or other storage resource), such as problems connecting to the resource, lack of disk space to store the object, and so on. When the flag is set to NO, the HDIG sends an Error message indicating that there is a problem in the processing flow, but without any other details.	NO YES
N RESPONSE DELAY (#2006.9192, 13)	This is the number of minutes the HDIG will wait before responding to a DIMSE N-ACTION request from this Remote AE TITLE. (MAG*3.0*79).	A number between 0 and 99999, 0 decimal digits.
N RESPONSE RETRIES (#2006.9192, 14)	This is the number of times an HDIG will attempt to re-deliver a DIMSE N-RESPONSE message to this Remote AE TITLE (MAG*3.0*79).	A number between 0 and 99999, 0 decimal digits.

Example DICOM AE SECURITY MATRIX Values (partial)

Parameter	Description	Storage Device	Q/R Device	Network Importer
AE NAME	The name of the device.	CT 3 rd Floor	QR 3D Workstation	SLC_3 rd _Party_PET
LOCAL AE TITLE	The AE title (name) of the local application entity (local to your VistA system) with which the device communicates.	VISTA_STORAGE	DICOM_QR	IMPORTER
REMOTE AE TITLE	The AE title of the device you are adding.	CT_SCAN3	QR_3D_WORKST	SLC_3 rd _Party_PET
FORCE RECONCILIATION	Relevant for network import only.	NO	NO	YES
ORIGIN INDEX	The origin (source) of the study.	not used accept defaults	not used accept defaults	<Choose a value> DoD
SITE	The division or the site.	<YourSite> Example: 660 for Salt Lake City	<YourSite>	<YourSite>
IP ADDRESS	The IP address (or host name) of the device.	not used accept defaults	<QRWorkstationIP>	not used accept defaults
PORT NUMBER	The port number used to connect to the remote device.	not used accept defaults	<3DWorkstationPort#>	not used accept defaults

Parameter	Description	Storage Device	Q/R Device	Network Importer
Flags	REJECT, WARNING RESERR, VALIDATE, RELAX VALIDATION, SERVICE TYPE	Select values based on your needs YES	not used accept defaults	not used accept defaults

Note: See the next section for defining DICOM Services and Roles.

Adding Devices to the DICOM AE SECURITY MATRIX

You must add an entry in the DICOM AE SECURITY MATRIX for each device (AE_Title) that you want to store data in the VistA system or to query the VistA system. You add devices to the DICOM AE SECURITY MATRIX using VistA menu option Configure AE SECURITY MATRIX Settings [MAGV AE SEC MX SETTINGS] located on the Imaging System Manager Menu [MAG SYS MENU].

Note: Bold in the screen samples indicates what you enter or select.

The following summarizes the objects you must define and their roles:

- Each device that sends data to the DICOM Gateway must be defined as a C-STORE SCU.
- Each device that queries the VistA system must be defined as a:
 - C-FIND SCU
 - C-MOVE SCU
 - C-STORE SCP (if the device stores the Q/R results on a local drive)
- Each DICOM Importer server instance that receives studies through the network from an outside location must be defined as a CSTORE SCU.
- To enable Storage Commitment for an SCU, the value STORAGE COMMIT has to be added to the entry's DICOM SERVICE AND ROLE multiple field as an SCU.

To add devices to the DICOM AE SECURITY MATRIX file and set their properties:

- 1 At the Select OPTION NAME prompt, enter **Imaging System Manager Menu**.

Log into VistA and choose the Imaging System Manager Menu [MAG SYS MENU] when prompted:

Select OPTION NAME: Imaging System
Manager Menu

HL7 Imaging HL7 Messaging Maintenance ...

IX Image Index Conversion Menu ...

LS Edit Network Location STATUS

TR Telereader Menu ...

Ad hoc Enterprise Site Report

Configure AE Security Matrix Settings

Delete Image Group

Delete Study by Accession Number

Enter/edit Reason

Imaging Database Integrity Checker Menu ...

Imaging Site Reports ...

Importer Menu ...

2 Press <Enter> to proceed.

3 When prompted with Select Imaging System Manager Menu Option: type **Con** and press <Enter> to select the option with Configure AE SECURITY MATRIX Settings. This option lets you add new devices to the DICOM AE SECURITY MATRIX and edit or delete existing ones.

Select Imaging System Manager Menu Option: Configure AE Security
Matrix Settings

DICOM AE SECURITY MATRIX
APPLICATION EDIT

4 To determine what devices have already been configured, type ? and press <Enter>. This displays the list of devices that have already been configured and their DICOM service and role as illustrated.

Select DICOM AE SECURITY MATRIX AE NAME: ?

Answer with DICOM AE SECURITY MATRIX NUMBER, or AE NAME:

1 IMPORTER SALT LAKE CITY IMPORTER
C-STORE SCU

You may enter a new DICOM AE SECURITY MATRIX, if you wish
Answer must be 1-30 characters in length.

Select DICOM AE SECURITY MATRIX AE NAME:

Adding a Storage Device

- 1 Type the name of the device at the prompt and press **<Enter>** to proceed. The name can be descriptive. It can be 1-30 characters long and must be unique for every VistA system

Select DICOM AE SECURITY MATRIX AE NAME:CT 3 rd Floor

- 2 Type **YES** when prompted to confirm the name of the device you are adding.

Are you adding 'CT 3 rd Floor' as a new DICOM AE SECURITY MATRIX (the 10TH)? No// YES (Yes)

- 3 Define the site of your VistA system when prompted. You can define the location using the site number or the site name. Typically, you would be prompted with the default site location as illustrated in the following example. If you do not need to change it, press **<Enter>** to accept the default. If there are multiple sites that match the default string, you are prompted to select one of them. Select the desired site and press **<Enter>** to continue.

DICOM AE SECURITY MATRIX SITE: 660//
1 660 SALT LAKE CITY UT 660
2 660AA SALT LAKE DOM UT VAMC 660AA
CHOOSE 1-2: 1 SALT LAKE CITY UT 660

- 4 Type the Remote AE_Title (the AE_Title of the device) at the prompt. The AE_Title can be a maximum of 16 characters , should NOT have spaces, and is not case sensitive.

DICOM AE SECURITY MATRIX REMOTE AE TITLE: CT_SCAN3

- 5 Press **<Enter>** to continue.

- 6 Accept the default value – VISTA_STORAGE – and press **<Enter>** to continue.

LOCAL AE TITLE: VISTA_STORAGE//

- 7 Accept the default value, **NO**.

FORCE RECONCILIATION: NO// NO

- 8 Accept the default value, **VA**, only required for MAG*3.0*118 Importer devices.

ORIGIN INDEX: V// VA

- 9 For IP address press **<Enter>** to continue.

Note: IP Address number are only required when configuring a device to use Query/Retrieve.

IP ADDRESS:

- 10 For TCP port number press **<Enter>** to continue.

Note: Port numbers are only required when configuring a device to use Query/Retrieve.

PORT NUMBER:

- 11 Define the flags of the device when prompted. If you choose to change the default values of any of the flags *for the specific device*, follow the prompts.

Note: The flag values are relevant only for devices that send images to the VistA system. If you are adding a device that queries the VistA system, accept the defaults.

- To accept the defaults, press **<Enter>**.
- To change the values of *any* of the flags, type **NO** and press **<Enter>**.

Flag Names Flag Values

REJECT YES

WARNING	YES
RESERR	YES
VALIDATE	YES
RELAX VALIDATION	YES
SERVICE TYPE	RADIOLOGY
Accept these defaults? YES//	

Note: SERVICE TYPE can accept either RADIOLOGY or CONSULT

12 When prompted, define the DICOM service of the device and its role.

Tip: You can enter ? to display the possible values.

Select DICOM SERVICE: 1 (1 C-STORE) Are you adding 'C-STORE' as a new DICOM SERVICE (the 3RD for this DICOM AE SEC URITY MATRIX)? No// Y (Yes) DICOM ROLE: 2 SCP Select DICOM SERVICE: "C-STORE" (1 C-STORE) Are you adding 'C-STORE' as a new DICOM SERVICE (the 4TH for this DICOM AE SEC URITY MATRIX)? No// Y (Yes) DICOM ROLE: 2 SCU

13 When you define the DICOM role and service pair, you are prompted to define another DICOM service and role pair. Press **<Enter>** to continue.

14 Repeat this procedure to define the properties of all the storage devices that you want to add to the DICOM AE SECURITY MATRIX.

Entries for Storage Commitment Requests

To enable Storage Commitment for an SCU, the value STORAGE COMMIT has to be added to the entry's DICOM SERVICE AND ROLE multiple field as an SCU. In addition, the entry requires the definition of the host (IP address) and port, of the remote SCU, needed to accept the association made with reverse role negotiation.

Any SCU (that has not been configured) issuing a Storage Commitment request in the AE Security Matrix will receive a reject response for the N-ACTION request issued. The association for DICOM Storage Commitment will be accepted because it is controlled by the DICOM DCF_Toolkit Listen file used by the SCP.

It is assumed that the SCU supports reverse role negotiation and is configured to accept an incoming association request.

In order to generate a meaningful Storage Commitment response for the sender, it is required that at least one remote C-MOVE SCU be defined in the DICOM AE SECURITY MATRIX (#2006.9192). This is because the entry's local AE title is where the Storage Commitment response building module picks up the C-MOVE SCP AE (Retrieve AE Title) of the VistA system.

Example 1:

A *Storage Commitment SCU* entry with new field values and fields highlighted (N-Response-Delay is entered in minutes):

AE NAME: IVV-SCU	LOCAL AE TITLE: VISTA_STORAGE
SITE: SALT LAKE CITY	IP ADDRESS: 172.16.0.128
PORT NUMBER: 60090	REMOTE AE TITLE: IVV_SCU
FORCE RECONCILIATION: NO	ORIGIN INDEX: VA
REJECT: YES	WARNING: YES
RESERR: YES	VALIDATE: NO
RELAX VALIDATION: YES	SERVICE TYPE: RADIOLOGY
N RESPONSE DELAY: 2	N RESPONSE RETRIES: 2
DICOM SERVICE: C-STORE	DICOM ROLE: SCU
DICOM SERVICE: C-FIND	DICOM ROLE: SCU
DICOM SERVICE: STORAGE COMMIT	DICOM ROLE: SCU

Example 2:

A *C-MOVE SCU* entry with needed field highlighted (used for Retrieve AE Title in DICOM Response message, so sender knows where to get committed item from):

AE NAME: QR	LOCAL AE TITLE: DICOM_QR
SITE: SALT LAKE CITY	REMOTE AE TITLE: QR_SCU
FORCE RECONCILIATION: NO	ORIGIN INDEX: VA
REJECT: YES	WARNING: YES
RESERR: YES	VALIDATE: YES
RELAX VALIDATION: YES	SERVICE TYPE: RADIOLOGY
DICOM SERVICE: C-MOVE	DICOM ROLE: SCU

Adding a Query Retrieve Remote Device (MAG*3.0*116)

- 1 Type the name of the device at the prompt and press <Enter> to proceed. The name can be descriptive. It can be 1-30 characters long and must be unique for every VistA system

Select DICOM AE SECURITY MATRIX AE NAME:CT 3D Workstation

- 2 Type **YES** when prompted to confirm the name of the device you are adding.

Are you adding 'CT 3D Workstation ' as a new DICOM AE SECURITY MATRIX (the 12TH)? No// YES (Yes)

- 3 Define the site of your VistA system when prompted. You can define the location using the site number or the site name. Typically, you would be prompted with the default site location as illustrated in the following example. If you do not need to change it, press <Enter> to accept the default. If there are multiple sites that match the default string, you are prompted to select one of them. Select the desired site and press <Enter> to continue.

DICOM AE SECURITY MATRIX SITE: 660//
1 660 SALT LAKE CITY UT 660
2 660AA SALT LAKE DOM UT VAMC 660AA
CHOOSE 1-2: 1 SALT LAKE CITY UT 660

- 4 Type the Remote AE_Title (the AE_Title of the device) at the prompt. The AE_Title can be a maximum of 16 characters, should NOT have spaces, and is not case sensitive.

DICOM AE SECURITY MATRIX REMOTE AE TITLE: CT_3D_Workstation

- 5 Press <Enter> to continue.

- 6 Change the default value – VISTA_STORAGE to DICOM_QR – and press <Enter> to continue.

LOCAL AE TITLE: DICOM_QR//

- 7 Accept the default value, **NO**.

FORCE RECONCILIATION: NO// NO

- 8 Accept the default value, **V**.

ORIGIN INDEX: V// V

- 9 For IP address, enter the IP Address or Host Name of the device and press <Enter> to continue.

Note: IP Address number/Host Name are required when configuring a device to use Query/Retrieve.

IP ADDRESS: 10.0.X.XXX

- 10 Type the TCP port number the remote device uses. Then press <Enter> to continue.

Note: Port numbers are required when configuring a device to use Query/Retrieve.

PORT NUMBER: 104

- 11 Define the flags of the device when prompted. Press <Enter> to accept the default values.

Note: The flag values are relevant only for devices that send images to the VistA system. If you are adding a device that queries the VistA system, accept the defaults.

Flag Names	Flag Values

REJECT	YES
WARNING	YES
RESERR	YES
VALIDATE	YES
RELAX VALIDATION	YES
SERVICE TYPE	
RADIOLOGY	
Accept these defaults?	
YES//	

- 12 When prompted, define the DICOM service of the device and its role.

DICOM Q/R Processing	DICOM Service	DICOM Role
Find	C-FIND	SCU
Retrieve	C-MOVE	SCU
Workstation storage	C-STORE	SCP
PACS storage	C-STORE	SCU
DICOM Storage Processing	DICOM Service	DICOM Role
Store	C-STORE	SCU
Store	C-STORE	SCP
Storage commit	STORAGE COMMIT	SCU

Note: You can define two roles for the same DICOM service. To do so, use quotes when you specify the service the second time. The following screen example illustrates defining two roles for the same DICOM service: C-STORE SCP and C-STORE SCU

```
Select DICOM SERVICE: ??
    You may enter a new DICOM SERVICE AND ROLE, if you wish
    This is the DICOM service associated with this entry.
Choose from:
1    C-STORE
2    C-FIND
3    C-MOVE
4    C-GET
5    N-ACTION
6    N-CREATE
7    N-EVENT-REPORT
8    N-GET
9    N-SET
10   N-DELETE
11   C-ECHO

Select DICOM SERVICE: 2 (2  C-FIND)
Are you adding 'C-FIND' as a new DICOM SERVICE (the 1ST for this
DICOM AE
SECURITY MATRIX)? No// ???
    Answer with 'Yes' or 'No'? yes (Yes)
DICOM ROLE: ??
    This is the DICOM role, Service Class User (SCU) or Service Class
    Provider ( SCP), associated with the entry.
```

Choose from:

1 SCU

2 SCP

DICOM ROLE: 1 SCU

Select DICOM SERVICE: 3 (3 C-MOVE)

Are you adding 'C-MOVE' as a new DICOM SERVICE (the 2ND for this DICOM AE SECURITY MATRIX)? No// yes (Yes)

DICOM ROLE: 1 SCU

Select DICOM SERVICE: 1 (1 C-STORE)

Are you adding 'C-STORE' as a new DICOM SERVICE (the 3RD for this DICOM AE SECURITY MATRIX)? No// yes (Yes)

DICOM ROLE: 1 SCU

Select DICOM SERVICE: "C-STORE" (1 C-STORE)

Are you adding 'C-STORE' as a new DICOM SERVICE (the 4TH for this DICOM AE SECURITY MATRIX)? No// y (Yes)

DICOM ROLE: 2 SCP

Select DICOM SERVICE: STORAGE COMMIT (5 STORAGE COMMIT)

Are you adding 'STORAGE COMMIT' as a new DICOM SERVICE (the 5TH for this DICOM AE SECURITY MATRIX)? No// y (Yes)

DICOM ROLE: 1 SCU

Tip: You can enter ? to display the possible values.

13 When you define the DICOM role and service pair, you are prompted to define another DICOM service and role pair. If you need to define another DICOM service and role pair, follow the prompts. Otherwise, press enter to continue.

14 Repeat this procedure to define the properties of all Query/Retrieve devices that you want to add to the DICOM AE SECURITY MATRIX.

15 Press <Enter> to continue.

Adding an Importer Network Storage Device (MAG*3.0*118)

1 Type the name of the device at the prompt and press <Enter> to proceed. The name can be descriptive. It can be 1-30 characters long and must be unique for every VistA system

Select DICOM AE SECURITY MATRIX AE NAME:SLC_3rd_Party_PET

--

- 2 Type **YES** when prompted to confirm the name of the device you are adding.

Are you adding 'SLC_3 rd _Party_PET' as a new DICOM AE SECURITY MATRIX (the 13TH)? No// YES (Yes)

- 3 Define the site of your VistA system when prompted. You can define the location using the site number or the site name. Typically, you would be prompted with the default site location as illustrated in the following example. If you do not need to change it, press <Enter> to accept the default. If there are multiple sites that match the default string, you are prompted to select one of them. Select the desired site and press <Enter> to continue.

DICOM AE SECURITY MATRIX SITE: 660//
1 660 SALT LAKE CITY UT 660
2 660AA SALT LAKE DOM UT VAMC 660AA
CHOOSE 1-2: 1 SALT LAKE CITY UT 660

- 4 Type the Remote AE_Title (the AE_Title of the device) at the prompt. The AE_Title can be a maximum of 16 characters, should NOT have spaces, and is not case sensitive.

DICOM AE SECURITY MATRIX REMOTE AE TITLE: SLC_3 rd _Party_PET

- 5 Press <Enter> to continue.
- 6 Change the default value – VISTA_STORAGE – to - IMPORTER - and press <Enter> to continue.

Note: IMPORTER is a default value in the DICOM AE SECURITY MATRIX.

LOCAL AE TITLE: IMPORTER//

- 7 Change the default value, **NO** to **YES**.

FORCE RECONCILIATION: NO// YES

8 Specify the value for the field ORIGIN INDEX.

Note: Choices are:

V = VA (US Department of Veterans Affairs)

D = Department of Defense

F = FEE (Commercial
institutions) **N** = NON-VA origin

I = IHS Indian Health Services

ORIGIN INDEX: V// VA

9 For IP address, press <Enter> to continue.

Note: IP Address number are only required when configuring a device to use Query/Retrieve.

IP ADDRESS:

10 For TCP port, press <Enter> to continue.

Note: Port numbers are only required when configuring a device to use Query/Retrieve.

PORT NUMBER:

11 Define the flags of the device when prompted. If you choose to accept the default values of any of the flags *for the specific device*, follow the prompts.

Note: The flag values are relevant only for devices that send images to the VistA system.

Note: Choices for SERVICE TYPE are RADIOLOGY or CONSULT.

- To accept the defaults, press <Enter>.
- To change the values of *any* of the flags, type **NO** and press <Enter>.

Flag Names	Flag Values

REJECT	YES
WARNING	YES
RESERR	YES
VALIDATE	YES
RELAX VALIDATION	YES
SERVICE TYPE	RADIOLOGY
Accept these defaults?	
YES//	

12 When prompted, define the DICOM service of the device and its role.

Select DICOM SERVICE: 1 (1 C-STORE) Are you adding 'C-STORE' as a new DICOM SERVICE (the 3RD for this DICOM AE SEC URITY MATRIX)? No// Y (Yes) DICOM ROLE: 2 SCP Select DICOM SERVICE: "C-STORE" (1 C-STORE) Are you adding 'C-STORE' as a new DICOM SERVICE (the 4TH for this DICOM AE SEC URITY MATRIX)? No// Y (Yes) DICOM ROLE: 2 SCU
--

Tip: You can enter ? to display the possible values.

Select DICOM SERVICE: ?

You may enter a new DICOM SERVICE AND ROLE, if you wish

Select a DICOM Service.

Choose from:

- 1 C-STORE
- 2 C-FIND
- 3 C-MOVE
- 4 C-GET
- 5 N-ACTION
- 6 N-CREATE
- 7 N-EVENT-REPORT
- 8 N-GET
- 9 N-SET
- 10 N-DELETE
- 11 C-ECHO

Select DICOM SERVICE: 2 (2 C-FIND)

Are you adding 'C-FIND' as a new DICOM SERVICE (the 1ST for this DICOM AE SECURITY MATRIX)? No// Y (Yes)

DICOM ROLE: ?

Select a DICOM Role.

Choose from:

- 1 SCU
- 2 SCP

DICOM ROLE: 1 SCU

Select DICOM SERVICE: 3 (3 C-MOVE)

Are you adding 'C-MOVE' as a new DICOM SERVICE (the 2ND for this DICOM AE

SEC

RITY MATRIX)? No// Y (Yes)

DICOM ROLE: 1 SCU

Select DICOM SERVICE: 1 (1 C-STORE)

Are you adding 'C-STORE' as a new DICOM SERVICE (the 3RD for this DICOM AE

SEC

URITY MATRIX)? No// Y (Yes)

DICOM ROLE: 2 SCP

Select DICOM SERVICE:

13 When you define the DICOM role and service pair, you are prompted to define another DICOM service and role pair. If you need to define another DICOM

service and role pair, follow the prompts. Otherwise, press <**Enter**> to continue.

- 14** Repeat this procedure to define the properties of all Network Storage devices that you want to add to the DICOM AE SECURITY MATRIX.

Appendix C Pre-Install Checklist

1. Site Info

- a Site Name: _____
- b Site Code: _____
- c Other Sites Supported: _____
- d Site Contact Name: _____
- e Site Contact Phone: _____
- f Site Contact E-mail Address: _____

2. Documentation Review Completed (Date):

- a Review related patch descriptions: _____
- b DICOM Gateway User Manual: _____
- c Appendix A of this document – Activating the DCF Toolkit
Product Serial Number: _____
- d Appendix B of this document – The DICOM AE Security
Matrix: _____
- e Review related user manuals: _____

3. Do you have a VIX installed (YES/NO)? _____

4. Are the prerequisite patches installed (YES/NO)?

5. Do you have a Radiology Commercial PACS System (cPACS)?

- a Manufacturer: _____
- b Model: _____
- c Software Version: _____
- d Does it receive DICOM data directly from modalities or from VistA
(Circle One): MODALITIES VISTA

6. Did you request and receive Product Serial Numbers (PSN) from Laurel Bridge (YES/NO)? _____

7. Dictionaries

- a Do all of your DICOM Gateways share a single set of dictionaries
(YES/NO)? _____
- b Copy of MODALITY.DIC provided (YES/NO)? _____

- c** Copy of INSTRUMENT.DIC provided (YES/NO)?_____
- d** What is the RPC VistA Server port number:_____
- 8.** What e-mail addresses will be used for gateway e-mail notifications?

- 9.** Was the .NET Framework 4.6.2 or above software able to be installed on all gateways (YES/NO)?_____

Appendix D Post-Install Checklist

1. KIDS install date: _____
2. VistA System Configured:
 - a. DICOM AE SECURITY MATRIX configured: _____
 - b. What method was used to configure?: _____
 - c. IMAGING SITE PARAMETER file updated: _____
 - d. Users Configured: _____
 - e. Outside Locations configured: _____
3. HDIG installed (Date): _____
4. HDIG update verified by: _____
5. Gateway Install
 - a. Gateway(s) install date - start: _____
 - b. Gateway(s) install date - complete: _____
 - c. Gateway update verified by: _____
 - d. Anti-virus exclusions configured: _____
 - e. Reviewed MODALITY.DIC file installed: _____
 - f. Reviewed INSTRUMENT.DIC file installed: _____
 - g. Legacy menu updates performed: _____
 - h. HDIG memory increased: _____
 - i. Verified that each instrument on the gateway is storing images correctly: _____
 - j. Verified new DICOM Correct is working for radiology: _____
 - k. Verified new DICOM Correct is working for consults: _____
 - l. Verified Query/Retrieve is working properly: _____
 - m. Verified Query/Retrieve for NTP is working correctly: _____
 - n. DICOM AE SECURITY MATRIX configuration verified via _____
 - o. HDIG Summary Logs: _____
 - p. HDIG Summary Log viewed for each HDIG: _____
 - q. ImagingExchangeWebApp.log reviewed for each server? _____
 - r. Gateway Inventory worksheet – Post Install completed: _____

6. Importer III Desktop Client Install

- a. User worksheet – Post Install configuration complete: _____
- b. Workstation worksheet – Post Install configuration
complete: _____
- c. Users trained on software: _____

Appendix E DCF Toolkit Enterprise License Request Form

Site Name: _____ (example: Biloxi, MS)

Station Number: _____ (as specified in the STATION NUMBER field 99 of the INSTITUTION file)

Contact Name: _____.

E-mail: _____.

Phone: _____

Server Name	# of CPUs	Previous DCF?	Product Serial Number

(Note 1: A CPU chip containing multiple hyper-threaded or multi-core processing elements is counted as a single CPU.) (Note

2: HP Sites - DL360 machines = 1 CPU, DL380 machines = 2CPUs)

(Note 3: Dell Sites - Normally only a single socket (Single socket = 1 CPU) is populated in the imaging servers but it is possible that this is not the case for all Dell systems in VHA. If you have questions call your DELL sales rep., and provide the service tag # and S/N of the processor/server.