VistA Blood Establishment Computer Software (VBECS) Version 2.0.0

Technical Manual-Security Guide

April 2015

Department of Veterans Affairs
Product Development

This page intentionally left blank.

Revision History

Date	Revision	Description	Author
9-9-13	1.0	Modified VistA Blood Establishment Computer Software (VBECS) 1.6.0 Technical Manual-Security Guide, Version 5.0: Global: Replaced “1.6.0” with “2.0.0”. Global: Replaced “July 2012” with “September 2013”. Global: Replaced “5.0” with “1.0” in the document footer. Rewrote entire document to account VBECS 2.0.0 architectural changes. Added Configuring the App Server and Lab Workstations for VBECS 2.0.0 section. Updated Appendix G for current VLAN guidance.	BBM Team
9-29-14	2.0 (cont. on next page)	Modified VistA Blood Establishment Computer Software (VBECS) 2.0.0 Technical Manual-Security Guide, Version 1.0: Global: Replaced “September 2013” with “September 2014”. Global: Replaced “1.0” with “2.0” in the document footer. Global: Changed “Remedy” to “Service Desk”. Global: Removed references to “Windows XP”. Global: Changed "RDS" to "RDP". Global: Removed all references to the VLAN and ACL. Global: Removed hyperlinks where not needed. Global: Added “(Enterprise Operations Only)” to applicable headings. Global: Changed “VBECS development” to “VBECS maintenance”. Global: Added a reference to the support section every time filing a ticket is mentioned. Global: Changed wording in Enterprise Operations section to separate ownership from the site. Global: Removed mentions of "cluster" server. Global: Changed "Admin" to "Administrator". Introduction: Moved Figure 2 above Figure 1. Deleted the box that explained version numbers. How This Technical Manual-Security Guide is Organized section: Added a section called Enterprise Operations Tasks. Remote Desktop Configuration: Removed Windows XP section. Create a Remote Desktop Connection Shortcut for VBECS section: Updated Step 1 with correct path. VBECS Version Numbers section: Added an explanation of revision for Figure 2. Added explanation of system error for code not matching database build number (Figure 1). Printers: Rewrote introduction to include mention of duplex printing and reference to second server. Installing a Printer section: Revised Steps 1 and 8. Required Peripherals section, Table 1: Revised first table row. Moved to front of section. Table 3: Added VBECS Reports row. Label Printer: Added Zebra ZM400 or Z4MPlus. Off-the-Shelf Software section, Table 2: Changed “SP1” to “SP2”. Workstation Configuration: Changed "Professional" to "Enterprise" Periodic System Maintenance, caution box: Corrected time and added time zones. Windows Updates section: Revised and renamed to “Applying Windows Updates”. ePolicy and Virus Definitions section: Revised paragraph. Firmware Updates: Deleted. VistA Maintenance Operations section: Revised. VBECS Maintenance Operations, Configure Interfaces, Configure VistALink Parameters section: Added Step 6 to account for new fields.	BBM Team

Date	Revision	Description	Author
9-29-14	2.0 (cont. from previous page)	Updated Steps 7 and 8 to describe the service restart. Updated Figure 63. Configure VistALink Parameters: Added a new Step 6. Revised Steps 4, 6, 7 and 8. Configure CPRS HL7 Interface Parameters: Revised Steps 6, 9 and 11 (updated Step 11 to describe the service restart). Configure Patient Update HL7 Interface Parameters: Revised Step 8 notes. Windows Updates: Revised and added Server Restart Warning screen. Configure Divisions: Added 2 bullet points to Assumptions, updated Step 10. Configure Users, Assumptions: Added bullets 12 through 15. Updated Steps 3, 5 and 6. Changed "Transmit Workload Data" to "Record Workload Data". Removed Appendix A: Installing the USB Emulation Driver and Visual Xpress. Updating the Hand-Held 4600 Scanner section, Step 10: Removed reference to VBECS Technical Bulletin BB10-01. Configure Patient Update HL7 Interface Parameters section, Step 8: Changed the note to describe including blood bank users in the email group. Server Hardware and System Configuration: Removed reference to Windows XP from Figure 19. Implementation and Maintenance, Table 3: Added a row for cleanup of the report share. Trouble Shooting section: Added a new sub-section, Remote Desktop Session Issues to describe disconnecting remote desktop sessions. Added VistALink configuration instructions. Released Technical Bulletins (one-time execution required) section: Removed entire section including its sub-sections. Application-Wide Exceptions section: Added a table and figure to describe the event sources that VBECS uses. Group Policy section: Added last paragraph. Configure a Shortcut to the Report Share section: Added note to second paragraph. VistA Maintenance Operations: Updated instruction to explain when the configuration must be updated. Set Up VBECS Outbound Logical Links section: Added a new step after #1 instructing site to shut down the link first. Monitor VBECS HL7 Logical Links section: Revised Step 6. Table14 and Table 15: Revised. Configure System Administrators section: Removed. Zebra Printer Problems section: Removed warning box. Virtual Local Area Network section: Incorporated this section into Group Policy section. Table 13 and Figure 116 (Event Sources): Added. VLAN section and Figure 171: Removed. Glossary: Added new items. Appendix D, Data Center Instructions, Windows Updates section: Revised paragraph. Appendix G Complete VLAN Requirements: Removed.	BBM Team
11/5/14	3.0	Modified VistA Blood Establishment Computer Software (VBECS) 2.0.0 Technical Manual-Security Guide, Version 2.0: Global: Replaced “September 2014” with “November 2014”. Global: Replaced “2.0” with “3.0” in the document footer. Global: Removed the word “Minimum” from all requirements and specifications sections.	BBM Team

Date	Revision	Description	Author
2/10/15	4.0	Modified VistA Blood Establishment Computer Software (VBECS) 2.0.0 Technical Manual-Security Guide, Version 3.0: Global: Replaced “November 2014” with “February 2015”. Global: Replaced “3.0” with “4.0” in the document footer. Introduction section: Removed 3rd warning box. Applying Windows Updates section: Adjusted to reflect change in update schedule per Enterprise Operations (EO). Configure VistALink Parameters, Step 8, VBECS Administrator column: Added sentence beginning “When you receive a message…”. Configure CPRS HL7 Interface Parameters section, Step 11, VBECS Administrator column: Added sentence beginning “When you receive a message…”.Appendix D, RDP Server section: Added the location of the group policy license server setting. Added a caution box with contact information for Terminal Server license issues.	BBM Team
4/27/15	5.0	Modified VistA Blood Establishment Computer Software (VBECS) 2.0.0 Technical Manual-Security Guide, Version 4.0: Global: Replaced “February 2015” with “April 2015”. Global: Replaced “4.0” with “5.0” in the document footer. • DR 5160: Global: Changed “Product Support” to “Health Product Support.” • DR 5160: Scanners section: Added configuration barcodes for Xenon 1900. • DR 5160: Security section: Added a subsection called Health Product Support Access.Applying Windows Updates section, Table 6, first row, last column, added that the updates are done “with notification.” • Applying Windows Updates section, Table 8: Updated schedule with App Server patch deployment on Wednesday, with notification and on the 8 day (previously the 11 day) after patch deployment. . • Applying Windows Updates section, App Server paragraph: updated with the details about the updates. • All Configure Interfaces sections: Change the text to better explain service restarts. • Added the opening paragraph, Table 11 and Table 12 to describe HL7 error messages and supported versions. • Configure Patient Update HL7 Interface Parameters table, step 8 and Configure CPRS HL7 Interface Parameters table step 9, added new note to clarify the email sent upon HL7 message failure and added a link to the troubleshooting section. • Globally corrected formatting for bullets verses numbering.	BBM Team

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Introduction

The main purpose of the VistA Blood Establishment Computer Software (VBECS) is to automate the daily processing of blood inventory and patient transfusions in a hospital transfusion service.

Unauthorized access or misuse of this system and/or its data is a federal crime. Use of all data, printed or electronic, must be in accordance with VA policy on security and privacy.

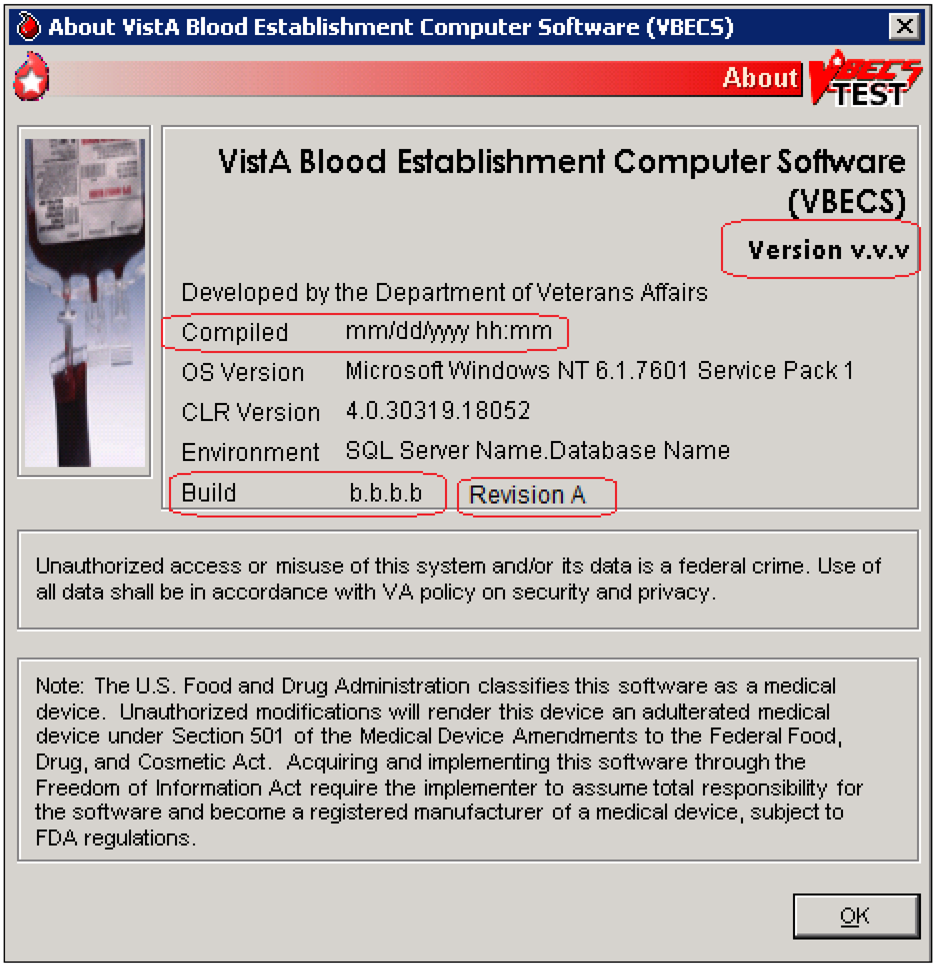
Do not change the system! The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations. Adding to or updating VBECS software without permission is prohibited.

VBECS Version Numbers

In earlier VBECS patch releases, the user documentation referred to the VBECS version in a 4-digit format (e.g., 2.0.0.2 – where 2.0.0 represents the patch version and the last digit (2) is the patch build number). The build number is used by VBECS Health Product Support for diagnostic and troubleshooting purposes.

The VBECS version will be represented with only the first three digits (e.g., 2.0.0) and will appear that way in all user documentation to simplify readability. The full 4-digit version can still be found under the **Help**, **About VBECS** window in VBECS (Figure 1) and will appear in patch installation guides where build specific files are referenced. The revision letter tracks database-only updates (e.g., blood product table updates, canned comments updates). The revision letter is normally a single alpha character (e.g., C), but can be two characters (e.g., AA, AB, AC) in the unlikely event that more than 25 database updates are made, before a code change is implemented. The revision letter starts at A with each new code change and is incremented to B when the first database-only update is made. The revision letter is then updated by one character in the alphabet for every successive database-only update until a new code change is implemented at which time the revision letter reverts back to A. The version submitted for system testing will be revision A, but the version customers receive can be revision A, B or higher revision letter.

Figure 1: Example of Help, About VBECS



VistA Blood Establishment Computer Software (VBECS)

Version v.v.v

Developed by the Department of Veterans Affairs

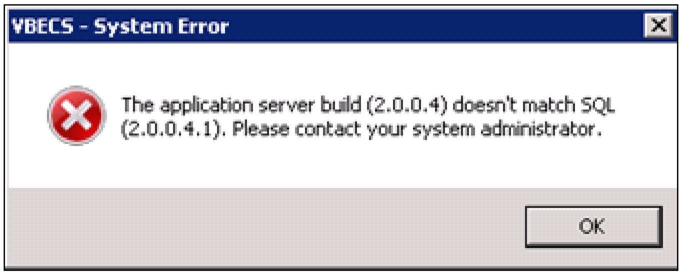
Compiled	mm/dd/yyyy hh:mm
OS Version	Microsoft Windows NT 6.1.7601 Service Pack 1
CLR Version	4.0.30319.18052
Environment	SQL Server Name.Database Name
Build	b.b.b.b Revision A

Unauthorized access or misuse of this system and/or its data is a federal crime. Use of all data shall be in accordance with VA policy on security and privacy.

Note: The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations.

The VBECS Administrator and VBECS applications, when started, will verify that the application code (binary build number) matches the SQL Server code (database build number) in order to ensure that application servers and SQL servers are patched and remain in sync with each other. In the rare event that they fall out of sync, the applications will present the following error message (Figure 2) and close until both the code and the database are in sync.

Figure 2: Example of System Error



VBECS - System Error

The application server build (2.0.0.4) doesn't match SQL (2.0.0.4.1). Please contact your system administrator.

Related Manuals and Reference Materials

HL7 V2.3.1 Implementation Guide http://www.hl7.org/implement/standards/product_brief.cfm?product_id=141#ImpGuides
*CPRS-VBECS Interface (OR*3.0*212) Release Notes April 2009*
PIMS V. 5.3 Technical Manual
DUPLICATE RECORD MERGE: PATIENT MERGE TECHNICAL MANUAL Version 7.3 April 1998 Revised December 2010
Kernel Systems Manual Version 8.0, Chapter 1: Sign-On Security/User Interface, pp. 13–20
Manage Open Sessions and Files in Windows 2008 R2, http://technet.microsoft.com/en-us/library/cc725689.aspx
Health Product Support Release of Products and Patches Guide V2.3 Updated: February 2014
VistA Blood Establishment Computer Software (VBECS) 2.0.0 Installation Guide
VistA Blood Establishment Computer Software (VBECS) 2.0.0 Data Center Installation Guide
VistA Blood Establishment Computer Software (VBECS) 2.0.0 Database Upgrade Instructions
VistA Blood Establishment Computer Software (VBECS) 2.0.0 Database Upgrade Installation Form
VistA Blood Establishment Computer Software (VBECS) 2.0.0 Template Creation Guide
VistA Blood Establishment Computer Software (VBECS) 2.0.0 SQL Server 2012 Installation Guide
VistA Blood Establishment Computer Software (VBECS) 2.0.0 User Guide
VistALink Version 1.5 Developer-System Manager Manual, Chapter 6: Security Management, pp. 34–35
Windows Server 2008R2 Security Guide, Microsoft Corporation (http://technet.microsoft.com/en-us/library/gg236605.aspx)

This page intentionally left blank.

How This Technical Manual-Security Guide Is Organized

Outlined text is used throughout this guide to highlight warnings, limitations, and cautions:

> *Warnings, limitations, cautions*

Terms

For consistency and space considerations, the pronouns “he,” “him,” and “his” are used as pronouns of indeterminate gender equally applicable to males and females.

In many instances, a user may scan a barcode or enter data manually (by typing). The term “enter” is used throughout this guide to mean “enter manually.”

See the Glossary for definitions of other terms and acronyms used in this guide.

Figures and Tables

If you refer to figures and tables from the technical manual-security guide in your local policy and procedure documents, you may wish to use their titles only, without figure or table numbers: as the technical manual-security guide is updated, those numbers may change.

Screen Shots

Because VBECS is a medical device, screen shots must be captured at various points throughout the technical manual-security guide to meet FDA requirements for objective evidence and documentation. A 📷 (camera) at the beginning of each step that requires a screen capture will identify these points. For more information, see Appendix A: Instructions for Capturing Screen Shots.

Commonly Used System Rules

This section includes system rules that apply to several or all options.

Only one instance of the VBECS Administrator can run at a time.

VBECS captures changes to verified data for inclusion in the Audit Trail Report.

VBECS protects application data through encapsulation. Encapsulation promotes data security by hiding the implementation details.

Enterprise Operations Tasks

Some of the tasks in this guide are executed by members of Enterprise Operations (EO) affiliated with the data center where VBECS Servers are hosted. These tasks are differentiated by the text in the headings with (Enterprise Operations Only) noted in the heading.

Appendices

The appendices contain truth tables and other materials for reference.

While pressing the Ctrl button, left-click on a section name or page number in the table of contents to move to that section or page. The index does not incorporate this feature.

.

Remote Desktop Configuration (Windows 7)

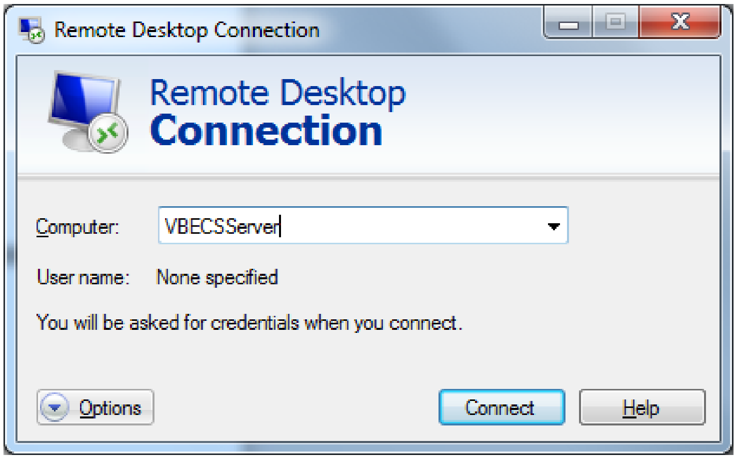
Configure the screen resolution, sound, and connection speed, and create a Remote Desktop Connection shortcut on each VBECS workstation.

Screen Resolution

To set the screen resolution:

1. Double-click (the **Remote Desktop Connection** icon).
2. Click **Options** (Figure 3).

Figure 3: Example of Remote Desktop Connection Options



Remote Desktop Connection

Remote Desktop Connection

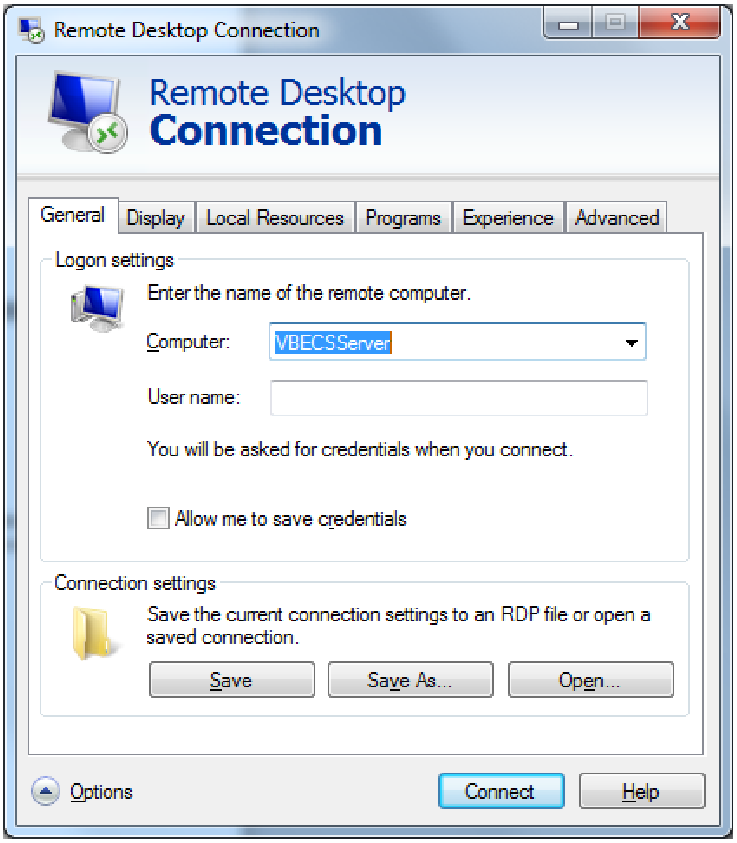
Computer: VBECSServer

User name: None specified

You will be asked for credentials when you connect.

3. Click the **General** tab (Figure 4).
4. Enter the VBECS application server name or application server IP address in the Computer field.
5. Enter **your Domain** (e.g., VHAMASTER) in the Domain field. Do not enter a user name or password.

Figure 4: Example of General Tab Computer and Domain



Logon settings

Enter the name of the remote computer.

Computer: VBECSServer

User name:

You will be asked for credentials when you connect.

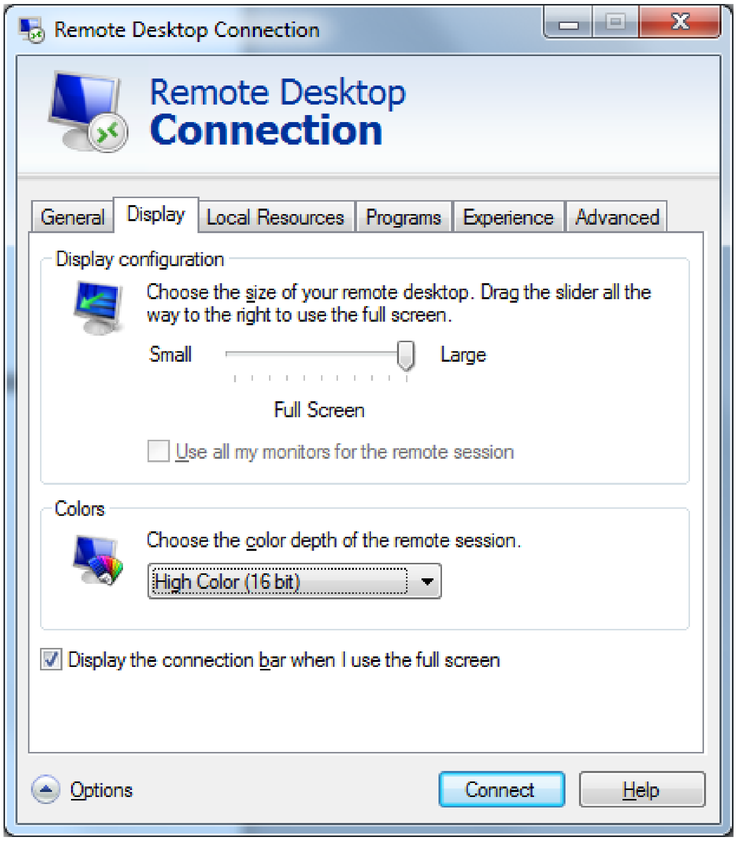
□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

6. Click the **Display** tab (Figure 5).
7. Click, hold, and slide the pointer to a screen resolution of Full Screen.

Figure 5: Example of Display Tab



Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.

Full Screen

□ Use all my monitors for the remote session

Choose the color depth of the remote session.

High Color (16 bit)

☑ Display the connection bar when I use the full screen

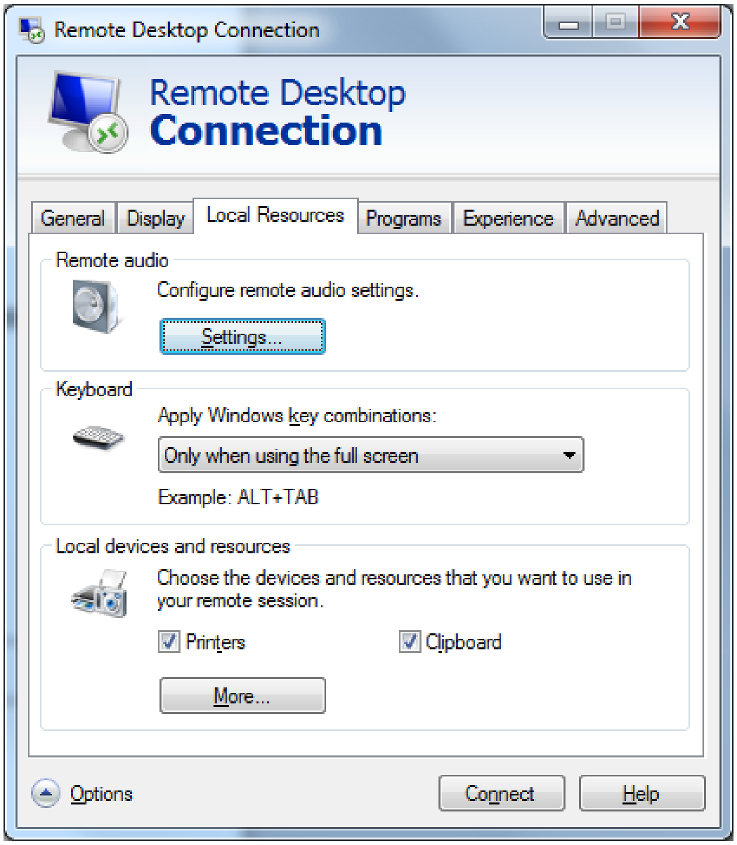
Sound

To enable sound:

8. Click the **Local Resources** tab (Figure 6).
9. Click the **Settings** button.

> *Failure to properly configure the sound disables audible alerts throughout VBECS.*

Figure 6: Example of Remote Computer Sound



Remote audio

Configure remote audio settings.

Keyboard

Apply Windows key combinations:

Only when using the full screen

Example: ALT+TAB

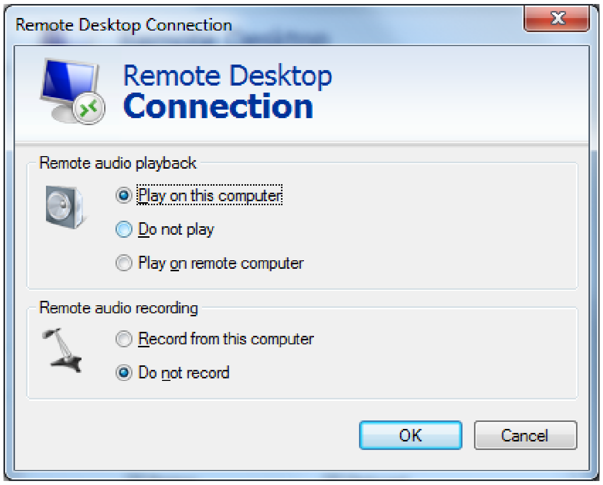
Local devices and resources

Choose the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard

10. Select **Play on this computer** (Figure 7) from the Remote audio playback section.
11. Click the **OK** button.

Figure 7: Remote audio playback selection



Remote audio playback

● Play on this computer

○ Do not play

○ Play on remote computer

Remote audio recording

○ Record from this computer

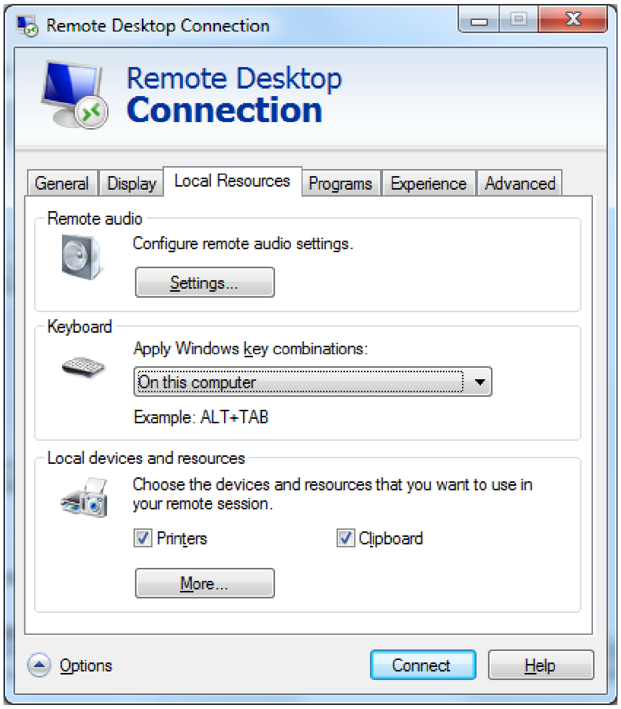
● Do not record

Keyboard

To configure keyboard settings:

12. Click the **Local Resources** tab (Figure 8).
13. Select **On this computer** from the Keyboard drop-down list.

Figure 8: Example of Remote Computer Keyboard



Remote audio

Configure remote audio settings.

Keyboard

Apply Windows key combinations:

On this computer

Example: ALT+TAB

Local devices and resources

Choose the devices and resources that you want to use in your remote session.

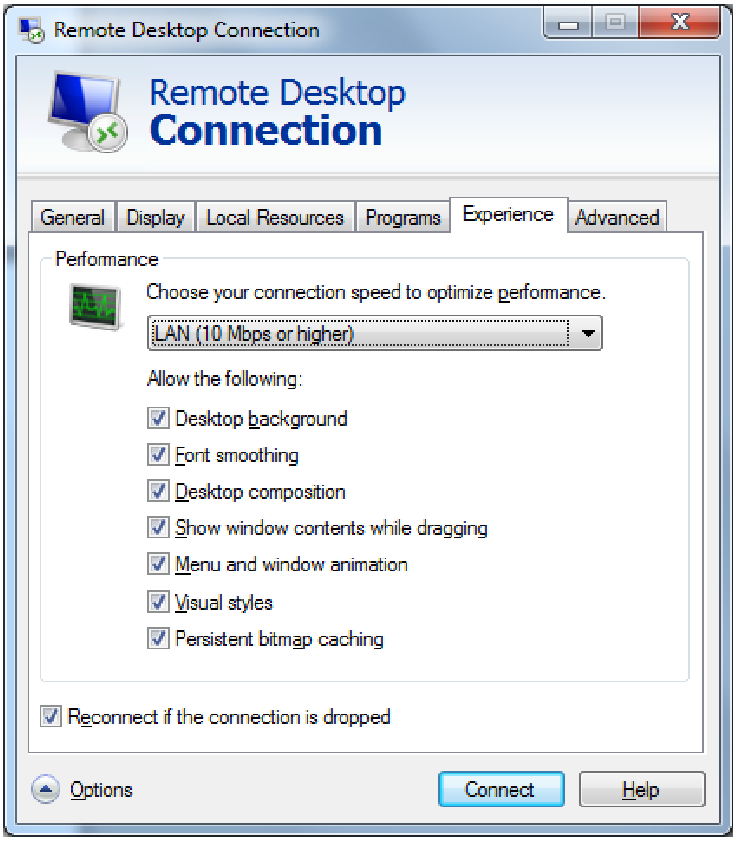
☑ Printers ☑ Clipboard

Connection Speed

To set the connection speed:

14. Click the **Experience** tab (Figure 9).
15. Select **LAN (10 Mbps or higher)** from the Choose your connection speed to optimize performance drop-down list.

Figure 9: Example of Connection Speed



Choose your connection speed to optimize performance.

LAN (10 Mbps or higher)

Allow the following:

☑ Desktop background

☑ Font smoothing

☑ Desktop composition

☑ Show window contents while dragging

☑ Menu and window animation

☑ Visual styles

☑ Persistent bitmap caching

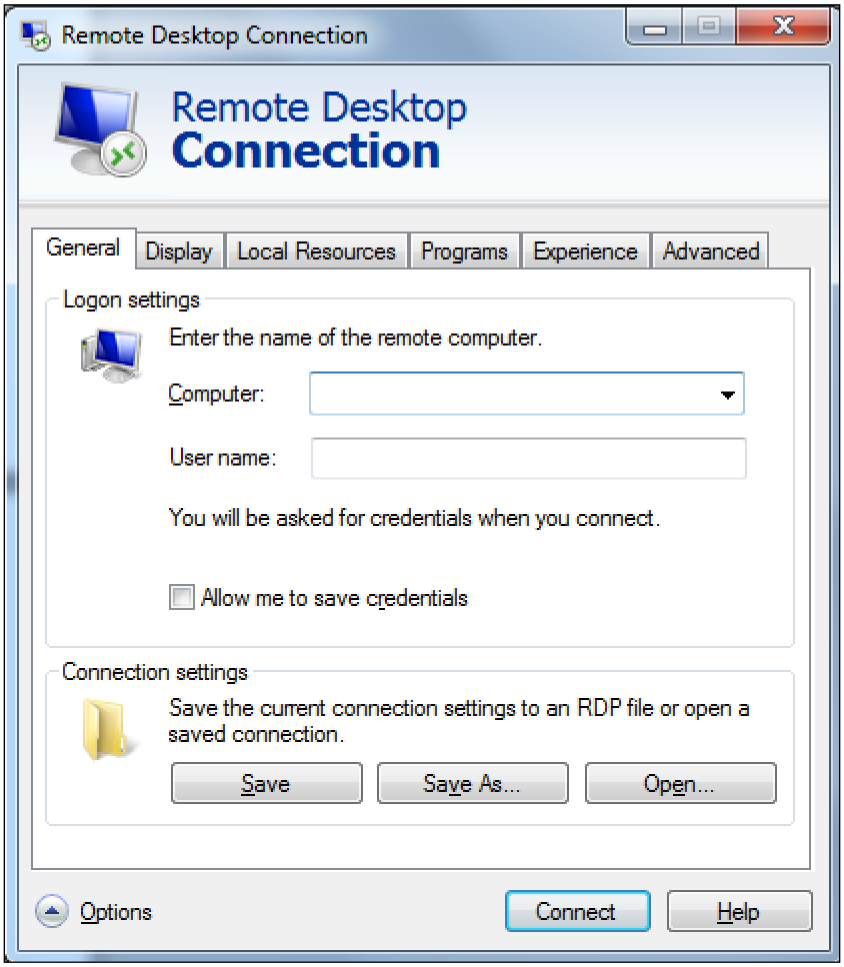
☑ Reconnect if the connection is dropped

Save Settings

To save the settings:

16. Click the **General** tab (Figure 10).
17. Click **Save As**.

Figure 10: Example of General Tab Save As



Enter the name of the remote computer.

Computer:

User name:

You will be asked for credentials when you connect.

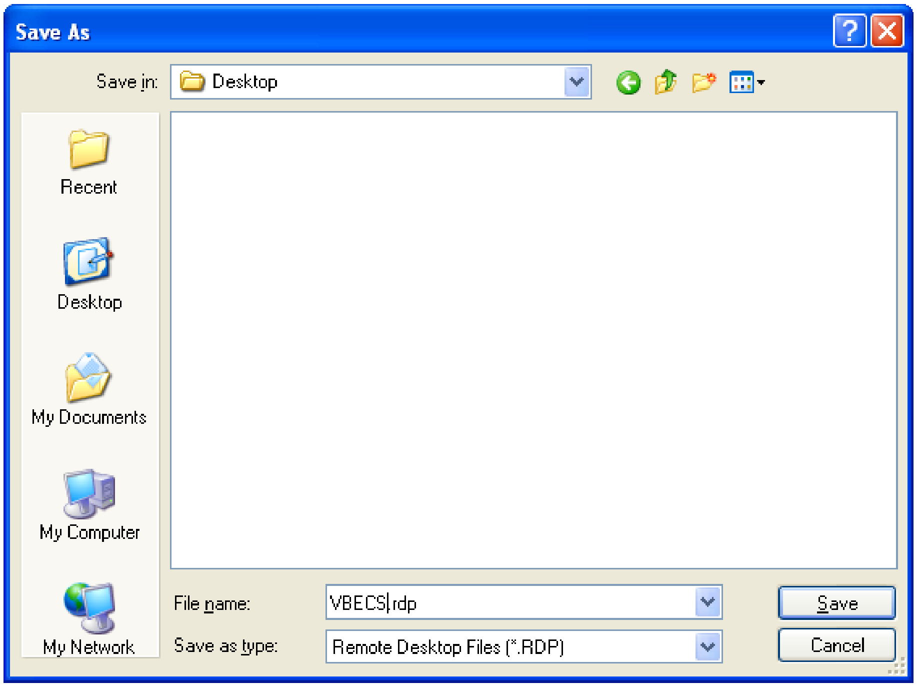
☐ Allow me to save credentials

Save the current connection settings to an RDP file or open a saved connection.

Create a Remote Desktop Connection Shortcut for VBECS

18. To create a Remote Desktop Connection shortcut for VBECS (Figure 11), save the file as VBECS.rdp in the **C:\Users\Public\Desktop** folder.

Figure 11: Example of Remote Desktop Connection Shortcut for VBECS



Save As

Save in: Desktop

File name: VBECS.rdp

Save as type: Remote Desktop Files (*.RDP)

Double-click the shortcut to launch the Remote Desktop Connection to VBECS.
The Windows start-up sound confirms that the sound functions.

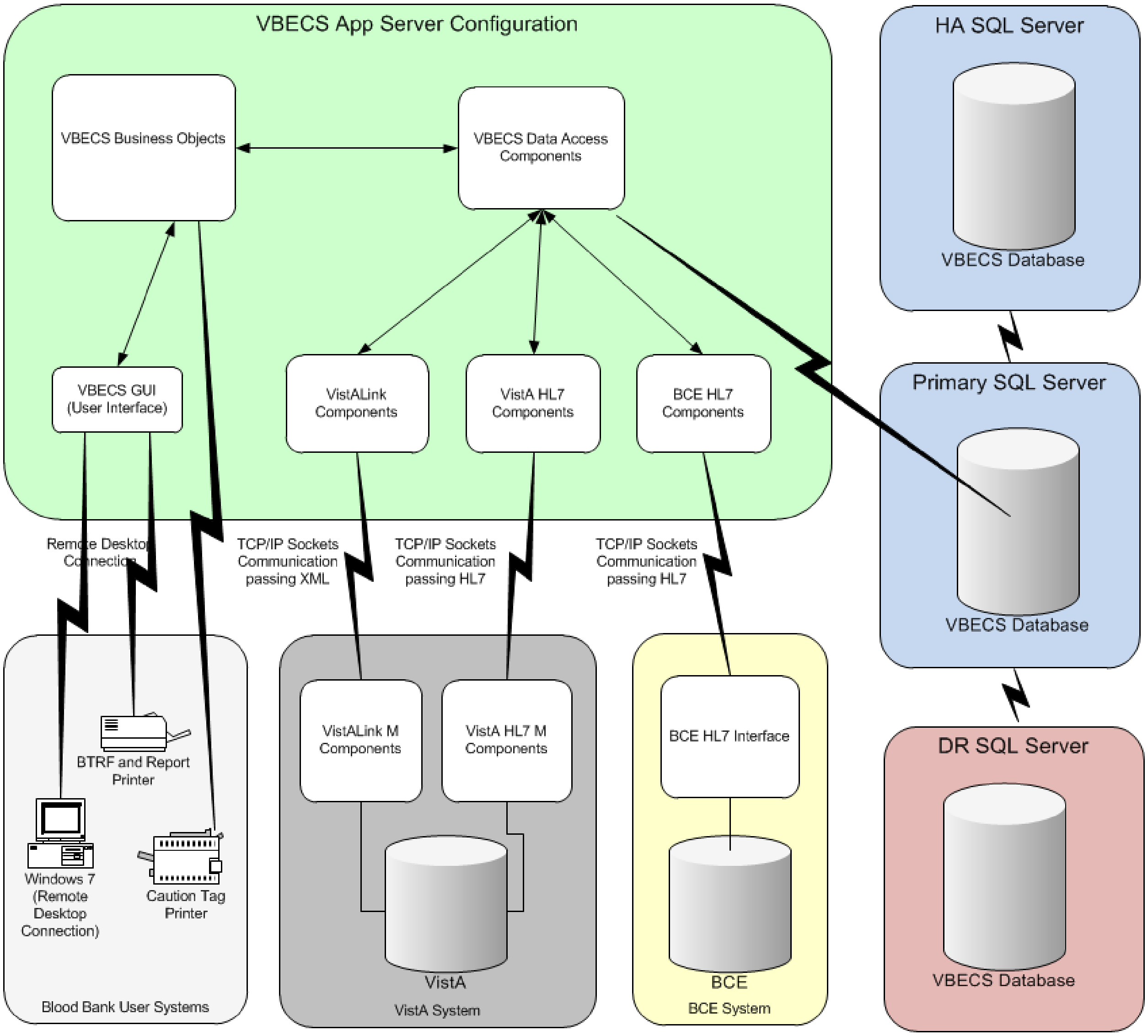
Server Hardware and System Configuration

The VBECS application requires that hardware and system software serve five users in a standard configuration and up to twenty-five users in an integrated Veterans Integrated Service Network (VISN) environment.

The System Schematic diagram (Figure 12) describes the major system components:

- **Application Server (App Server)**: This is a Windows 2008 Server Enterprise Edition R2 (x64) server and is the execution environment for the VBECS application (both Test and Production). It also functions as a Remote Desktop Protocol (RDP) Server. Each VBECS instance (single or multidivisional) has a unique App Server.
  The App Server also communicates with and exchanges information with VistA applications and BCE COTS through messages formatted using Extensible Markup Language (XML) and Health Level 7 (HL7) over Transmission Control Protocol/Internet Protocol (TCP/IP) networking.
- **SQL Server**: This is a Windows 2008 Server Enterprise Edition R2 (x64) server that runs SQL Server 2012. It hosts the VBECS databases for each single or multidivisional instance.
  SQL Servers exist in an AlwaysOn cluster, which consists of three nodes. The Primary and High Availability servers reside at the primary site while a Disaster Recovery server resides at an alternate location:
  - Primary server: This server fields all requests. Its data are replicated to the High Availability and Disaster Recovery servers.
  - High Availability (HA) server: This server provides database backup services through synchronous replication. Its data are guaranteed to be consistent with the Primary. It becomes the Primary should the original Primary server fail or become unreachable. Failover to this server is automatic.
  - Disaster Recovery (DR) server: This server resides at a remote site and provides database backup services through asynchronous replication. It becomes the Primary server should both the Primary and HA server fail or become unreachable. Failover to this server is a manual process.
- **Windows 7 Workstations**: Users continue to access the VBECS application using Remote Desktop Services.

Figure 12: System Schematic



Required Peripherals

Table 1 describes additional required hardware.

Table 1: Additional Required Hardware

Additional Required Hardware	
Barcode Scanner	Hand-Held Model 4600 (This is the model distributed with the original VBECS deployment and is now discontinued. The successor is the Honeywell Xenon 1900.)
Report Printer	HP LaserJet 9040dn (sites may elect to use a different report printer)
Label Printer	Zebra ZM400 or Z4MPlus, Must print at 300 DPI

Printers

Report Printer

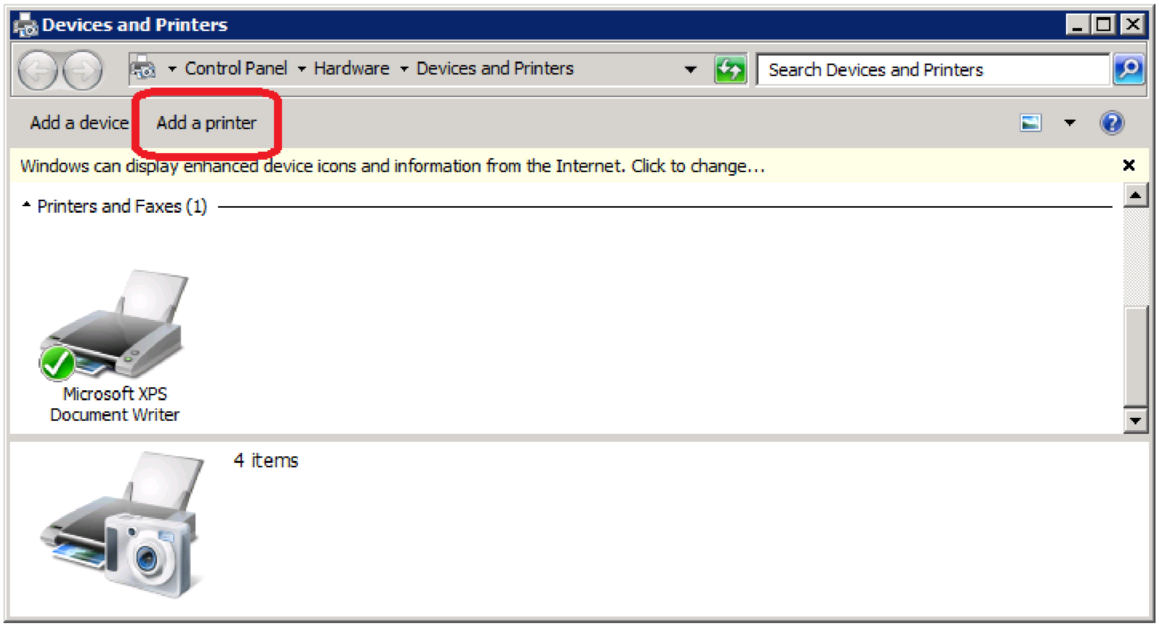
A laser printer capable of printing 8.5" x 11" sheets may be used. VBECS supports duplex printing, but not all printers are duplex capable. Consult the printer documentation to determine if it has this capability.

Installing a Printer (Enterprise Operations Only)

To install a printer, execute the following instructions:

1. Log into the app server with administrative privileges.
2. Click **Start**, **Devices and Printers.** The Device and Printers window is displayed (Figure 13). Click the **Add a printer** button**.**

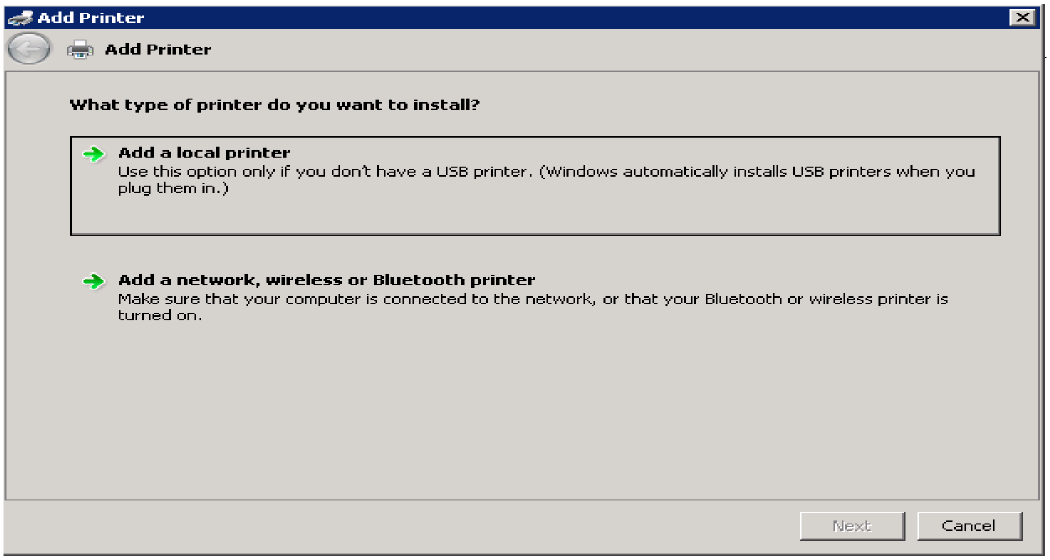
Figure 13: Example of Devices and Printers, Add a printer


Devices and Printers
Control Panel ▸ Hardware ▸ Devices and Printers
Search Devices and Printers
Add a device
Add a printer
Printers and Faxes (1)
Microsoft XPS Document Writer
4 items

Windows can display enhanced device icons and information from the Internet. Click to change...

3. In the Add Printer Wizard screen, select the **Add a local printer** button (Figure 14).

Figure 14: Example of Add Printer Wizard



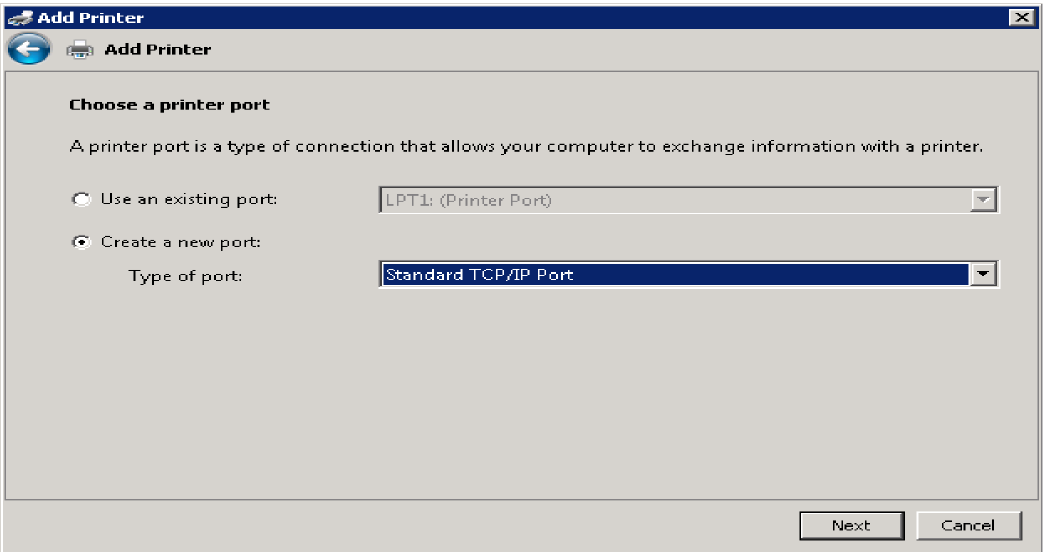
What type of printer do you want to install?

Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

4. On the Choose a printer port window, select **Create a new port** radio button. From the Type of port: drop-down, select **Standard TCP/IP Port**. Click **Next** (Figure 15).

Figure 15: Example of Add Printer Wizard



Choose a printer port

A printer port is a type of connection that allows your computer to exchange information with a printer.

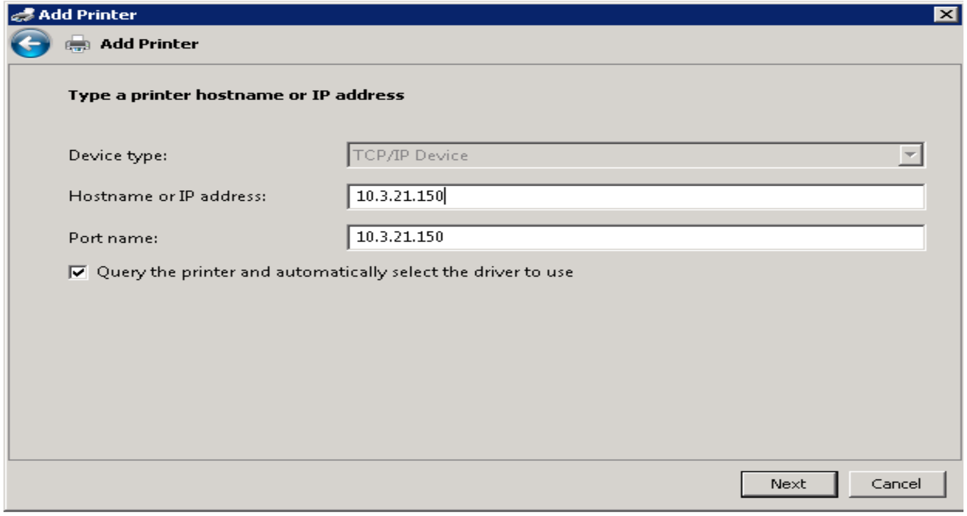
○ Use an existing port: LPT1: (Printer Port)

● Create a new port:

Type of port: Standard TCP/IP Port

5. Enter the IP address of the printer in the Hostname or IP address field (the Port Name field will populate automatically). Click **Next** (Figure 16).

Figure 16: Example of TCP/IP Settings



Type a printer hostname or IP address

Device type: TCP/IP Device

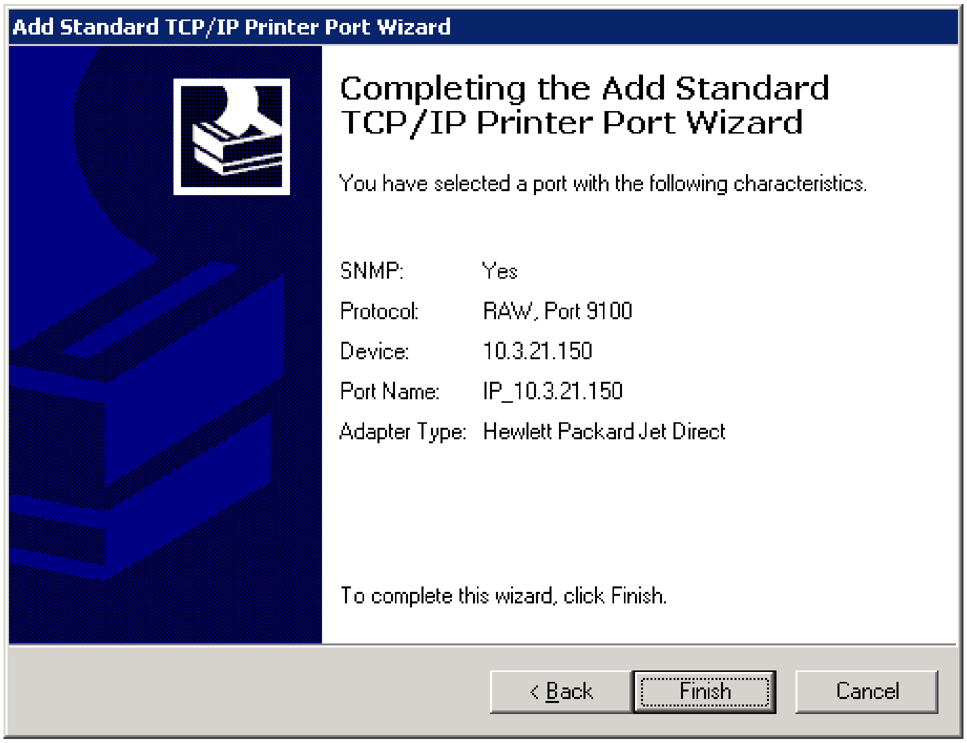
Hostname or IP address: 10.3.21.150

Port name: 10.3.21.150

☑ Query the printer and automatically select the driver to use

6. Click **Finish** (Figure 17).

Figure 17: Example of Review Settings



Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP: Yes

Protocol: RAW, Port 9100

Device: 10.3.21.150

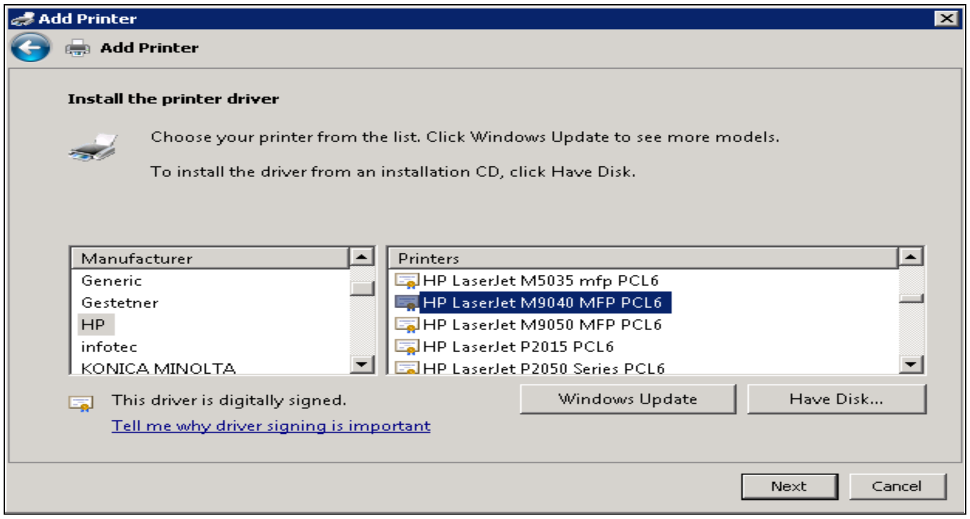
Port Name: IP_10.3.21.150

Adapter Type: Hewlett Packard Jet Direct

To complete this wizard, click Finish.

7. To select a driver, click **Have Disk** (Figure 18). Note: If the site has chosen to use a printer other than the HP LaserJet 9040, you must point to the correct driver at this point; continue at Step 10.

Figure 18: Example of Add Printer Wizard


Add Printer
Add Printer
Install the printer driver
Choose your printer from the list. Click Windows Update to see more models.
To install the driver from an installation CD, click Have Disk.
Manufacturer
Generic
Gestetner
HP
infotec
KONICA MINOLTA
Printers
HP LaserJet M5035 mfp PCL6
HP LaserJet M9040 MFP PCL6
HP LaserJet M9050 MFP PCL6
HP LaserJet P2015 PCL6
HP LaserJet P2050 Series PCL6
This driver is digitally signed.
Tell me why driver signing is important
Windows Update
Have Disk...
Next
Cancel

8. Click **Browse** (Figure 19). Navigate to **C:\temp\HP9040 PCL6 Driver** and select **HP9040 PCL6 driver**. Click **Open** (Figure 20). Note: If the site is using a printer other than the HP 9040, you will have to supply this driver.

Figure 19: Example of Install From Disk

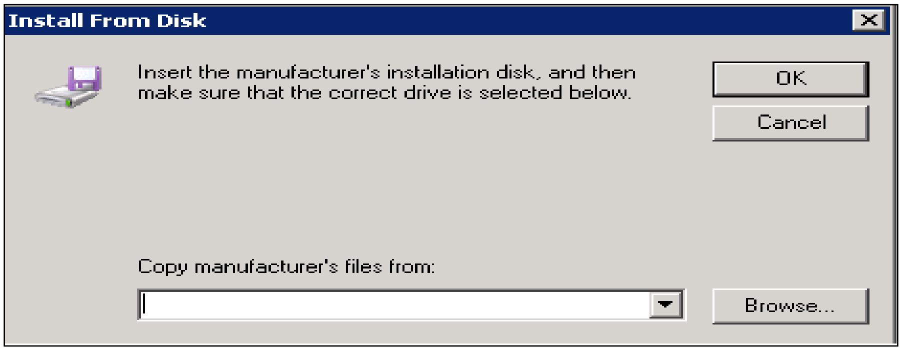
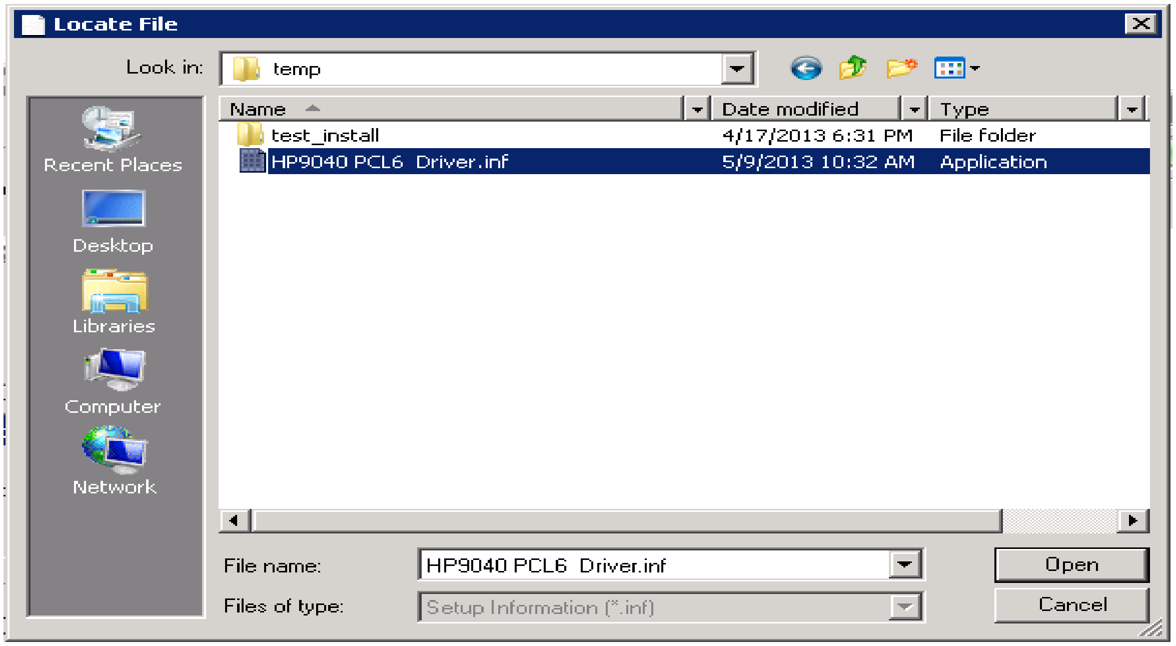

Install From Disk
Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.
OK
Cancel
Copy manufacturer's files from:
Browse...

Figure 20: Example of Select Driver



Name	Date modified	Type
test_install	4/17/2013 6:31 PM	File folder
HP9040 PCL6 Driver.inf	5/9/2013 10:32 AM	Application

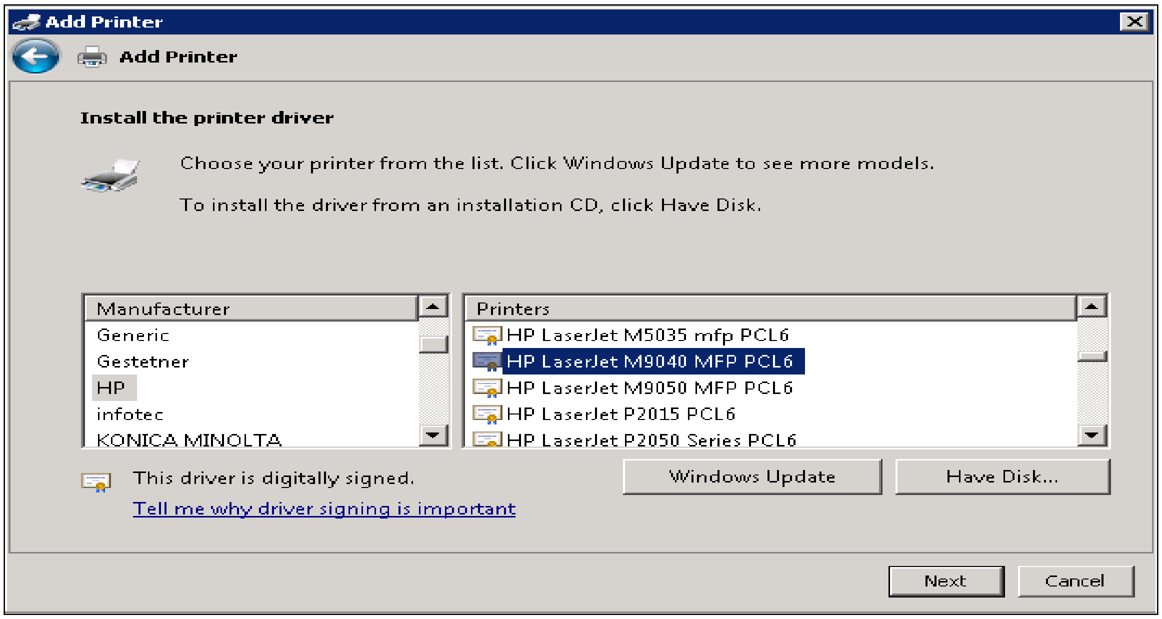
File name: HP9040 PCL6 Driver.inf

Files of type: Setup Information (*.inf)

9. Click **OK** (Figure 19).

Make sure that the HP LaserJet M9040 MFP PCL6 driver is selected (Figure 21)

Figure 21: Example of Add Printer Driver Wizard



Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

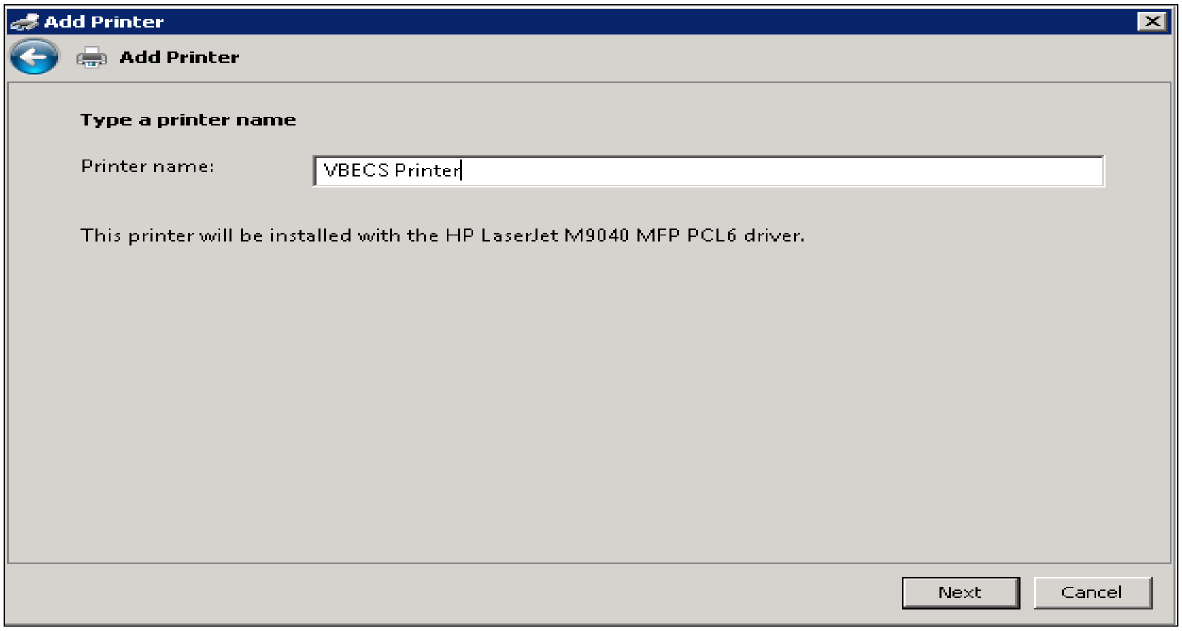
To install the driver from an installation CD, click Have Disk.

This driver is digitally signed.

Tell me why driver signing is important

10. For a single-division site, enter **VBECS Printer** as the printer name. For a multidivisional site, enter **VBECS Printer** and the site name (e.g., VBECS Printer Hines). Click **Next** (Figure 22)

Figure 22: Example of Add Printer Wizard



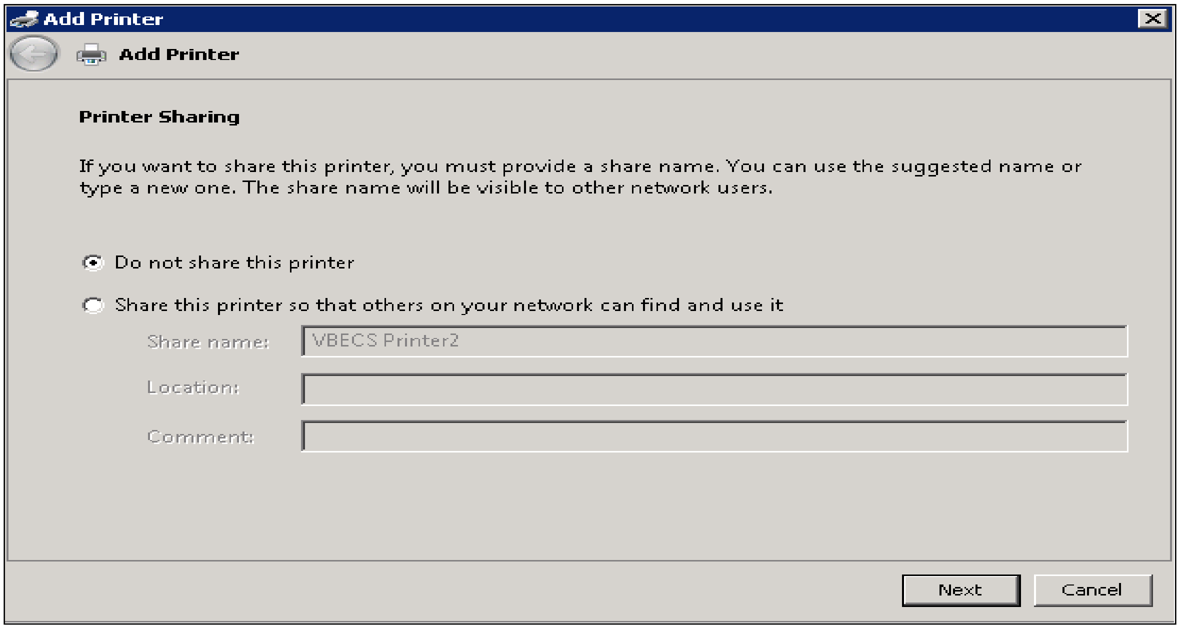
Type a printer name

Printer name: VBECS Printer

This printer will be installed with the HP LaserJet M9040 MFP PCL6 driver.

11. Click the **Do not share this printer** radio button. Click **Next** (Figure 23).

Figure 23: Example of Add Printer Wizard



Printer Sharing

If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.

● Do not share this printer

○ Share this printer so that others on your network can find and use it

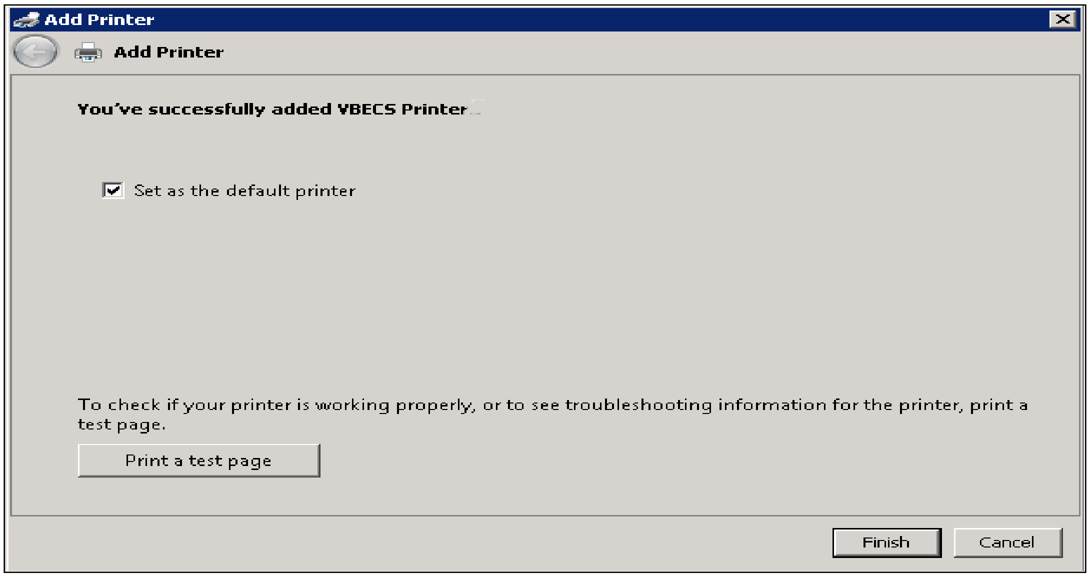
Share name: VBECS Printer2

Location:

Comment:

12. Click **Next** (Figure 24).

Figure 24: Example of Add Printer Wizard



Add Printer

Add Printer

You've successfully added VBECS Printer

☑ Set as the default printer

To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.

Label Printer (Zebra ZM400 or Z4MPlus)

These instructions are for a Zebra Z4M and Z4MPlus. If using a different model Zebra printer, please consult the manual.

Do not install the label printer on the VBECS Server. Connectivity is configured in VBECS Administrator.

VBECS is configured to work only with Zebra printers: VBECS uses Zebra printing language to communicate with the printer. Other requirements:

Ethernet connectivity: the label printer must have an Ethernet card.
Must print on 4" x 4" label stock
Must print at 300DPI

Prior to configuring the label printer, load the ribbon and label stock and ensure that the printer is on. If the printer does not display PRINTER READY, there is a problem that must be resolved before proceeding. Refer to the Zebra user guide or printer CD for more information.

Set the IP Address on the Printer

Press **SETUP/EXIT** to access the configuration menus.
Press **+** or **–** to scroll through the configuration menu options. Stop when IP PROTOCOL is displayed and press **SELECT**. If there is a prompt for a password, press **–** to change positions and **+** to change numbers. Enter **1234**. Press **SELECT**.
Press **+** to select PERMANENT. Press **SELECT**. The IP address is configured to be static.
Press **+** to navigate to the IP ADDRESS menu option. Press **SELECT**.

Press **+** or **–** to change numbers (as in Step 2) to enter the IP address specified in the Configuration Checklist. Press **SELECT**.
Press **SETUP/EXIT** to save the new configuration. PERMANENT is displayed. Press **SETUP/EXIT** to save the changes.

Test the Printer

To print a label, press and hold the Network Configuration button (on the back of the printer just above the Ethernet socket) until the DATA LED on the front of the printer blinks. Retain the test label for validation records. If the printer configuration on the label print is blank or faint or it is printing off center, adjust the settings.

Adjust Label Darkness

If the printer configuration on the label print is blank or faint, adjust the darkness:

Press **SETUP/EXIT**. Press **+** or **–** until DARKNESS is displayed. Press **SELECT**.
Press **+** to adjust the darkness to a higher number. Press **SELECT**. Move up in small increments: setting the printer to a setting that is too dark may compromise the quality of the labels.
Repeat these steps to retest the printer.
If parts of the label are cut off, adjust the X and Y offsets.
Press **SETUP/EXIT** twice to permanently change the setting.

Adjust Label Offsets

If the printer is printing off center, adjust the X and Y offsets:

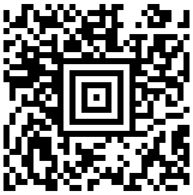
Press **SETUP/EXIT**. Press **+** or **–** until LABEL TOP (if vertical alignment is not correct) or LEFT POSITION (if horizontal alignment is not correct) is displayed. Press **SELECT**.
Press **+** or **–** to adjust the alignment to a higher number. Press **+** in the LABEL TOP menu to move the printing down on the label. Press **+** in the LEFT POSITION menu to move the printing to the right on the label.
Press **SELECT**. Adjust in small increments until the label is centered on the label stock.
Press **SETUP/EXIT** twice to permanently change the setting.

Scanners

Scanners used with VBECS must be able to scan Codabar, ISBT 128, and PDF-417 barcodes. To configure a scanner:

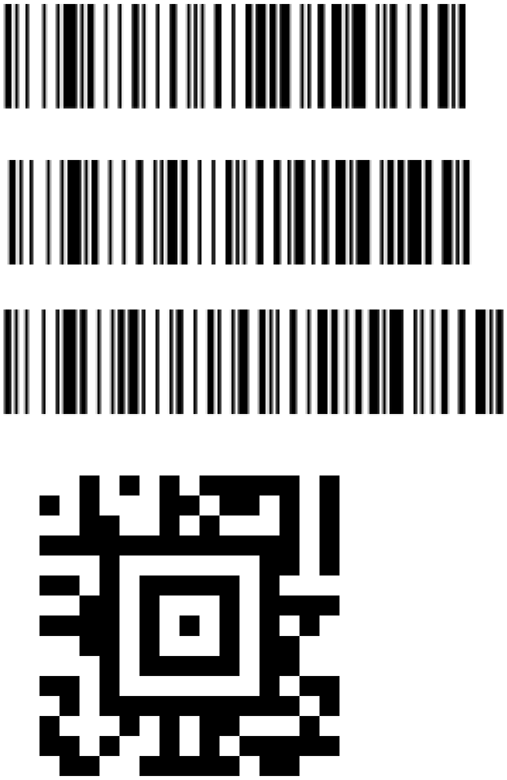
1) Connect the scanner to the workstation.
    a. To configure a **Hand-Held 4600** scanner, scan the barcode in Figure 25.

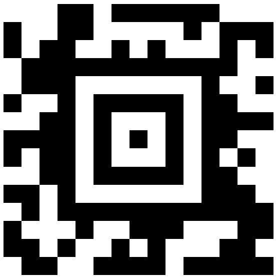
Figure 25: Configuration barcode for a Hand-Held 4600



    b. To configure a **Honeywell Xenon 1900** scanner, scan the series of barcodes in Figure 26.

Figure 26: Configuration barcodes for a Xenon 1900



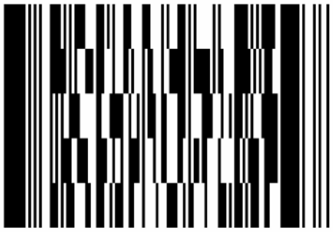


To test the scanner, open Notepad. Print and scan the barcodes in Figure 27, Figure 28, and Figure 29. The Codabar and ISBT barcodes must scan as “~123456789”; the PDF 417 must scan as “~Testing.” Save and print the Notepad file for validation records.

Figure 27: Codabar

Figure 28: ISBT 128

Figure 29: PDF 417



Workstation Configuration

Specifications are as follows:

- Memory: 2GB
- Display: 17”
- Video: video card with 16-bit color and 1024 x 768 resolution
- Operating System: Microsoft Windows 7 Enterprise
- Input Devices: U.S. 101-key keyboard, mouse
- Audio: Sound card and speakers
- Personal Identity Verification (PIV) card reader: required to utilize PIV card access

Implementation and Maintenance (Enterprise Operations Only)

The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations.

Periodic System Maintenance

The VBECS SQL Maintenance jobs run nightly from 10:00 PM to 1:00 AM (CST). Do not reboot the server during this time interval. Doing so may cause consistency and allocation errors.

The system will fail to function as intended when maintenance checks are not performed or are not performed correctly (Table 2).

Table 2: Periodic System Maintenance

Action	Frequency	Description
System Center Operations Manager (SCOM) Alerts	Daily	SCOM emails alert messages to a Server Administrators mail group. Investigate all alerts to completion.
Review Database Integrity Reports	Daily	Take action only upon receipt of a job failure email. See the SQL Maintenance Jobs section for more details.
Apply Windows Updates	2nd Tuesday of the month	See Applying Windows Updates.
VBECS Reports folder cleanup	Annually or as needed	Users are able to export reports to the D:\VBECSReports folder on the App Server. The D drive is 10 GB in size and logs are also stored there. On an annual basis or whenever the folder is over 90% full, old reports must be deleted. This activity must be performed by a server administrator and should be coordinated with blood bank personnel.

SQL Maintenance Jobs

The VBECS databases are contained within Microsoft SQL Server and require regular maintenance jobs to backup, validate integrity, and improve performance. The jobs are automated and configured to run according to the specifications shown in Table 3, Table 4 and Table 5.

System Level Jobs: Each system level job executes against all databases found on the SQL system not contained in an Availability Group. Email alerts are sent to *VAOITVBECSSQLSupport@va.gov*.

Table 3: System Level Jobs

Databases Affected	Job Name	Start Time
All databases not in an Availability Group	System_IntegrityCheck	10:00pm
All databases not in an Availability Group (except TempDB)	System_FullBackups	11:00pm
n/a	System_ResetServerLog	Every Saturday at 12:00am

Availability Group Level Jobs: Each Availability Group level job executes against all VBECS databases found within the Availability Group indicated by the job name (Table 4). Email alerts are sent to the recipients defined in the targeted database's CPRS interface (see SQL Maintenance Job Alerts section).

Table 4: Availability Group Level Jobs

Databases Affected	Job Name	Start Time
All VBECS databases in the Availability Group AGVISN*XX (XX is equal to the VISN number)*	AGVISN*XX*_DifferentialBackups	Every 6 hours between 3:00am and 10:00pm
	AGVISN*XX*_TransactionalLogBackups	Every 2 hours between 2:00am and 11:00pm
	AGVISN*XX*_ReIndexTables	10:00pm
	AGVISN*XX*_UpdateStats	10:30pm
	AGVISN*XX*_IntegrityCheck	11:30pm
	AGVISN*XX*_FullBackups	12:15am

VBECS Level Jobs: Each VBECS level job targets a single VBECS database indicated in the job name (Table 5). These jobs affect user data by expiring Component and Test Orders and marking units Presumed Transfused. Email alerts are sent to the recipients defined in the targeted database's CPRS interface (see SQL Maintenance Job Alerts section). Site codes are unique per site and listings of assigned codes are located in Appendix G: VBECS Production Site Codes.

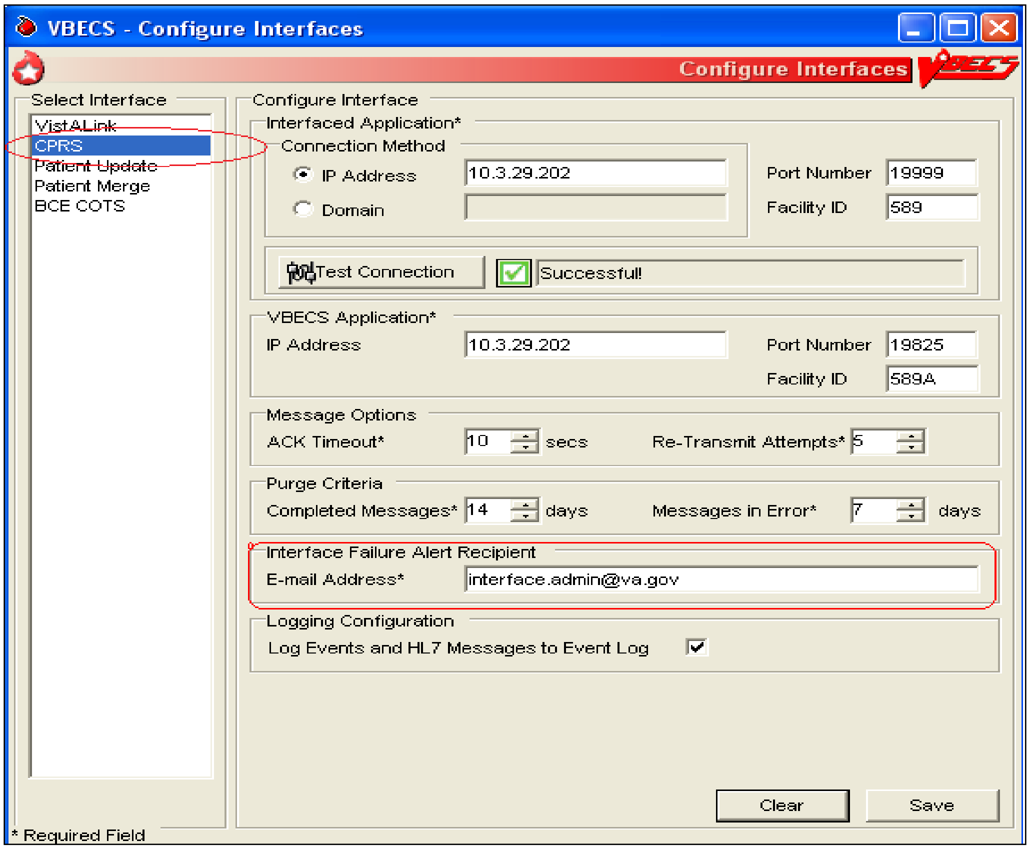
Table 5: VBECS Level Jobs

Databases Affected	Job Name	Start Time
(Test SQL Server) VBECS_*SSS*_TEST (SSS is equal to the Site Code)	AGVISN*XX*_VBECS_*SSS*_TEST_Background_Jobs	12:01am
(Production SQL Server) VBECS_*SSS*_PROD	AGVISN*XX*_VBECS_*SSS*_PROD_Background_Jobs	

SQL Maintenance Job Alerts

Email alert messages are sent only when a SQL maintenance job fails. System Level job alerts are sent to *VAOITVBECSSQLSupport@va.gov* and EOVBEDatabaseAdministration@va.gov. The Availability Group and VBECS level job alerts use the email address entered in the **Interface Failure Alert Recipient** field of the CPRS interface (VBECS Administrator software; see Figure 30).

Figure 30: Example of Setting SQL Maintenance Job Alert Recipients



VBECS - Configure Interfaces

Configure Interfaces

Select Interface
- VistALink
- CPRS
- Patient Update
- Patient Merge
- BCE COTS

Configure Interface

Interfaced Application*

Connection Method
- ● IP Address: 10.3.29.202
- ○ Domain:

Port Number: 19999
Facility ID: 589

Test Connection ✓ Successful!

VBECS Application*

IP Address: 10.3.29.202
Port Number: 19825
Facility ID: 589A

Message Options

ACK Timeout*: 10 secs
Re-Transmit Attempts*: 5

Purge Criteria

Completed Messages*: 14 days
Messages in Error*: 7 days

Interface Failure Alert Recipient

E-mail Address*: interface.admin@va.gov

Logging Configuration

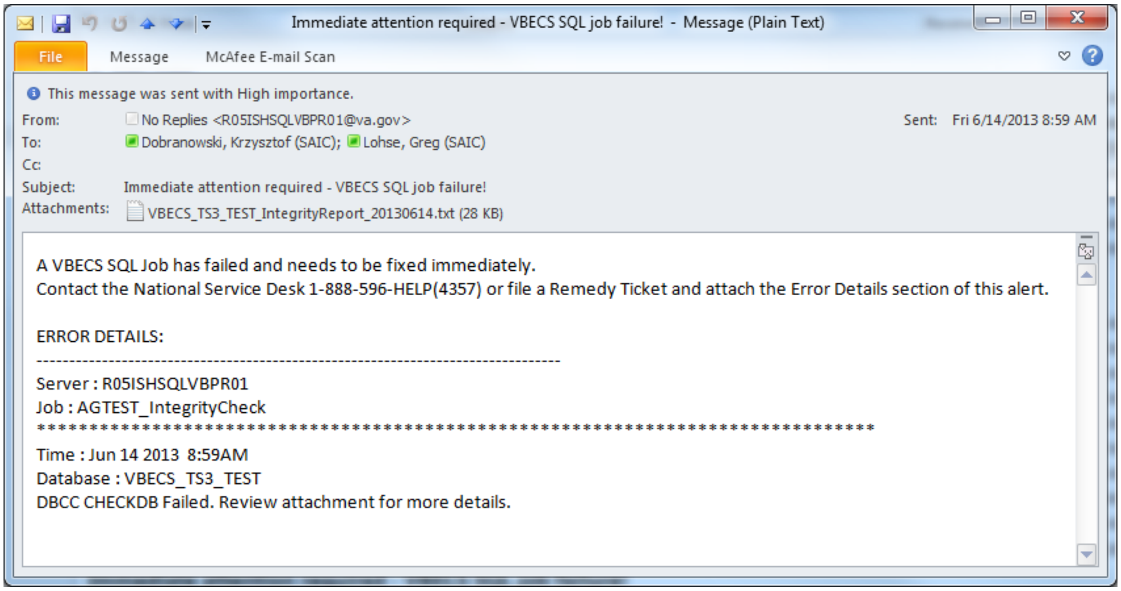
Log Events and HL7 Messages to Event Log ☑

Clear | Save

* Required Field

SQL maintenance job alerts are marked with High Importance and must be acted upon immediately. The email will contain details of the failure and instructions for contacting support to correct the issue. When a SQL integrity job fails, a report will be included as an attachment with the alert – include this with any support ticket (Service Desk Primary Contact) or communication (Figure 31).

Figure 31: Example of a SQL Maintenance Job Failure Email



Immediate attention required - VBECS SQL job failure! - Message (Plain Text)
File
Message
McAfee E-mail Scan

This message was sent with High importance.

From: No Replies <R05ISHSQLVBPR01@va.gov>

Sent: Fri 6/14/2013 8:59 AM

To: Dobranowski, Krzysztof (SAIC); Lohse, Greg (SAIC)

Cc:

Subject: Immediate attention required - VBECS SQL job failure!

Attachments: VBECS_TS3_TEST_IntegrityReport_20130614.txt (28 KB)

```
A VBECS SQL Job has failed and needs to be fixed immediately.
Contact the National Service Desk 1-888-596-HELP(4357) or file a Remedy Ticket and attach the Error Details section of this alert.

ERROR DETAILS:
--------------------------------------------------------------------------------
Server : R05ISHSQLVBPR01
Job : AGTEST_IntegrityCheck
********************************************************************************
Time : Jun 14 2013  8:59AM
Database : VBECS_TS3_TEST
DBCC CHECKDB Failed. Review attachment for more details.
```

SQL Database Backups

To assist recovery and support options, database backup files and integrity reports are retained for 7 days for each SQL database and can be found on the SQL Server at **H:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup**. If tape or offsite backups are desired, locate and backup the folders associated with the 3-character site code (*SSS*). For example, on a production SQL server, Hines ("HIN" site code) would backup the VBECS_HIN_PROD and VBECS_HIN_PROD_MIRROR folders.

Applying Windows Updates

The VistA Blood Establishment Computer Software (VBECS) systems are updated with Microsoft Windows Security patches by Austin Information Technology Center (AITC) staff during defined maintenance periods (Table 6, Table 7 and Table 8). The monthly maintenance schedule begins the second Tuesday of the month that Microsoft defines as patch Tuesday.

1) Enterprise Operations installs Windows Updates patches to VBECS maintenance team pre-production servers.
2) VBECS maintenance team tests the patched pre-production servers and proves that the updates do not affect VBECS.
3) After the VBECS team approves the updates, Enterprise Operations creates change orders for the customer-test system and another for the production system.

4) Enterprise Operations will submit an ANR and then install the patches, using the approved schedule, on the customer-test systems.
5) Enterprise Operations will submit an ANR and then install the patches, using the approved schedule, on the production systems.

Table 6: Pre-Production Patch Schedule

Server	Day
VAAUSVBEAPP7AUS, VAAUSVBEPRD200, VAAUSVBEPRD201 (Application Server)	2 days after patch Tuesday, 6-8 PM CST (automatic with notification)
SQL Server, Disaster Recovery node	3 days after patch Tuesday, 8-9 AM CST (manual)
SQL Server, High Availability node	3 days after patch Tuesday, 9-10 AM CST (manual)
SQL Server, Primary node	3 days after patch Tuesday, 10-11 AM CST (manual)

Table 7: Customer Test System Patch Schedule

Server	Day
SQL Server, Disaster Recovery node	8 days after patch Tuesday, 8-9 AM CST (manual)
SQL Server, High Availability node	8 days after patch Tuesday, 9-10 AM CST (manual)
SQL Server, Primary node	8 days after patch Tuesday, 10-11 AM CST (manual)

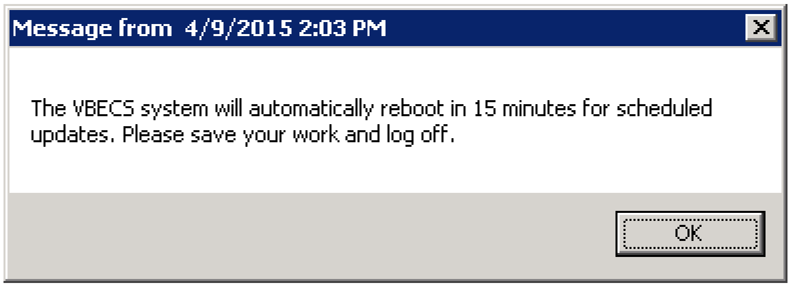
Table 8: Production System Patch Schedule

Server	Day
Application Servers	8 days after patch Tuesday, 10 AM local time (automatic with notification)
SQL Server, Disaster Recovery node	10 days after patch Tuesday, 9-10 AM CST (manual)
SQL Server, High Availability node	10 days after patch Tuesday, 10-11 AM CST (manual)
SQL Server, Primary node	10 days after patch Tuesday, 11-12 PM CST (manual)

The App Servers are updated differently than the SQL Servers:

- **App Servers**: The App Servers are updated and rebooted by an automated process at 10:00am local time on the Wednesday following the week of patch release. VBECS users connected to the server receive a warning at the following time intervals: 15 minutes, 10, 5, 4, 3, 2 and 1 (Figure 32).
- If the App Server is not operational by 10:15AM local time, contact the Service Desk.

Figure 32: Example of Server Restart Warning



Message from 4/9/2015 2:03 PM

The VBECS system will automatically reboot in 15 minutes for scheduled updates. Please save your work and log off.

- **SQL Servers**: Due to clustering, the SQL Servers require manual update. The manual process is described in the *Applying Updates to VBECS SQL Server System* section.

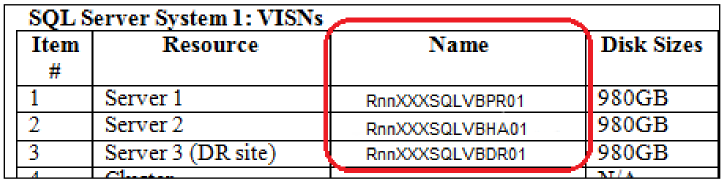
Applying Updates to VBECS SQL Server System

Each VBECS SQL Server system is comprised of three servers that are setup for redundancy with the use of Windows Failover Clustering and the Microsoft SQL AlwaysOn technology:

- Server 1: referred to as the Primary server
- Server 2: local secondary server, referred to as the High Availability (HA) server
- Server 3: remote secondary server, referred to as the Disaster Recovery (DR) server

The names of the VBECS SQL servers can be found on the Data Center Worksheet (Figure 33).

Figure 33: Example Data Center Worksheet



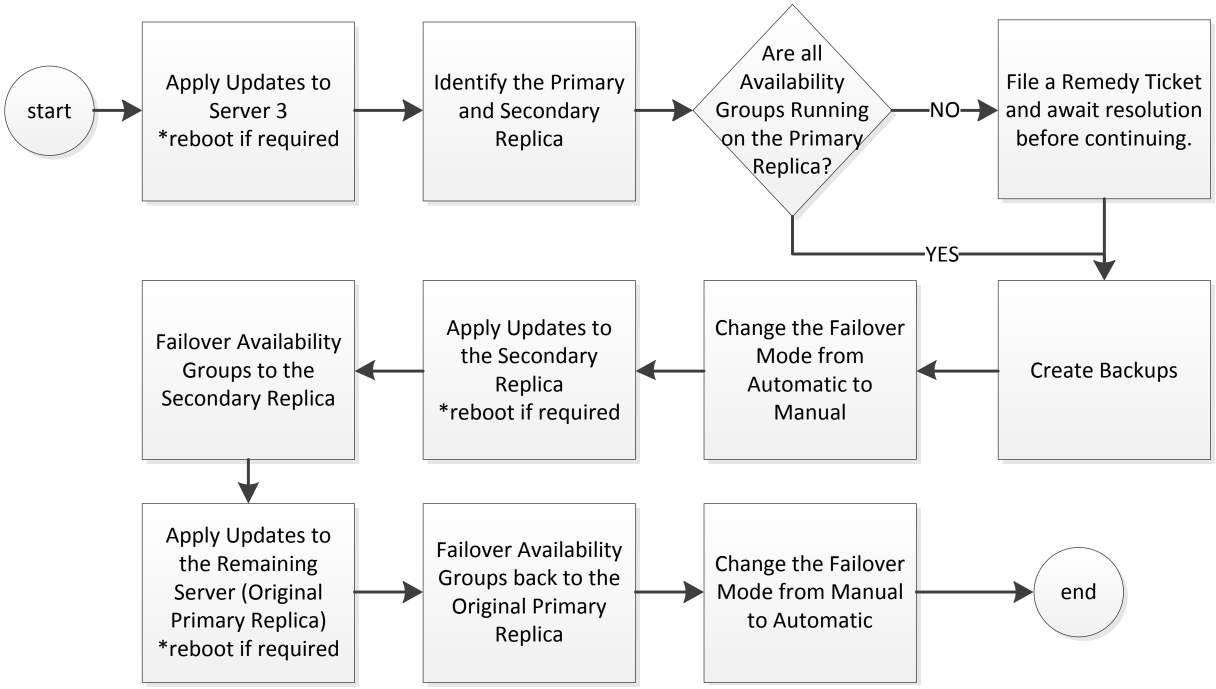
SQL Server System 1: VISNs

Item #	Resource	Name	Disk Sizes
1	Server 1	RnnXXXSQLVBPR01	980GB
2	Server 2	RnnXXXSQLVBHA01	980GB
3	Server 3 (DR site)	RnnXXXSQLVBDR01	980GB
4	Cluster		N/A

Failure to adhere to these instructions could result in data loss and/or system failure. Always apply updates to Server 3 first and the Primary Replica last.

When updating a VBECS SQL Server system, refer to the flowchart in Figure 34 for the proper execution order.

Figure 34: Updating a VBECS SQL Server System Process Flow


start
Apply Updates to Server 3 *reboot if required
Identify the Primary and Secondary Replica
Are all Availability Groups Running on the Primary Replica?
NO
File a Remedy Ticket and await resolution before continuing.
YES
Create Backups
Change the Failover Mode from Automatic to Manual
Apply Updates to the Secondary Replica *reboot if required
Failover Availability Groups to the Secondary Replica
Apply Updates to the Remaining Server (Original Primary Replica) *reboot if required
Failover Availability Groups back to the Original Primary Replica
Change the Failover Mode from Manual to Automatic
end

Failover is a term used to describe the process of changing which server in a SQL AlwaysOn configuration is designated as the Primary Replica. Never use the following instructions to failover to Server 3 (DR Server). Instructions for forcing a failover to Server 3 are provided in the VBECS Disaster and Recovery guide.

A Server Administrator should only initiate manual failover when client usage of the system is minimal. Users may briefly lose VBECS database connectivity depending on how long the failover takes.

Apply Updates to Server 3

1) Open a remote desktop connection to Server 3 of the VBECS SQL Server system.
2) Apply the Windows/Software Updates using the supplied instructions for the updates (reboot Server 3 only if instructed).

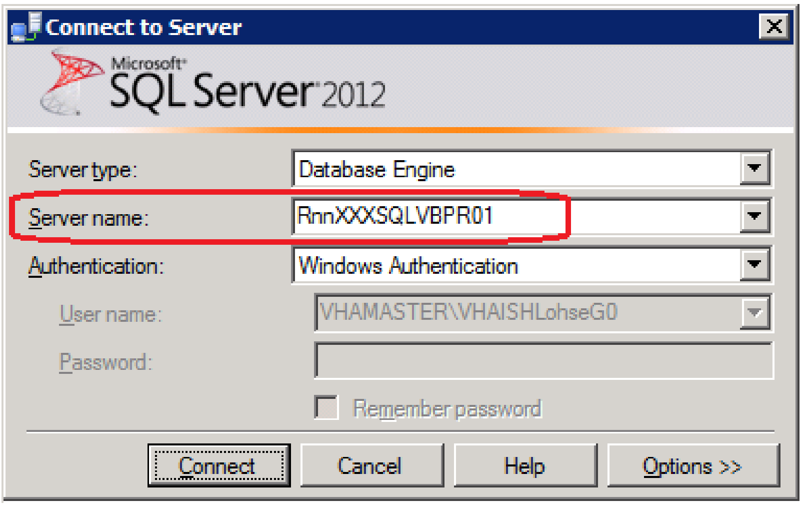
Replica is another name for a server within a SQL Server AlwaysOn configuration.

Identify the Primary and Secondary Replica

3) Open a remote desktop connection to Server 1 of the VBECS SQL Server system. On the Start menu, click **All Programs, Microsoft SQL Server 2012, SQL Server Management Studio**.

4) When prompted to connect to a server, enter the name of Server 1 in the **Server Name** field and click **Connect** (Figure 35). Note: VBECS Test system SQL Servers are named differently than production SQL servers.

Figure 35: Example of the Connect to SQL Server Window



Server type: Database Engine

Server name: RnnXXXSQLVBPR01

Authentication: Windows Authentication

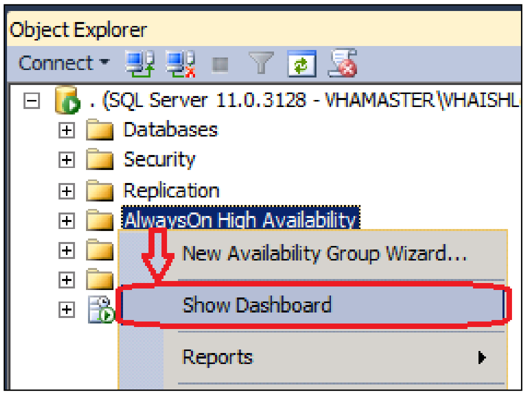
User name: VHAMASTER\VHAISHLohseG0

Password:

□ Remember password

5) On the left side of the SQL Server Management Studio (SSMS) screen is the Object Explorer pane. Within the Object Explorer pane, right-click on the **AlwaysOn High Availability** folder and select **Show Dashboard** (Figure 36).

Figure 36: Example of Launching the SQL Dashboard



Object Explorer
Connect
. (SQL Server 11.0.3128 - VHAMASTER\VHAISHL
Databases
Security
Replication
AlwaysOn High Availability
New Availability Group Wizard...
Show Dashboard
Reports

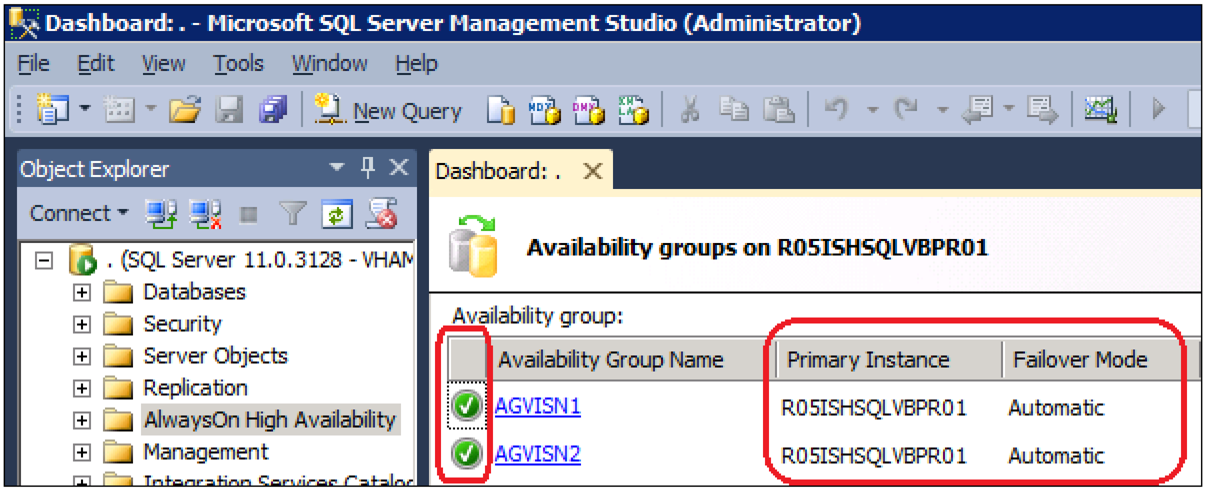
6) A Dashboard tab (Figure 37) displays the Primary Instance and Failover Mode of the VBECS SQL Availability Groups (AG). Each AG has one of the following status indicator icons:

✓: your SSMS is connected to the AG's Primary Instance server (i.e., the Primary Replica)

○: your SSMS is not connected to the AG's Primary Instance server

✖: there is a severe issue with the AG

Figure 37: Example of the SQL Server Dashboard



Dashboard: . - Microsoft SQL Server Management Studio (Administrator)

Availability groups on R05ISHSQLVBPR01

Availability group:

	Availability Group Name	Primary Instance	Failover Mode
✓	AGVISN1	R05ISHSQLVBPR01	Automatic
✓	AGVISN2	R05ISHSQLVBPR01	Automatic

If any Availability Group status indicators are ✖ or if there are a mix of ✓ and ○ indicators, VBECS is down and the problem must be resolved immediately.

7) If all of the indicators are ○, close SSMS. Restart at Step 3 connecting to the server listed in the Primary Instance column.

8) Make a note of the Primary and Secondary Replicas (i.e., if Server 1 is the Primary Replica, then Server 2 is the Secondary Replica and visa-versa).

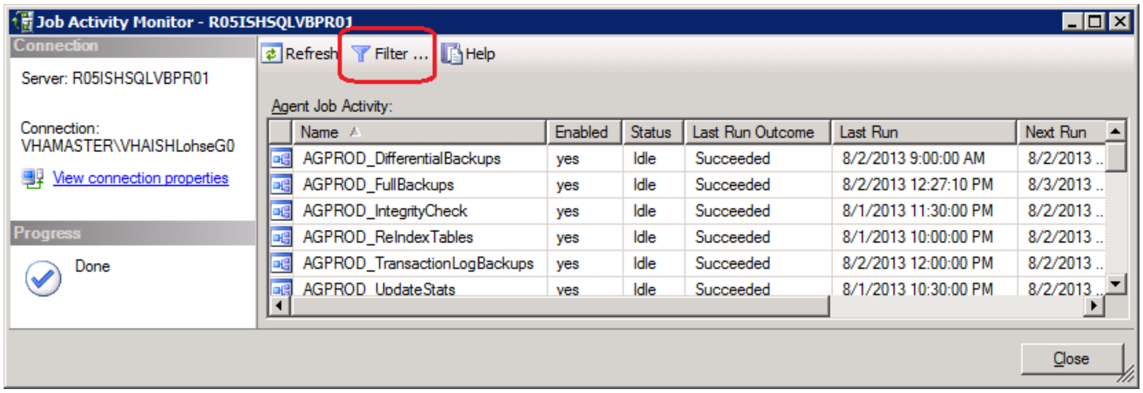
Create Backups

9) Now that all of the AGs are running under the Primary Replica, navigate to and expand the **SQL Server Agent, Jobs** folder in the Object Explorer pane.

10) Double-click on **Job Activity Monitor**.

11) In the Job Activity window, click the Filter ... button (Figure 38).

Figure 38: Example of Job Activity Monitor



Job Activity Monitor - R05ISHSQLVBPR01

Connection

Server: R05ISHSQLVBPR01

Connection:
VHAMASTER\VHAISHLohseG0

View connection properties

Progress

Done

Refresh Filter ... Help

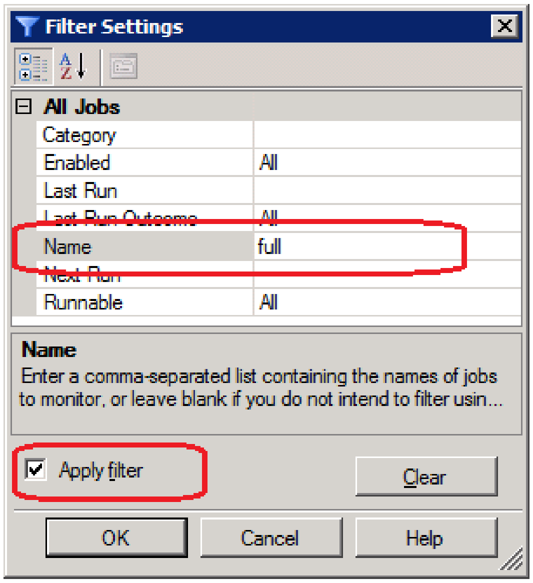
Agent Job Activity:

Name	Enabled	Status	Last Run Outcome	Last Run	Next Run
AGPROD_DifferentialBackups	yes	Idle	Succeeded	8/2/2013 9:00:00 AM	8/2/2013 ..
AGPROD_FullBackups	yes	Idle	Succeeded	8/2/2013 12:27:10 PM	8/3/2013 ..
AGPROD_IntegrityCheck	yes	Idle	Succeeded	8/1/2013 11:30:00 PM	8/2/2013 ..
AGPROD_ReIndexTables	yes	Idle	Succeeded	8/1/2013 10:00:00 PM	8/2/2013 ..
AGPROD_TransactionLogBackups	yes	Idle	Succeeded	8/2/2013 12:00:00 PM	8/2/2013 ..
AGPROD_UpdateStats	yes	Idle	Succeeded	8/1/2013 10:30:00 PM	8/2/2013 ..

Close

12) In the Filter Settings window, enter **full** in the **Name** field, check the **Apply filter** box and click **OK** (Figure 39).

Figure 39: Filter Settings



Filter Settings

All Jobs	
Category	
Enabled	All
Last Run	
Last Run Outcome	All
Name	full
Next Run	
Runnable	All

Name
Enter a comma-separated list containing the names of jobs to monitor, or leave blank if you do not intend to filter usin...

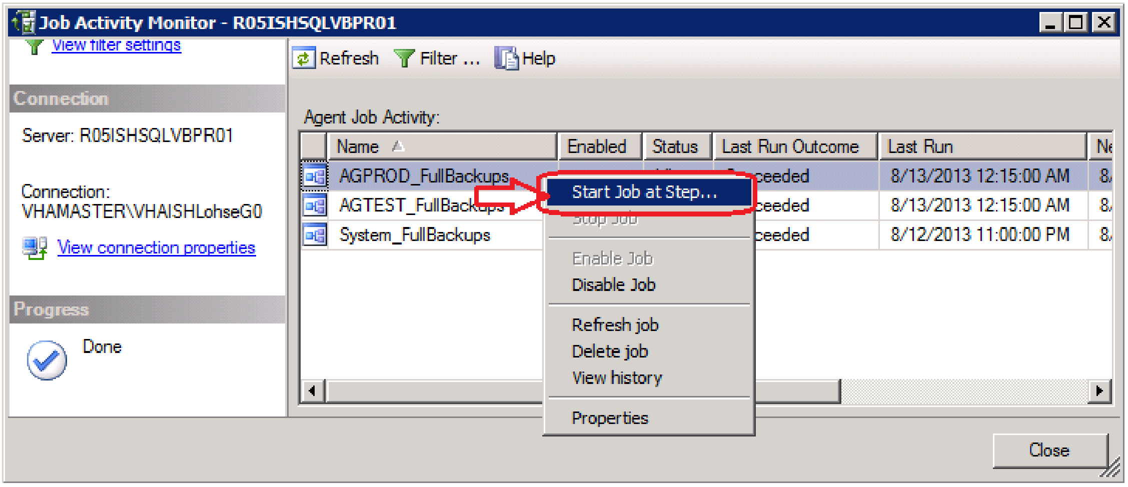
☑ Apply filter

Clear

OK Cancel Help

13) Right-click the first job in the filtered list and select **Start Job at Step…** (Figure 40).

Figure 40: Example Starting a SQL Job



Server: R05ISHSQLVBPR01

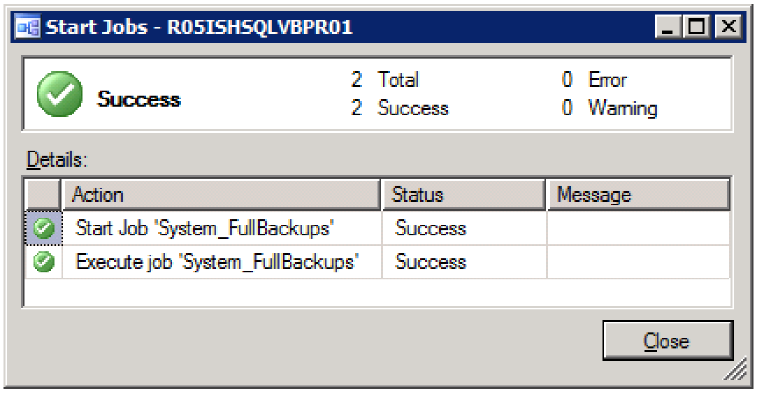
Connection:
VHAMASTER\VHAISHLohseG0

Agent Job Activity:

Name	Enabled	Status	Last Run Outcome	Last Run	Ne
AGPROD_FullBackups			ceeded	8/13/2013 12:15:00 AM	8/
AGTEST_FullBackups			ceeded	8/13/2013 12:15:00 AM	8/
System_FullBackups			ceeded	8/12/2013 11:00:00 PM	8/

14) Wait for the job to finish (Figure 41). Verify the status indicator is **Success** before clicking **Close**.

Figure 41: Example Job Completion Message



Success

2 Total
2 Success
0 Error
0 Warning

Details:

Action	Status	Message
Start Job 'System_FullBackups'	Success	
Execute job 'System_FullBackups'	Success	

15) Repeat Steps 13 and 14 for each job in the list.

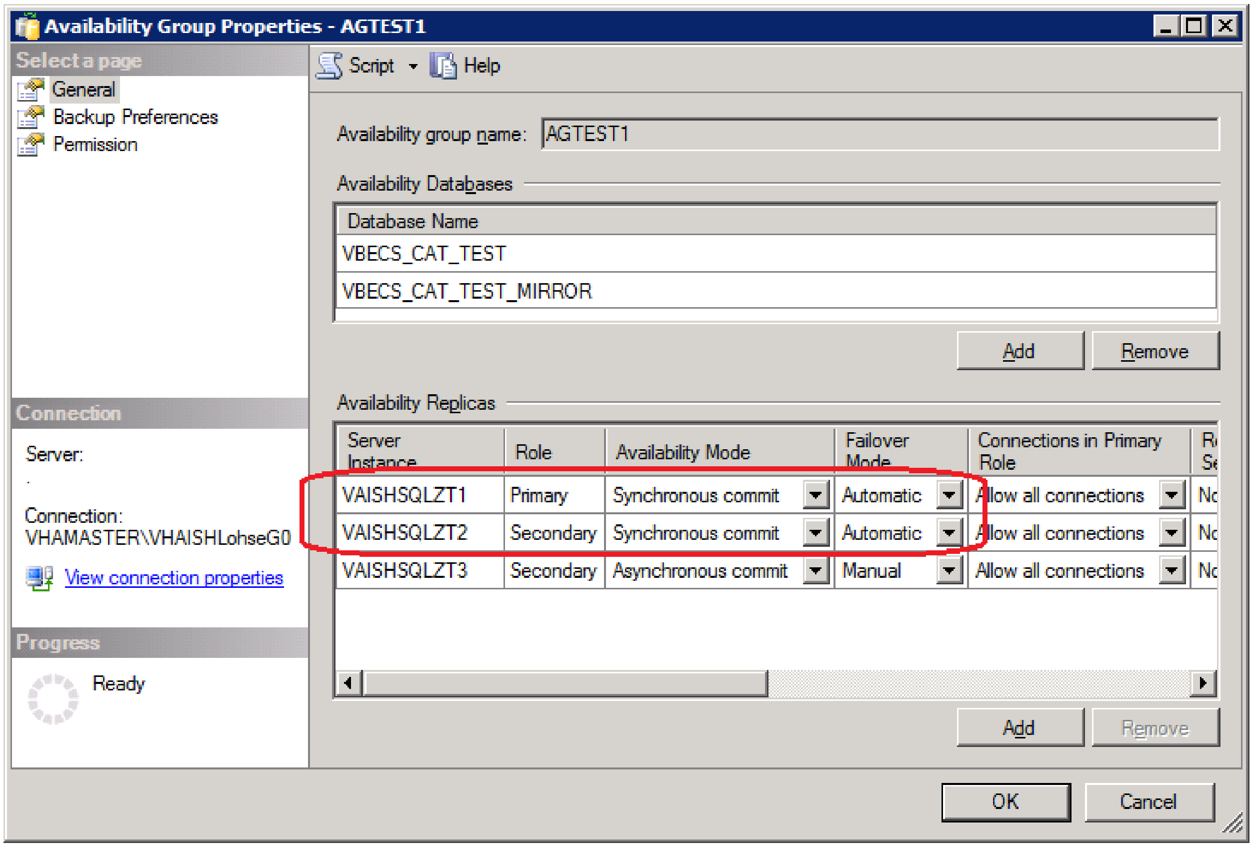
> *If any of the jobs fail to complete successfully, please notify the appropriate support personnel immediately.*

16) Click **Close** on the Job Activity Monitor window.

Change the Failover Mode from Automatic to Manual

17) In the Object Explorer pane, navigate to and expand the **AlwaysOn High Availability**, **Availability Groups** folder**.**
18) Right-click on the first AG and select **Properties**; the Availability Group Properties window opens.
19) Locate the two servers with an Availability Mode of **Synchronous commit** (Figure 42). Change both **Failover Mode** cells from Automatic to **Manual** and click **OK**. If the fields are greyed-out, you are not connected to the Primary Replica: close SSMS, logoff the server and restart at Step 3.

Figure 42: Example of the Availability Group Properties



Availability group name: AGTEST1

Availability Databases

Database Name
VBECS_CAT_TEST
VBECS_CAT_TEST_MIRROR

Availability Replicas

Server Instance	Role	Availability Mode	Failover Mode	Connections in Primary Role	R Se
VAISHSQLZT1	Primary	Synchronous commit	Automatic	Allow all connections	No
VAISHSQLZT2	Secondary	Synchronous commit	Automatic	Allow all connections	No
VAISHSQLZT3	Secondary	Asynchronous commit	Manual	Allow all connections	No

Server:
.

Connection:
VHAMASTER\VHAISHLohseG0

Ready

20) Repeat Steps 18 and 19 for each AG on the server until each has their **Failover Mode** set to **Manual**.
21) Close SSMS.

> *To prevent an unintentional automatic failover during the upgrade process, the Failover Mode must be set to Manual on each replica before performing a Manual Failover of the Availability Groups.*

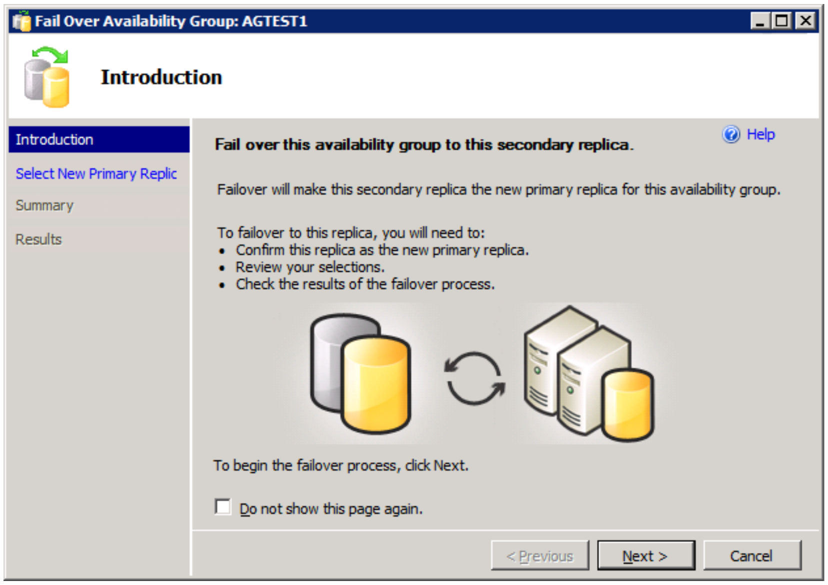
Apply Updates to the Secondary Replica

22) Open a remote desktop connection to the Secondary Replica identified in Step 8 of the VBECS SQL Server system.
23) Apply the Windows/Software Updates using the supplied instructions for the updates (reboot the server only if instructed).

Failover the Availability Groups to the Secondary Replica

24) Open SSMS and connect to the Secondary Replica noted in Step 8.
25) Inside the Object Explorer pane, navigate to and expand the **AlwaysOn High Availability**, **Availability Groups** folder**.**
26) Right-click on the first AG and select **Failover…**; an Availability Group Failover wizard starts.
27) Click **Next** (Figure 43).

Figure 43: Example of the Availability Group Failover Wizard



Fail Over Availability Group: AGTEST1

Introduction

Fail over this availability group to this secondary replica.

Failover will make this secondary replica the new primary replica for this availability group.

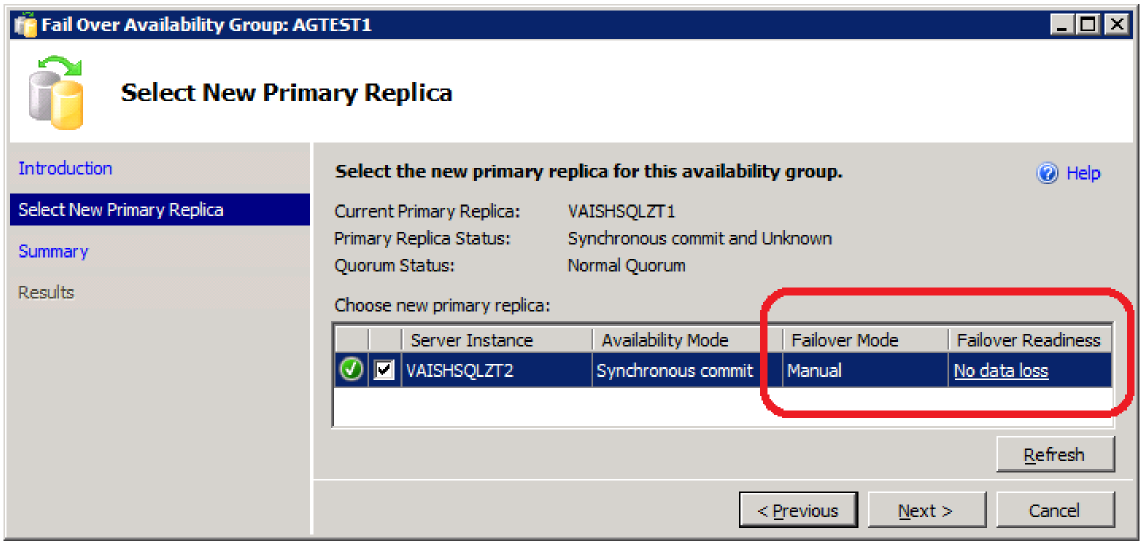
To failover to this replica, you will need to:
- Confirm this replica as the new primary replica.
- Review your selections.
- Check the results of the failover process.

To begin the failover process, click Next.

□ Do not show this page again.

28) Verify the Failover Mode is **Manual** and Failover Readiness is **No data loss**. Click **Next** (Figure 44). Note: If two servers appear in the list, then you are connected to the Primary Replica. Click **Cancel** and close SSMS. Restart at Step 24.

Figure 44: Example of Selecting the New Primary Replica



Fail Over Availability Group: AGTEST1

Select New Primary Replica

Select the new primary replica for this availability group.

Current Primary Replica: VAISHSQLZT1
Primary Replica Status: Synchronous commit and Unknown
Quorum Status: Normal Quorum

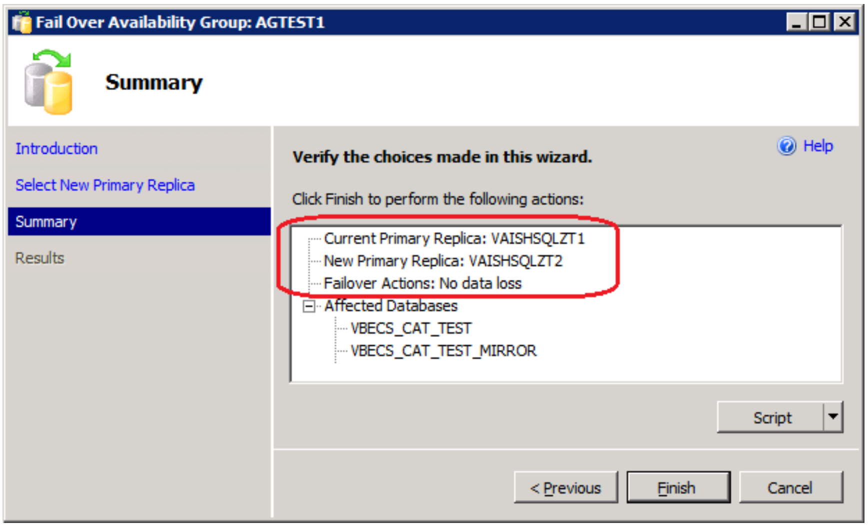
Choose new primary replica:

		Server Instance	Availability Mode	Failover Mode	Failover Readiness
✓	☑	VAISHSQLZT2	Synchronous commit	Manual	No data loss

*If the Failover Readiness field is not in a state of **No data loss**, notify SQL Server support personnel immediately*.

29) A Summary window is displayed (Figure 45). If any of the field values are incorrect (Failover Actions must be No data loss), click **Cancel** and close SSMS. Restart at Step 24.

Figure 45: Example of Availability Group Failover Wizard Summary



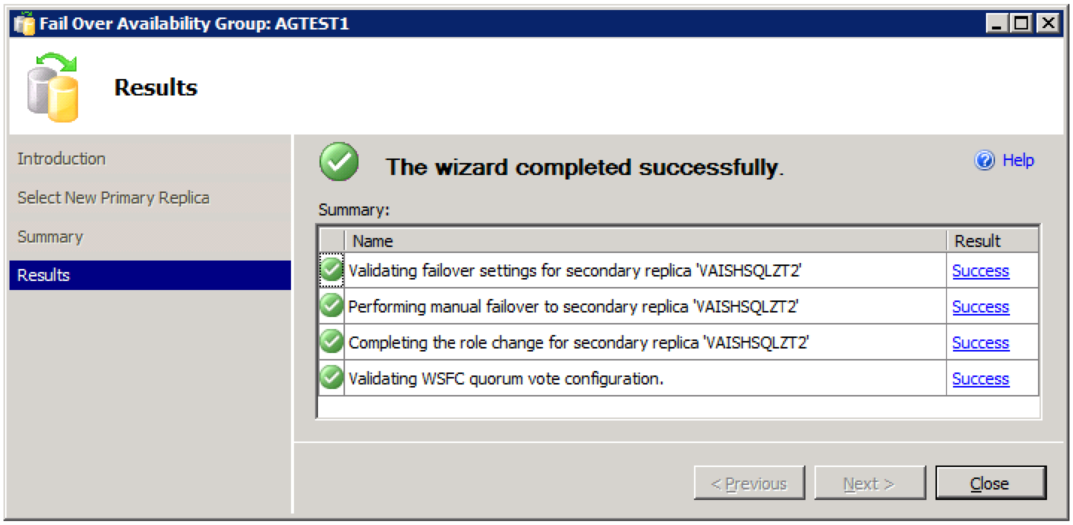
Verify the choices made in this wizard.

Click Finish to perform the following actions:

- Current Primary Replica: VAISHSQLZT1
- New Primary Replica: VAISHSQLZT2
- Failover Actions: No data loss
- Affected Databases
  - VBECS_CAT_TEST
  - VBECS_CAT_TEST_MIRROR

30) Click **Finish** to initiate the failover.
31) A failover may take several minutes to complete. Click **Close** (Figure 46).

Figure 46: Example of Successful Failover Wizard


Fail Over Availability Group: AGTEST1
Results
Introduction
Select New Primary Replica
Summary
Results
Help
< Previous
Next >
Close

The wizard completed successfully.

Summary:

Name	Result
Validating failover settings for secondary replica 'VAISHSQLZT2'	Success
Performing manual failover to secondary replica 'VAISHSQLZT2'	Success
Completing the role change for secondary replica 'VAISHSQLZT2'	Success
Validating WSFC quorum vote configuration.	Success

If any of the Results indicate Error, Warning or Failure, contact SQL Server support personnel. Databases contained in the problem Availability Group will not be available for use until the problem is resolved.

32) Repeat Steps 26 through 31 for each AG on the server.
33) Close SSMS.

Apply Updates to the Remaining Server (Original Primary Replica)

34) Open a remote desktop connection to the Original Primary Replica (identified in Step 8) of the VBECS SQL Server system.
35) Apply the Windows/Software Updates using the supplied instructions for the updates (reboot the server only if instructed).

Failover the Availability Groups Back to the Original Primary Replica

36) Open SSMS and connect to the Primary Replica noted in Step 8.
37) Inside the Object Explorer pane, navigate to and expand the **AlwaysOn High Availability**, **Availability Groups** folder**.**
38) Right-click on the first AG and select **Failover…**; an Availability Group Failover wizard starts. Click **Next** (Figure 43).
39) Verify the Failover Mode is **Manual** and Failover Readiness is **No data loss**. Click **Next** (Figure 44). If two servers appear in the list, then you are connected to the Secondary Replica. Click **Cancel** and close SSMS. Restart at Step 36.

> *If the Failover Readiness field is anything other than **No data loss**, contact SQL Server support personnel.*

40) A Summary window is displayed (Figure 45). If any of the field values are incorrect (Failover Actions must be No data loss), click **Cancel** and close SSMS. Restart at Step 36.
41) Click **Finish** to initiate the failover.
42) The failover may take several minutes to complete. Click **Close** (Figure 46).

> *If any of the Results indicate Error, Warning or Failure. Databases contained in the problem, contact SQL Server support personnel. Availability Group will not be available for use until the problem is resolved.*

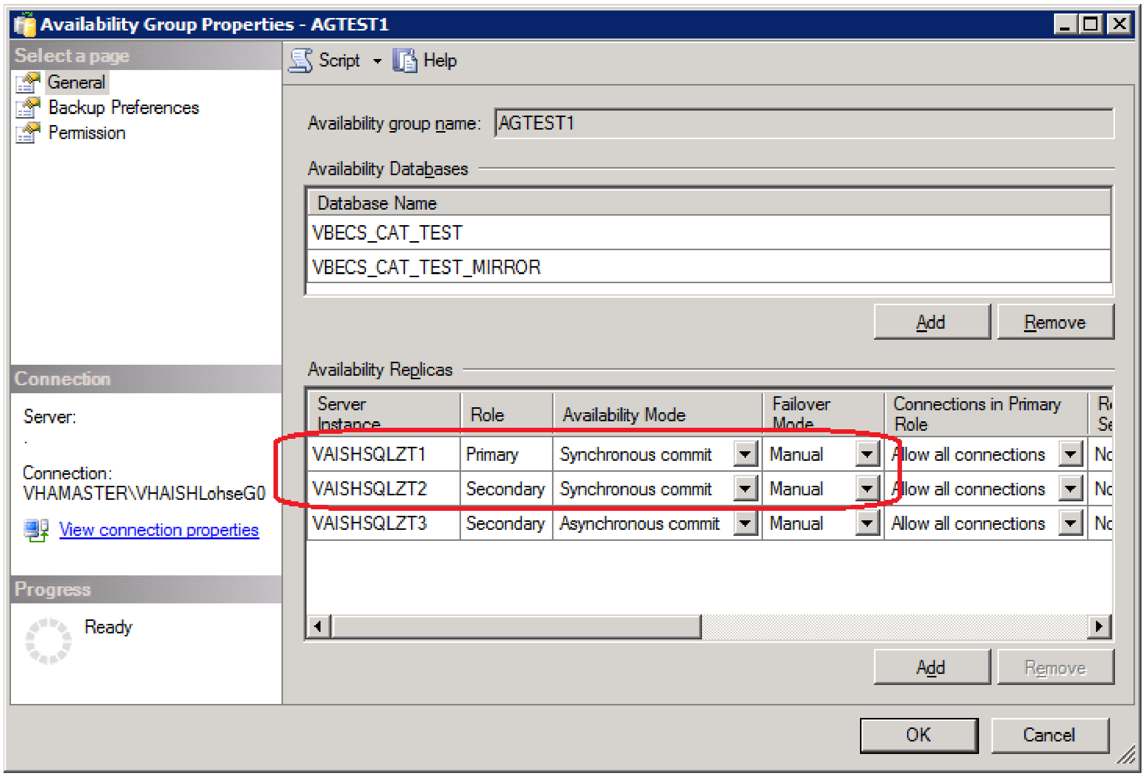
43) Repeat Steps 28 through 42 for each AG on the server.

Change the Failover Mode from Manual to Automatic

44) Right-click on the first AG and select **Properties**; the Availability Group Properties window open.

45) Locate the two servers with an Availability Mode of **Synchronous commit** (Figure 47). Change both **Failover Mode** cells from **Manual** to **Automatic** and click **OK**.

Figure 47: Example of the Availability Group Properties



Availability group name: AGTEST1

Availability Databases

Database Name
VBECS_CAT_TEST
VBECS_CAT_TEST_MIRROR

Availability Replicas

Server Instance	Role	Availability Mode	Failover Mode	Connections in Primary Role	Re Se
VAISHSQLZT1	Primary	Synchronous commit	Manual	Allow all connections	No
VAISHSQLZT2	Secondary	Synchronous commit	Manual	Allow all connections	No
VAISHSQLZT3	Secondary	Asynchronous commit	Manual	Allow all connections	No

Server:
.

Connection:
VHAMASTER\VHAISHLohseG0

Ready

46) Repeat Steps 44 and 45 for each AG on the server until each has their **Failover Mode** set to **Automatic**.

47) Close SSMS and log off the server.

ePolicy and Virus Definitions

Virus definitions are automatically updated on the VBECS system. The VBECS maintenance team monitors the releases.

Do not change the system! The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations. Adding to or updating VBECS software without permission is prohibited.

VistA Maintenance Operations

Four HL7 Logical Links and one VistALink connection must be established and configured to establish proper communication with VBECS. The HL7 links are OERR-VBECS, VBECS-OERR, VBECSPTU, and VBECSPTM. The VistALink connection configuration is the data that VistA will use to transmit data in XML format to VBECS. The following set of instructions will aid in the proper configuration of these links, and ensure reliable communication between VistA and VBECS. These links must be configured during the initial installation of VBECS, and after any changes to the HL7 or VistALink configuration on VBECS. The settings should also be updated after the VistA Test account has been remirrored.

Set Up VBECS Outbound Logical Links

1) At the “Select HL7 Main Menu Option:” prompt, enter **Filer**.
2) Shut down the logical link.
3) At the “Select Filer and Link Management Options Option:” prompt, enter **Link Edit**.
4) At the “Select HL LOGICAL LINK NODE:” prompt, enter **OERR-VBECS** (Figure 48).

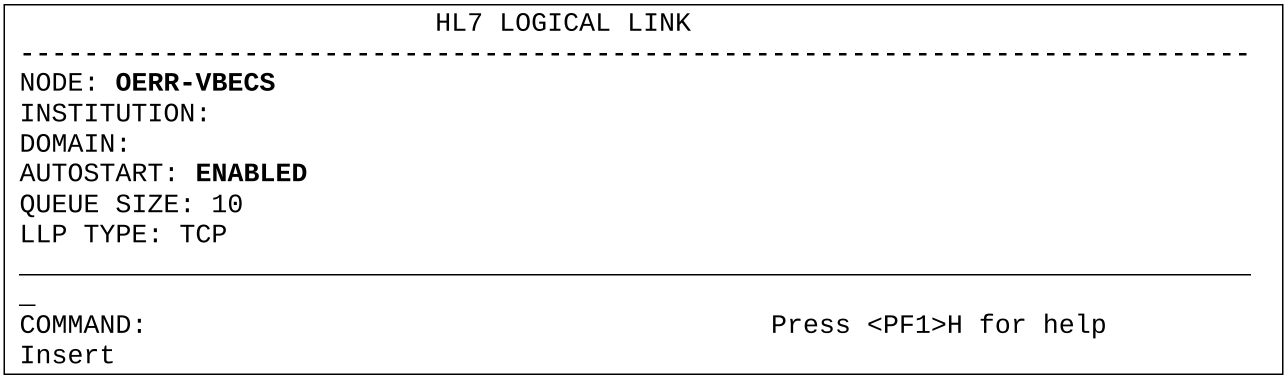
Figure 48: HL7 Logical Link Edit Menu Navigation

```
HL7 Main Menu
   Event monitoring menu ...
   Systems Link Monitor
   Filer and Link Management Options ...
   Message Management Options ...
   Interface Developer Options ...
   Site Parameter Edit

Select HL7 Main Menu Option: FILER

   SM     Systems Link Monitor
   FM     Monitor, Start, Stop Filers
   LM     TCP Link Manager Start/Stop
   SA     Stop All Messaging Background Processes
   RA     Restart/Start All Links and Filers
   DF     Default Filers Startup
   SL     Start/Stop Links
   PI     Ping (TCP Only)
   ED     Link Edit
   ER     Link Errors ...

Select Filer and Link Management Options Option: ED

Select HL LOGICAL LINK NODE: OERR-VBECS
```

5) Enter **Enabled** in the AUTOSTART field (Figure 49).

6) Move the cursor to the LLP TYPE field and press **Enter** (Figure 49).

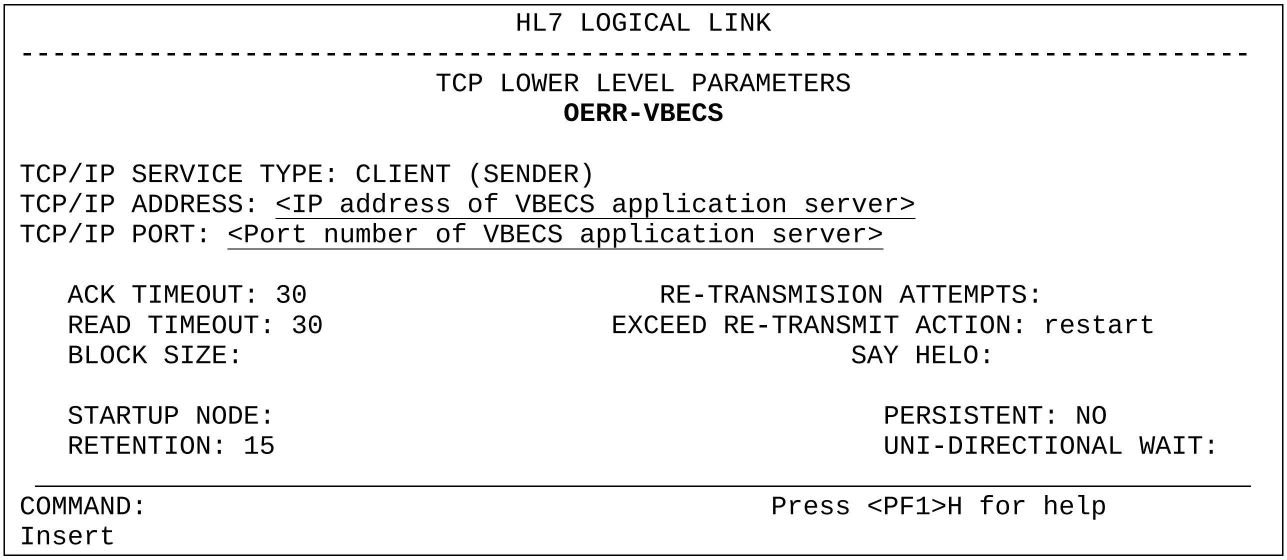
Figure 49: HL7 Logical Link



```
                          HL7 LOGICAL LINK
-----------------------------------------------------------------------------
NODE: OERR-VBECS
INSTITUTION:
DOMAIN:
AUTOSTART: ENABLED
QUEUE SIZE: 10
LLP TYPE: TCP

_
COMMAND:                                              Press <PF1>H for help
Insert
```

7) Change the value of the “TCP/IP ADDRESS” and “TCP/IP PORT” parameters to the Internet Protocol (IP) address and port number of the Blood Bank medical device application server at your site. Enterprise Operations should be contacted for the correct port numbers and IP address. Standard port numbers of 21993 for Test and 21994 for Prod are typically used. The application server IP address should be used and can be found in the completed VBECS 2.0.0 Data Center worksheet.
8) Move the cursor to the “COMMAND:” prompt.
9) Enter **Close** to return to the previous screen.
10) At the “COMMAND:” prompt, enter **Save**.
11) Enter **Exit**.

Figure 50: TCP Lower Level Parameters: OERR-VBECS



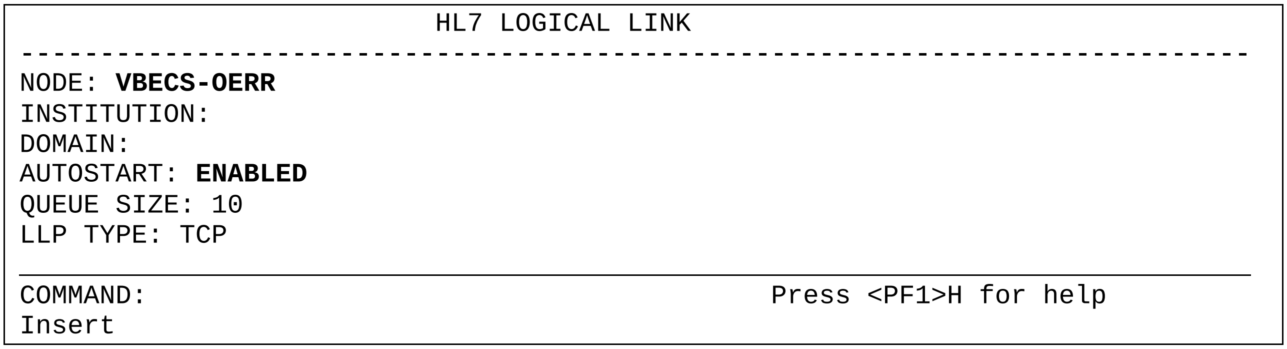
```
                               HL7 LOGICAL LINK
-----------------------------------------------------------------------------
                          TCP LOWER LEVEL PARAMETERS
                                  OERR-VBECS

TCP/IP SERVICE TYPE: CLIENT (SENDER)
TCP/IP ADDRESS: <IP address of VBECS application server>
TCP/IP PORT: <Port number of VBECS application server>

   ACK TIMEOUT: 30                       RE-TRANSMISION ATTEMPTS:
   READ TIMEOUT: 30                   EXCEED RE-TRANSMIT ACTION: restart
   BLOCK SIZE:                                      SAY HELO:

   STARTUP NODE:                                      PERSISTENT: NO
   RETENTION: 15                                      UNI-DIRECTIONAL WAIT:

COMMAND:                                              Press <PF1>H for help
Insert
```

12) Repeat Steps 3 through 11 substituting “VBECSPTM” and “VBECSPTU” for “OERR-VBECS” when prompted for the logical link name to change the IP address and port numbers for the VBECSPTM and VBECSPTU logical links.

Set Up the VBECS Inbound Logical Link

1) At the “Select HL7 Main Menu Option:” prompt, enter **Filer**.
2) At the “Select Filer and Link Management Options Option:” prompt, enter **Link Edit**.
3) At the “Select HL LOGICAL LINK NODE:” prompt, enter **VBECS-OERR** (as shown for OERR-VBECS in Figure 48).
4) Enter **Enabled** in the AUTOSTART field (Figure 51).
5) Move the cursor to the LLP TYPE field and press **Enter** (Figure 51).

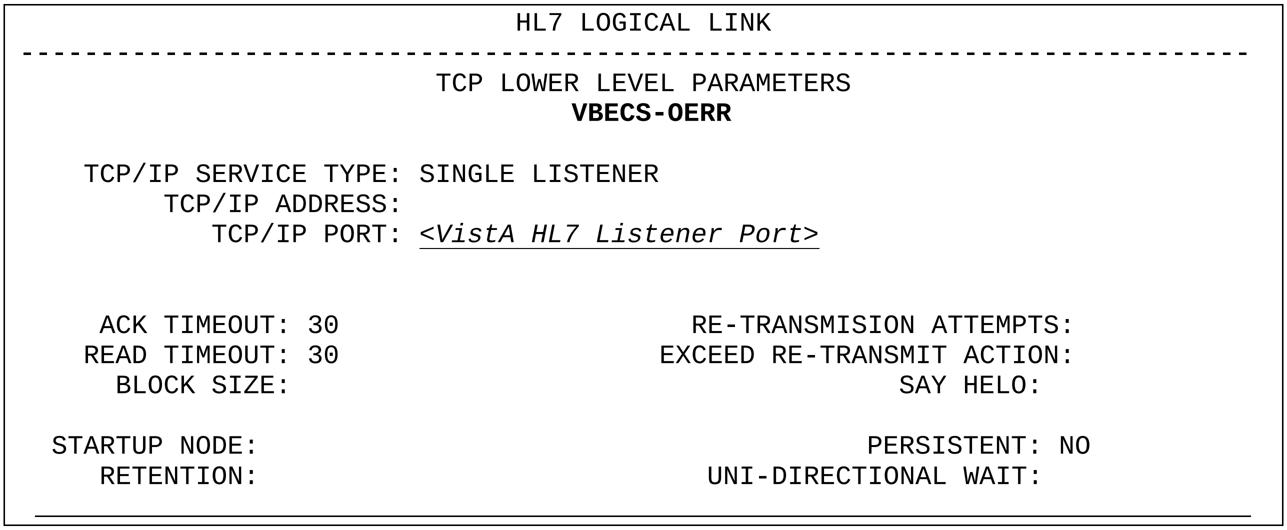
Figure 51: HL7 Logical Link



```
                          HL7 LOGICAL LINK
-----------------------------------------------------------------------------
NODE: VBECS-OERR
INSTITUTION:
DOMAIN:
AUTOSTART: ENABLED
QUEUE SIZE: 10
LLP TYPE: TCP
_____________________________________________________________________________
COMMAND:                                               Press <PF1>H for help
Insert
```

6) No “TCP/IP ADDRESS” should be entered. Change the value of the “TCP/IP PORT” parameter to the port number of the VistA HL7 Listener at your site. Regional support should be contacted for the correct port numbers. Standard port numbers of 21993 for Test and 21994 for Prod can be used if unique ports have not been assigned.
7) Move the cursor to the “COMMAND:” prompt.
8) Enter **Close** to return to the previous screen.
9) At the “COMMAND:” prompt, enter **Save**.
10) Enter **Exit**.

Figure 52: TCP Lower Level Parameters: VBECS-OERR



```
                               HL7 LOGICAL LINK
-----------------------------------------------------------------------------
                          TCP LOWER LEVEL PARAMETERS
                                  VBECS-OERR

    TCP/IP SERVICE TYPE: SINGLE LISTENER
         TCP/IP ADDRESS:
            TCP/IP PORT: <VistA HL7 Listener Port>


     ACK TIMEOUT: 30                    RE-TRANSMISION ATTEMPTS:
    READ TIMEOUT: 30                  EXCEED RE-TRANSMIT ACTION:
      BLOCK SIZE:                                     SAY HELO:

  STARTUP NODE:                                     PERSISTENT: NO
     RETENTION:                           UNI-DIRECTIONAL WAIT:
 ____________________________________________________________________________
```

```
COMMAND:                                       Press <PF1>H for help
Insert
```

Start VistA HL7 Logical Links

1) Before data can be transmitted over the VBECS logical links, edit the link definitions as described above.
2) To turn on the new VBECS logical links, select **START/STOP LINKS [HL START]**.
3) Start the “OERR-VBECS” logical link.
4) Start the “VBECS-OERR” logical link.
5) Start the “VBECSPTM” logical link.
6) Start the “VBECSPTU” logical link.
7) Ensure that the VistA HL7 Link Manager is running; VBECS messaging cannot occur without it.
8) To check the status of the Link Manager (and, if necessary, restart it), access the **HL START/STOP LINK MANAGER** menu option.

Monitor VBECS HL7 Logical Links

Once two-way communication has been established, you can monitor the links.

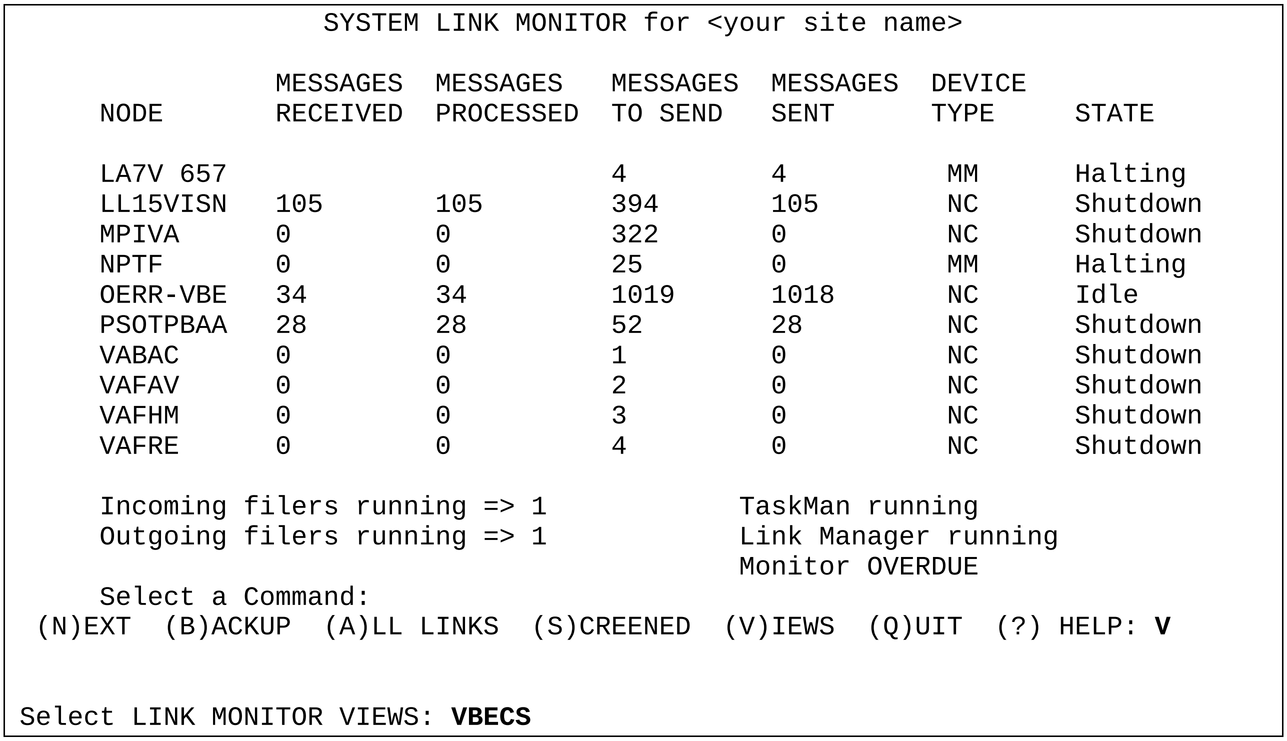
1) Use the “System Link Monitor” to view the status of the VBECS Logical Links.
2) From the “HL7 Main Menu”, select **System Link Monitor** (Figure 53).

Figure 53: HL7 System Link Monitor Menu Navigation

```
   HL7 Main Menu
      Event monitoring menu ...
      Systems Link Monitor
      Filer and Link Management Options ...
      Message Management Options ...
      Interface Developer Options ...
      Site Parameter Edit

   Select HL7 Main Menu Option: System Link Monitor
```

3) When a list of VistA HL7 links defined at your site appears, press **V** at the “Select a Command:” prompt (Figure 54).
4) At the “Select LINK MONITOR VIEWS:” prompt, enter **VBECS** (Figure 54).

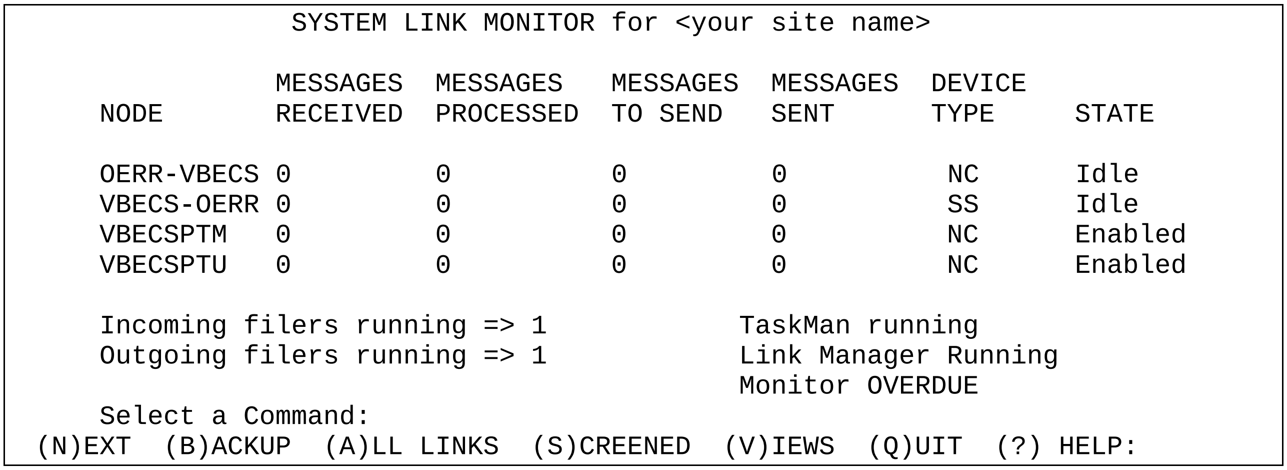
Figure 54: System Link Monitor



```
                   SYSTEM LINK MONITOR for <your site name>

                MESSAGES  MESSAGES   MESSAGES  MESSAGES  DEVICE
     NODE       RECEIVED  PROCESSED  TO SEND   SENT      TYPE     STATE

     LA7V 657                        4         4          MM      Halting
     LL15VISN   105       105        394       105        NC      Shutdown
     MPIVA      0         0          322       0          NC      Shutdown
     NPTF       0         0          25        0          MM      Halting
     OERR-VBE   34        34         1019      1018       NC      Idle
     PSOTPBAA   28        28         52        28         NC      Shutdown
     VABAC      0         0          1         0          NC      Shutdown
     VAFAV      0         0          2         0          NC      Shutdown
     VAFHM      0         0          3         0          NC      Shutdown
     VAFRE      0         0          4         0          NC      Shutdown

     Incoming filers running => 1           TaskMan running
     Outgoing filers running => 1           Link Manager running
                                            Monitor OVERDUE
     Select a Command:
 (N)EXT  (B)ACKUP  (A)LL LINKS  (S)CREENED  (V)IEWS  (Q)UIT  (?) HELP: V


Select LINK MONITOR VIEWS: VBECS
```

5) A screen similar to Figure 55 appears.

Figure 55: System Link Monitor



```
                 SYSTEM LINK MONITOR for <your site name>

                MESSAGES  MESSAGES   MESSAGES  MESSAGES  DEVICE
     NODE       RECEIVED  PROCESSED  TO SEND   SENT      TYPE     STATE

     OERR-VBECS 0         0          0         0          NC      Idle
     VBECS-OERR 0         0          0         0          SS      Idle
     VBECSPTM   0         0          0         0          NC      Enabled
     VBECSPTU   0         0          0         0          NC      Enabled

     Incoming filers running => 1           TaskMan running
     Outgoing filers running => 1           Link Manager Running
                                            Monitor OVERDUE
     Select a Command:
 (N)EXT  (B)ACKUP  (A)LL LINKS  (S)CREENED  (V)IEWS  (Q)UIT  (?) HELP:
```

6) To exit the “System Link Monitor”, at the “Select a Command:” prompt, enter **q** to quit.

The volume of HL7 traffic over these links depends on the number of daily CPRS Blood Bank orders and updates to the VistA clinical information at your site. These can be significant at large sites. Monitor the links closely the first few days after the installation and purge the HL7 log data (as appropriate) in accordance with your standard HL7 monitoring and purging procedures.

Configure VBECS VistAlink Links

1) Use the "Edit Parameter Values" option on the "GENERAL PARAMETER TOOLS" menu to edit the values for the VistALink connection to VBECS.
2) At the "Select Instance:" prompt, enter **LISTENER IP ADDRESS**.
3) At the "Value:" prompt, enter the VBECS application server IP address.
4) At the "Select Instance:" prompt, enter **LISTENER PORT NUMBER**.
5) At the "Value:" prompt, enter the VBECS VistALink listener port number. This is typically 21991 for Test and 21992 for Prod.
6) Press Enter to exit the option.

VistALink Configuration

```
Select OPTION NAME: GENERAL PARAMETER TOOLS  XPAR MENU TOOLS     General
Parameter Tools


   LV     List Values for a Selected Parameter
   LE     List Values for a Selected Entity
   LP     List Values for a Selected Package
   LT     List Values for a Selected Template
   EP     Edit Parameter Values
   ET     Edit Parameter Values with Template
   EK     Edit Parameter Definition Keyword


Select General Parameter Tools Option: EP  Edit Parameter Values
                         --- Edit Parameter Values

Select PARAMETER DEFINITION NAME: VBECS VISTALINK

---------------- Setting VBECS VISTALINK  for Package: VBECS
Select Instance: LISTENER IP ADDRESS

Instance: LISTENER IP ADDRESS//    LISTENER IP ADDRESS
Value: 10.3.7.150//     ← Enter the VBECS application server IP address here.
Select Instance: LISTENER PORT NUMBER

Instance: LISTENER PORT NUMBER  Replace    LISTENER PORT NUMBER
Value: 8000//     ←Enter the VBECS VistALink listener port here.
Select Instance:
```

VBECS Maintenance Operations

These maintenance operations are performed, using the VBECS Administrator software, during the initial installation of VBECS and during post-installation maintenance activities.

When VBECS Administrator is used for the first time, Configure Interfaces is the only option available. Completion of Configure Interfaces enables Configure Divisions. Completion of Configure Divisions enables Configure Users.

Configured options will be available at startup to perform maintenance operations. Only one instance of the VBECS Administrator can run at a time.

The dialogs defined in Configure Interfaces and Configure Divisions cannot run when VBECS is operational. VBECS cannot run when a dialog in these options is operational.

Do not change the system! The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations. Adding to or updating VBECS software without permission is prohibited.

Prerequisites

VistALink is installed and running on the associated VistA system.

The user is defined in VistA, and has a DUZ and Access and Verify Codes necessary to establish a VistA connection.

The user has a valid Windows account and is defined as a member of the Active Directory (AD) domain group (see Add and Maintain Users in Active Directory).

The user is defined as a member of the Windows Administrator group on the Active Directory domain group.

The VBECS database is installed and operational.

The VBECS Outbound logical links have been set up.

The VBECS Inbound Logical Link has been set up.

The VistA HL7 Logical Links have been started.

The VBECS HL7 Logical Links are being monitored.

Outcome

Parameters necessary to establish the connection to VistA through VistALink are available to the main VBECS application, as defined in the Configure Interfaces option.

VBECS-VistA HL7 interface parameters are defined in the Configure Interfaces option.

One or more divisions are defined for use in VBECS in the Configure Divisions option.

One or more divisions are activated as local facilities in VBECS in the Configure Divisions option.

The System Administrator has VBECS login[1] access to all active divisions.
VBECS users are defined and able to use VBECS in the Configure Users option.

Limitations and Restrictions

> *When the division changes from full-service to transfusion-only or from transfusion-only to full-service, information must be in a final state.*

Additional Information

Refer to the completed Appendix: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide* for required information when performing maintenance operations.

User Roles with Access to This Application

VBECS Administrator

Log into VBECS Administrator

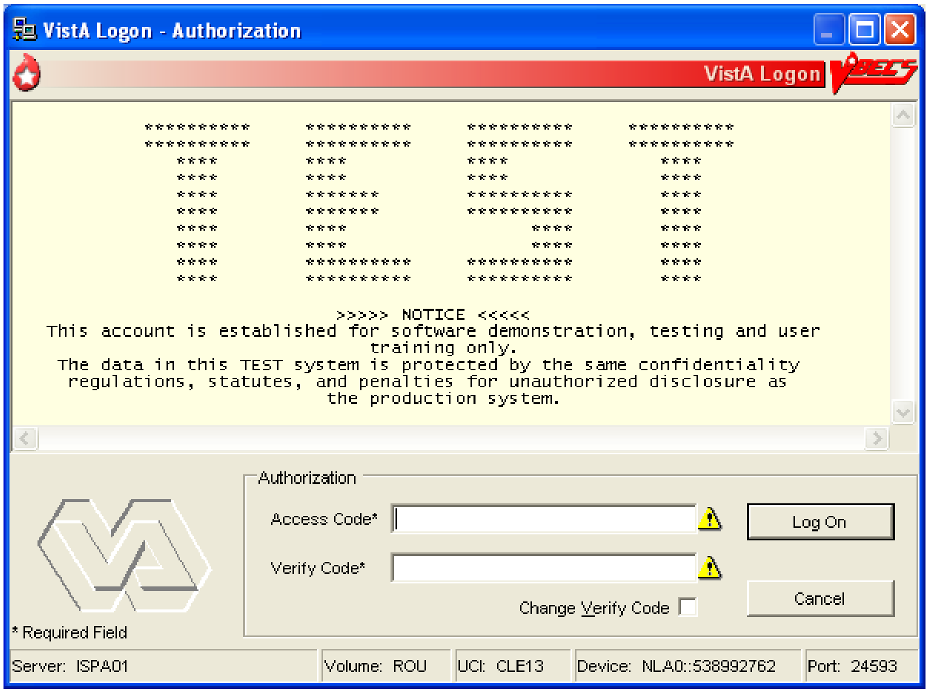
The VBECS Administrator performing the initial installation and setup must have the XOBV VISTALINK TESTER and VBECS VISTALINK CONTEXT options defined as secondary options in VistA.

User Action	VBECS Administrator
1. Open a **Remote Desktop Connection** to the VBECS Application Server and logon with your user id and password. .	Logs onto the Application Server.
2. Double-click the **VBECS Administrator** icon.	Opens VBECS Administrator. **NOTES** When the user logs into VBECS Administrator for the first time to set VistALink parameters, the system does not display the VistA Logon – Authorization screen. Continue at Step 6.
3. Continue to the VistA logon screen (Figure 56).	Opens the VistA Logon – Authorization screen. The user may log onto VistA or continue and log on as needed. **NOTES** The VistA logon screen is displayed only after initial setup of VistALink parameters.
4. Log onto VistA when VBECS Administrator starts up or at the invocation of any option that uses VistALink when VistALink is not connected. Enter the VistA Access	Allows a user to log on by entering VistA Access and Verify Codes, separated by a semicolon (;), in the Access Code data entry field. When a user accesses an option that requires a VistALink connection and the connection becomes unavailable, allows the user to restore the connection.

[1] There is a slight difference in terminology between VistA and VBECS: VistA uses “log on” and “logon,” and VBECS uses “log in” and “login.” Therefore, both terms are used throughout this manual. “Log in” and “login” are used generically when referring to both systems at one time.

User Action	VBECS Administrator
and Verify Codes.	When a reconnection attempt is successful, VBECS closes the connection status window and returns to the desktop. The VistALink Connected icon in the status bar indicates a successful connection. When a reconnection attempt is unsuccessful, attempts to reconnect to VistALink until the user cancels. Verifies that user credentials for the VBECS Administrator and VistA Access and Verify Codes belong to the same user. **NOTES** When a user logs into VBECS Administrator, the connection to VistA is established through VistALink. When the VistALink connection is not restorable, VBECS Administrator displays a message that the requested use cannot be executed because VistALink is unavailable.
5. Continue working in VBECS Administrator (Figure 57).	Displays the main menu.

Figure 56: Example of VistA Logon



```
**********     **********     **********     **********
**********     **********     **********     **********
   ****        ****           ****              ****
   ****        ****           ****              ****
   ****        *******        **********        ****
   ****        *******        **********        ****
   ****        ****                 ****        ****
   ****        ****                 ****        ****
   ****        **********     **********        ****
   ****        **********     **********        ****

                       >>>>> NOTICE <<<<<
 This account is established for software demonstration, testing and user
                          training only.
  The data in this TEST system is protected by the same confidentiality
   regulations, statutes, and penalties for unauthorized disclosure as
                       the production system.
```

Authorization

Access Code*

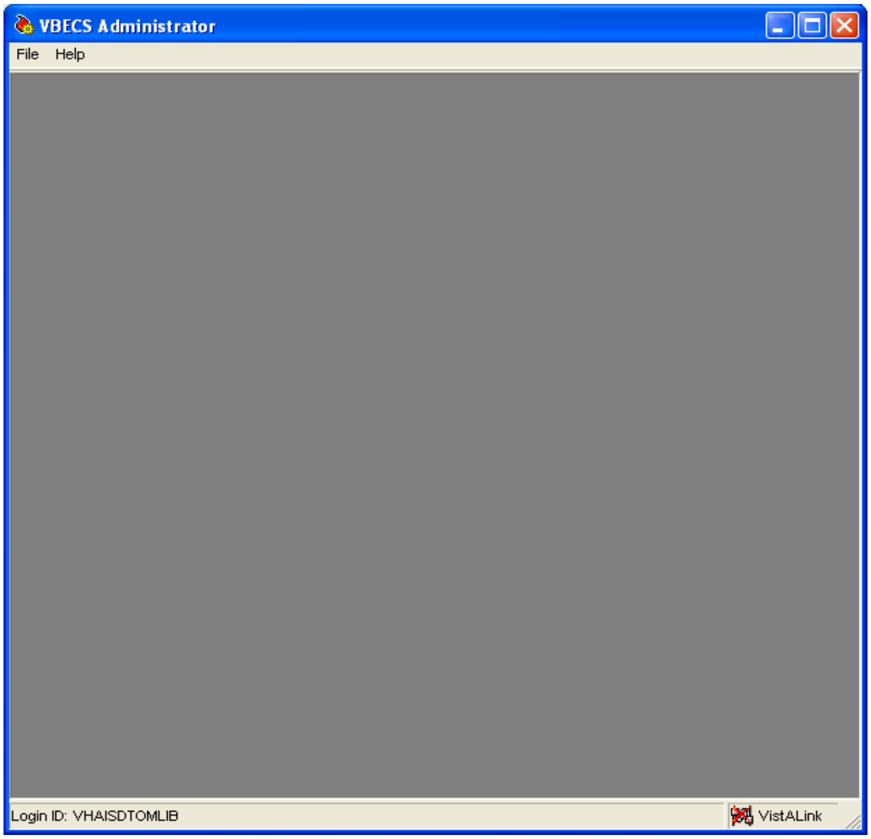
Verify Code*

Change Verify Code □

* Required Field

Server: ISPA01 | Volume: ROU | UCI: CLE13 | Device: NLA0::538992762 | Port: 24593

Figure 57: Example of VBECS Administrator



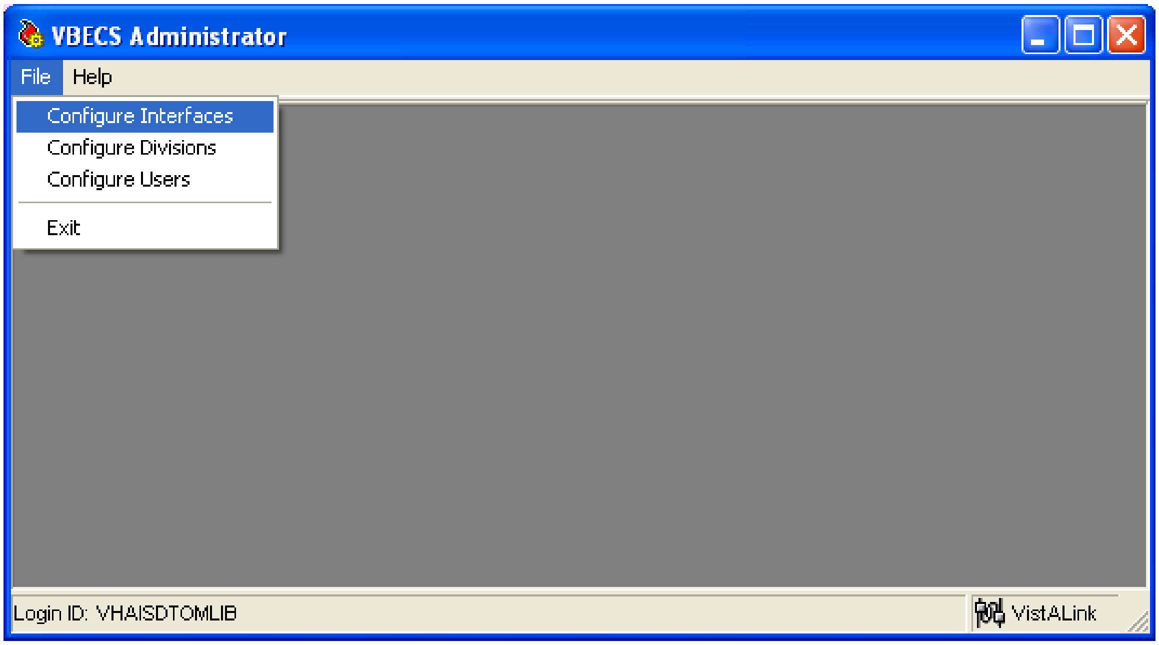
Login ID: VHAISDTOMLIB

Configure Interfaces

The System Administrator sets parameters for the connection to VistA to enable retrieval of VistA data and to configure HL7 interfaces between VBECS and VistA.

User Action	VBECS Administrator
1. To configure VBECS VistALink and HL7 interface parameters, click **File** on the main menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces** (Figure 58).	Displays the VBECS Configure Interfaces dialog for data entry.

Figure 58: Example of Configure Interfaces

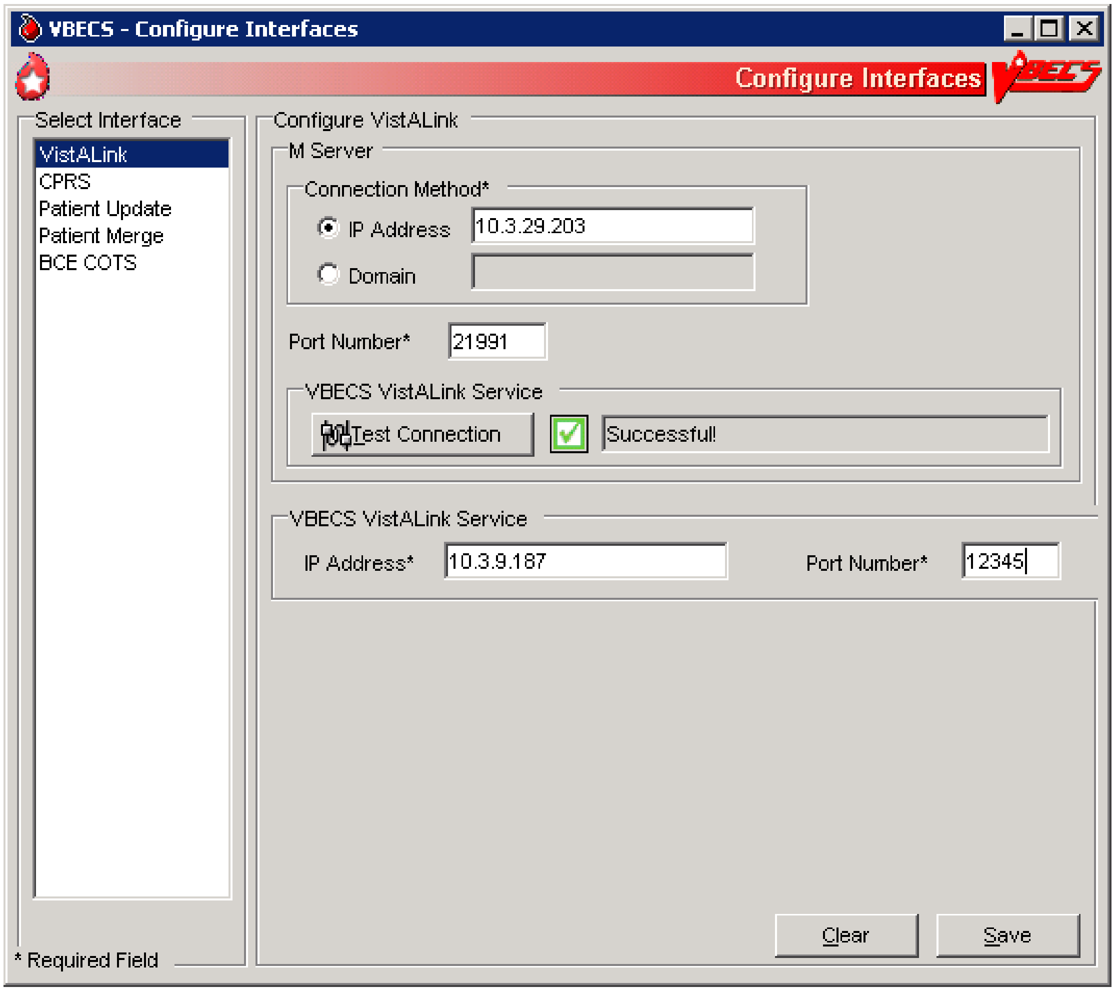


Configure VistALink Parameters

User Action	VBECS Administrator
1. To configure VistALink Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure VistALink parameters, select **VistALink** from the Select Interface list box (Figure 59).	Displays the Configure VistALink group and allows data entry of the IP address (or domain name) and port number of the VistA system VistALink listener. Allows the user to test the VistALink connection parameters. **NOTES** The user may modify the IP address (or domain name) and port number, as required.
4. For the VistALink interface, enter a	Validates that the IP address is in the standard four-octet notation (e.g.,

User Action	VBECS Administrator
valid IP address (or domain name) and port number of the VistA system VistALink listener in the M Server group box fields.	127.0.0.1) or that the Domain field was filled in. Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VistALink IP address to which VBECS will direct messages. The Port Number field represents the VistALink port number to which VBECS will direct messages.
5. Click **Test Connection**. Record the IP and port numbers.	**NOTES** The Test Connection button is enabled only when valid entries exist in the IP Address (or Domain) and Port Number fields. If connection to the VistA system is successful, the VistA Logon – Authorization dialog is displayed and the user is required to enter valid Access and Verify Codes. If connection to the VistA system is unsuccessful, hover over the red square and a detailed error message will display.
6. To configure the VBECS VistALink Service, enter a valid IP and port number. 📷 Capture a screen shot.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS application server IP address to which VistA will direct messages. The Port Number field represents the VBECS application server port number to which VistA will direct messages. This is typically 21991 for Test and 21992 for Prod.
7. Click **Save** to save changes.	Displays a confirmation dialog. Also warns the user that the VBECS VistALink service will be restarted if parameters changed.
8. Click **Yes** to commit changes to the database.	Changes are saved to the VBECS database and VBECS will attempt to restart the VBECS Prod (or Test) VistALink Listener service if the IP or Port Number has changed. If the restart fails, you will receive the following message: **The service failed to restart. Please contact VBECS support to have the service restarted**. If you receive the failure message, please file a support ticket (Service Desk Primary Contact).

Figure 59: Example of Configure Interfaces: VistALink



● IP Address 10.3.29.203

○ Domain

Port Number* 21991

VBECS VistALink Service

✓ Successful!

VBECS VistALink Service

IP Address* 10.3.9.187

Port Number* 12345

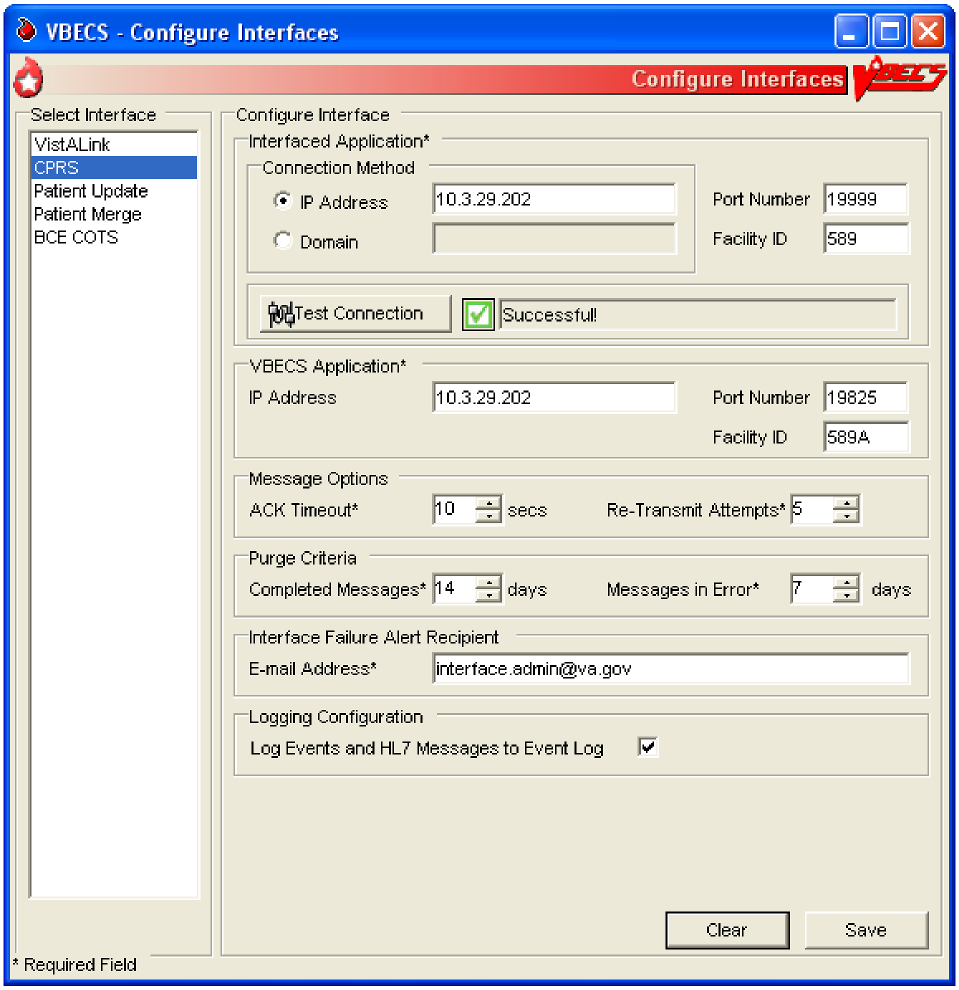
Configure CPRS HL7 Interface Parameters

User Action	VBECS Administrator
1. To configure CPRS HL7 Interface Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure CPRS HL7 Interface Parameters, select **CPRS** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 60).	Displays the Configure Interface group and allows data entry of HL7 interface-related parameters.
4. To configure Interfaced Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1) or that the Domain field was filled in. Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VistA CPRS IP address to which VBECS will direct messages to CPRS via the VBECS-OERR HL7 Link. The Domain name field represents the fully qualified domain name to which VBECS will direct messages. The Port Number field represents the VistA CPRS port number to which VBECS will direct messages. The Facility ID is used in the MSH segment of the HL7 interface to help identify the system. This free-text field is usually set to the primary site's station number. Messaging to VBECS will fail if this Facility ID is not supplied.
5. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS application server IP address to which CPRS will direct messages to VBECS via the OERR-VBECS HL7 Link. The Port Number field represents the VBECS application server port number to which CPRS will direct messages. This is typically 21993 for Test and 21994 for Prod. The VBECS Facility ID must be different from the VistA. The Facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. Messaging to VBECS will fail if this Facility ID is not supplied.
6. Click **Test Connection**. Record the IP and port numbers.	**NOTES** The Test Connection button is enabled only when valid entries

User Action	VBECS Administrator
📷 Capture a screen shot.	exist in the IP Address (or Domain) and Port Number fields. If connection to the CPRS system is unsuccessful, hover over the red square and a detailed error message will display.
(This step is optional.) 7. To configure Message Options group parameters, enter an ACK timeout period and a number of retransmission attempts in the related data fields.	Validates that the ACK timeout period is a whole number from 1 to 999 (seconds) (default: 10). Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5).
(This step is optional.) 8. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields.	Validates that purge periods are whole numbers from 1 to 30 (days) (default: 7).
9. To configure the Interface Failure Alert Recipient group parameter, enter a valid **Administrator distribution (Active Directory) group** email address in the related data field.	Validates the email address is entered correctly e.g., VBECSWatchers@va.gov. **NOTES** Only one email address can be entered which is recommended to contain local IRM support and/or the Blood Bank ADPAC. VBECS Windows Services will send email alerts to this address when HL7 order messaging errors occur. Email alerts will not contain PII or PHI. For assistance troubleshooting the email alerts, see the VBECS Application Interfaces section. This email address is also used for notifications concerning database problems. See the SQL Maintenance section.
10. To configure the Logging Configuration group parameter, click or clear the **Log Events and HL7 Messages to Event Log** check box. 📷 Capture a screen shot.	**NOTES** This check box indicates whether to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Application Server. (This is the only way to view VBECS HL7 messages on the VBECS server.)
11. Click **Save** and **Yes** to confirm the save and service restart is related parameters were change.	Changes are saved to the VBECS database and VBECS will attempt to restart the VBECS Prod (or Test) HL7 Dispatcher and/or the VBECS Prod (or Test) HL7 Listener if the IP or Port Number has changed for the respective service. If the restart(s) fail, you will receive the following message: **The service failed to restart. Please contact VBECS support to have the service restarted**. If you receive the failure message, please file a support ticket (Service Desk Primary Contact).
12. To close the VBECS – Configure	Validates that the data was saved.

User Action	VBECS Administrator
Interfaces dialog, click ☒ in the upper-right corner.	

Figure 60: Example of Configure Interfaces: CPRS



Interfaced Application*

Connection Method

● IP Address 10.3.29.202

○ Domain

Port Number 19999

Facility ID 589

☑ Successfull

VBECS Application*

IP Address 10.3.29.202

Port Number 19825

Facility ID 589A

Message Options

ACK Timeout* 10 secs

Re-Transmit Attempts* 5

Purge Criteria

Completed Messages* 14 days

Messages in Error* 7 days

Interface Failure Alert Recipient

E-mail Address* interface.admin@va.gov

Logging Configuration

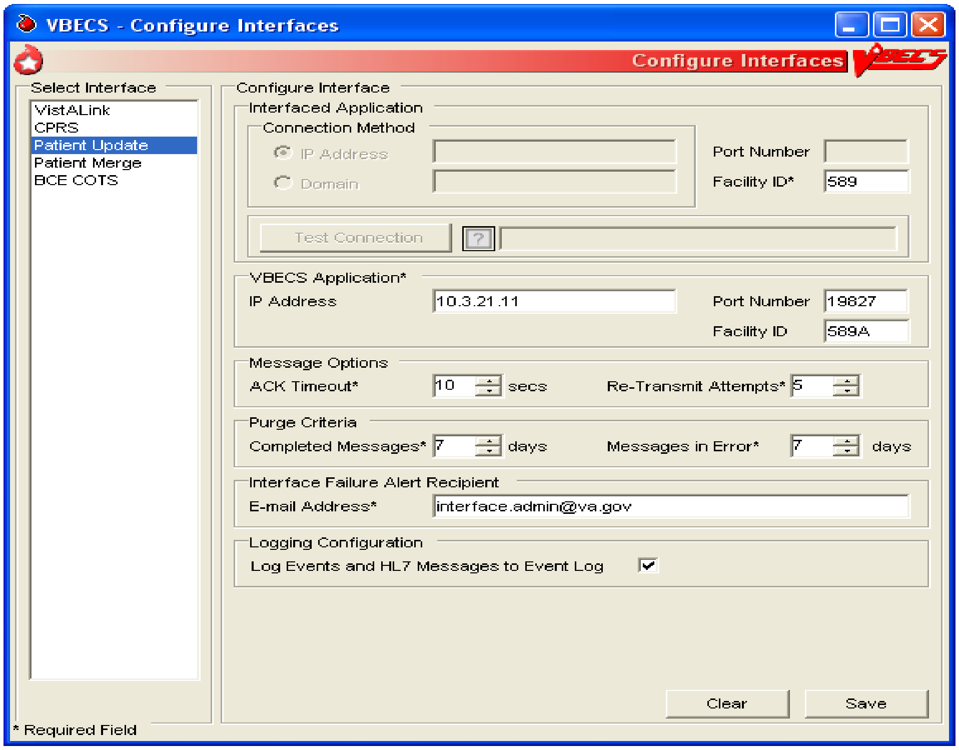
Log Events and HL7 Messages to Event Log ☑

Configure Patient Update HL7 Interface Parameters

User Action	VBECS Administrator
1. To configure Patient Update HL7 Interface Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure Patient Update HL7 Interface Parameters, select **PatientUpdate** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 61).	Displays the Configure Interface group and allows data entry of HL7 interface-related parameters.
4. To configure Interfaced Application group parameters, enter a facility ID in the related data fields.	**NOTES** The IP Address and Port Number fields are disabled: no outbound messages are sent to VistA for this interface. The facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. Messaging to VBECS will fail if this Facility ID is not supplied.
5. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS application server IP address to which VistA will direct messages to VBECS via the VBECSPTU HL7 Link. The Port Number field represents the VBECS application server port number to which VistA will direct messages. This is typically 21993 for Test and 21994 for Prod.
(This step is optional.) 6. To configure Message Options group parameters, enter an ACK Timeout period and number of retransmission attempts in the related data fields.	Validates that the ACK timeout period is a whole number from 1 to 999 (seconds) (default: 10). Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5).
(This step is optional.) 7. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields.	Validates that the purge periods are whole numbers from 1 to 30 (days) (default: 7).
8. To configure the Interface Failure Alert Recipient group parameter, enter a valid **Administrator**	Validates the email address is entered correctly e.g., VBECSWatchers@va.gov.

User Action	VBECS Administrator
distribution (Active Directory) group email address in the related data field.	**NOTES** Only one email address can be entered which is recommended to contain local Blood Bank users and/or the Blood Bank ADPAC. VBECS Windows Services will send email alerts to this address when patient update HL7 messaging errors occur. Email alerts will not contain PII or PHI. For assistance troubleshooting the email alerts, see the VBECS Application Interfaces section.
9. To configure the Logging Configuration group parameter, click or clear **the Log Events and HL7 Messages to Event Log** check box. 📷 Capture a screen shot.	**NOTES** This check box indicates whether to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS application Server. (This is the only way to view VBECS HL7 messages on the VBECS server.)
10. Click **Save** and **Yes** to confirm the save.	Changes are saved to the VBECS database and VBECS will attempt to restart the VBECS Prod (or Test) HL7 Listener service if the IP or Port Number has changed. If the restart fails, you will receive the following message: **The service failed to restart. Please contact VBECS support to have the service restarted**. If you receive the failure message, please file a support ticket (Service Desk Primary Contact).
11. To close the VBECS – Configure Interfaces dialog, click ☒ in the upper-right corner.	Validates that the data was previously saved.

Figure 61: Example of Configure Interfaces: PatientUpdate



VBECS - Configure Interfaces

Configure Interfaces

Select Interface
- VistALink
- CPRS
- Patient Update
- Patient Merge
- BCE COTS

Configure Interface

Interfaced Application

Connection Method

● IP Address

○ Domain

Port Number

Facility ID* 589

Test Connection ?

VBECS Application*

IP Address 10.3.21.11

Port Number 19827

Facility ID 589A

Message Options

ACK Timeout* 10 secs

Re-Transmit Attempts* 5

Purge Criteria

Completed Messages* 7 days

Messages in Error* 7 days

Interface Failure Alert Recipient

E-mail Address* interface.admin@va.gov

Logging Configuration

Log Events and HL7 Messages to Event Log ☑

Clear Save

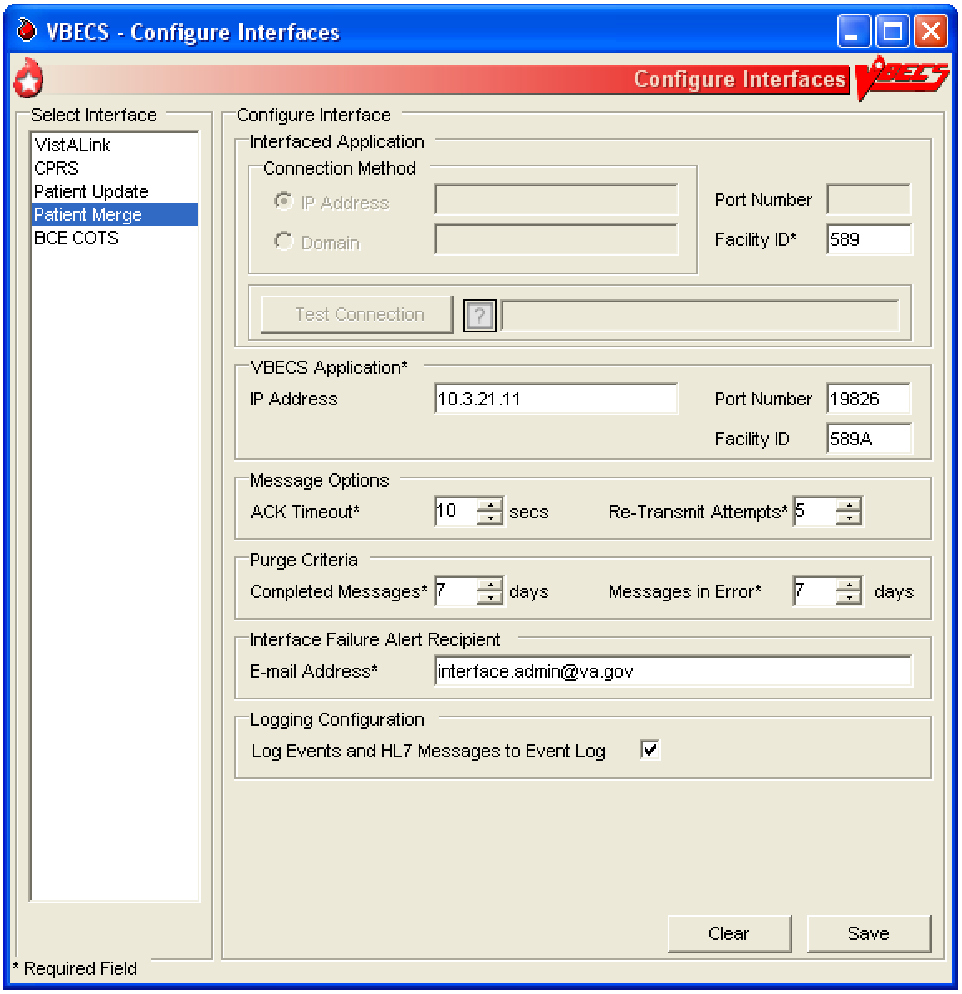
* Required Field

Configure Patient Merge HL7 Interface Parameters

User Action	VBECS Administrator
1. To configure Patient Merge HL7 Interface Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure Patient Merge HL7 Interface Parameters, select **PatientMerge** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 62).	Displays the Configure Interfaces group and allows data entry of HL7 interface-related parameters.
4. To configure Interfaced Application group parameters, enter a facility ID in the related data field.	**NOTES** The IP Address and Port Number fields are disabled: no outbound messages are sent to VistA for this interface. The facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. Messaging to VBECS will fail if this Facility ID is not supplied.
5. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS application server IP address to which VistA will direct messages to VBECS via the VBECSPTM HL7 Link. The Port Number field represents the VBECS application server port number to which VistA will direct messages. This is typically 21993 for Test and 21994 for Prod.
(This step is optional.) 6. To configure Message Options group parameters, enter an ACK Timeout period and number of retransmission attempts in the related data fields.	Validates that the ACK Timeout period is a whole number from 1 to 999 (seconds) (default: 10). Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5).
(This step is optional.) 7. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields.	Validates that the purge periods are whole numbers from 1 to 30 (days) (default: 7).
8. To configure the Interface Failure	Validates the email address is entered correctly e.g.,

User Action	VBECS Administrator
Alert Recipient group parameter, enter a valid **Administrator distribution (Active Directory) group** email address in the related data field.	VBECSWatchers@va.gov. **NOTES** Only one email address can be entered which is recommended to contain local Blood Bank users and/or the Blood Bank ADPAC. VBECS Windows Services will send email alerts to this address when patient update HL7 messaging errors occur. Email alerts will not contain PII or PHI. For assistance troubleshooting the email alerts, see the VBECS Application Interfaces section.
9. To configure the Logging Configuration group parameter, click or clear the **Log Events and HL7 Messages to Event Log** check box. 📷 Capture a screen shot.	**NOTES** This check box indicates whether to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Application Server. (This is the only way to view VBECS HL7 messages on the VBECS server.)
10. Click **Save** and **Yes** to confirm the save.	Changes are saved to the VBECS database and VBECS will attempt to restart the VBECS Prod (or Test) HL7 Listener service if the IP or Port Number has changed. If the restart fails, you will receive the following message: **The service failed to restart. Please contact VBECS support to have the service restarted**. If you receive the failure message, please file a support ticket (Service Desk Primary Contact).
11. To close the VBECS – Configure Interfaces dialog, click ☒ in the upper-right corner.	Validates that the data was previously saved.

Figure 62: Example of Configure Interfaces: PatientMerge



Port Number
Facility ID* 589

VBECS Application*
IP Address 10.3.21.11
Port Number 19826
Facility ID 589A

Message Options
ACK Timeout* 10 secs
Re-Transmit Attempts* 5

Purge Criteria
Completed Messages* 7 days
Messages in Error* 7 days

Interface Failure Alert Recipient
E-mail Address* interface.admin@va.gov

Logging Configuration
Log Events and HL7 Messages to Event Log ☑

* Required Field

Configure BCE COTS Interface Parameters

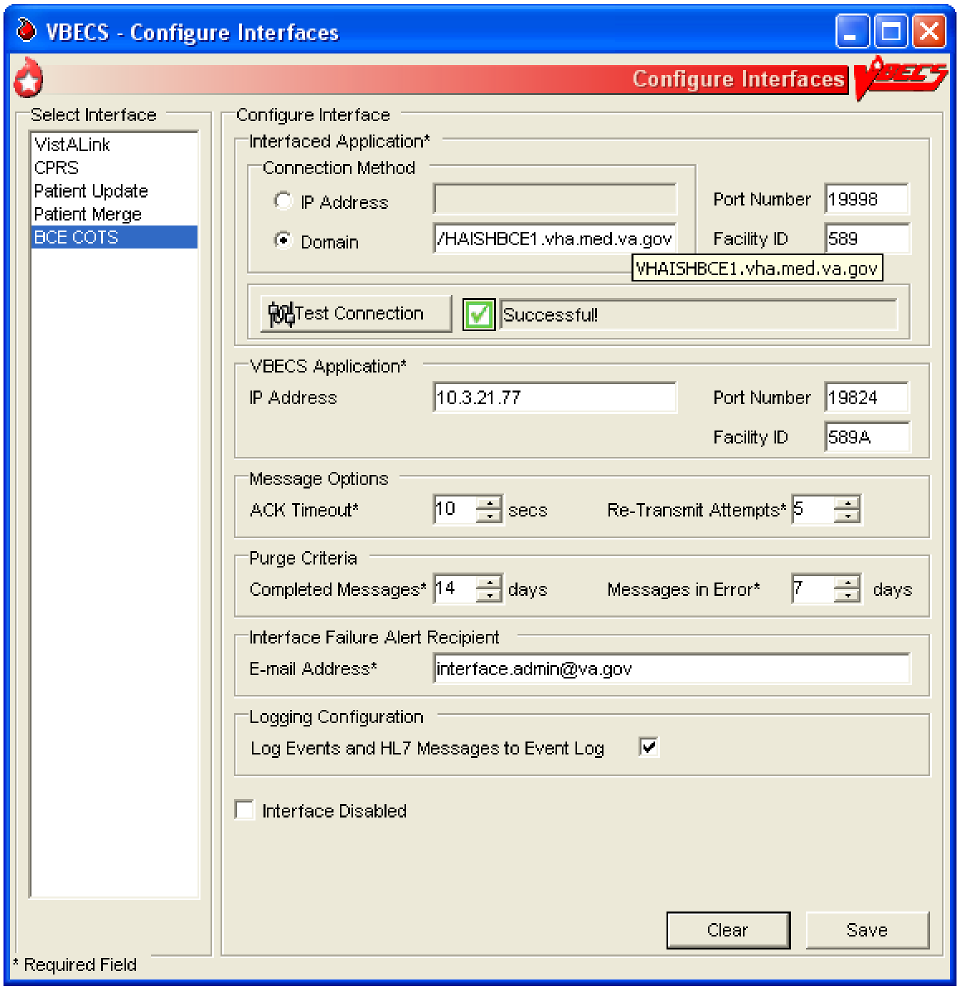
Do not configure this interface until the BCE COTS software is available.

User Action	VBECS Administrator
1. To configure BCE COTS Interface Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure BCE COTS Interface Parameters, select **BCE COTS** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 63).	Displays the Configure Interfaces group and allows data entry of BCE COTS interface-related parameters.

User Action	VBECS Administrator
4. To configure Interfaced Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1) or that the Domain field was filled in. Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the BCE COTS IP address to which VBECS will direct messages. The Domain name field represents the fully qualified domain name to which VBECS will direct messages. The Port Number field represents the BCE COTS port number to which VBECS will direct messages. The Facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field that is usually set to the primary site's station number. This field is typically validated only when using an interface engine to assist with routing HL7 messages. The VBECS HL7 interfaces do not currently require the use of an interface engine.
5. Click **Test Connection**. Record the IP and port numbers.	**NOTES** The Test Connection button is enabled only when valid entries exist in the IP Address (or Domain) and Port Number fields.
6. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS application server IP address to which BCE COTS will direct messages. The Port Number field represents the VBECS application server port number to which BCE COTS will direct messages. The facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. This field is validated only when using an interface engine to assist with routing HL7 messages. The VBECS HL7 interfaces do not require the use of an interface engine.
(This step is optional.) 7. To configure Message Options group parameters, enter an ACK timeout period and a number of retransmission attempts in the related data fields.	Validates that the ACK timeout period is a whole number from 1 to 999 (seconds) (default: 10). Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5).
(This step is optional.)	Validates that purge periods are whole numbers from 1 to 30 (days) (default: 7).

User Action	VBECS Administrator
8. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields.	Note: Error message purging functionality will be added in a future release.
9. To configure the Interface Failure Alert Recipient group parameter, enter a valid **Administrator distribution (Active Directory) group** email address in the related data field.	Validates the email address is entered correctly e.g., VBECSWatchers@va.gov. **NOTES** Only one email address can be entered which is recommended to contain local Blood Bank users and/or the Blood Bank ADPAC. VBECS Windows Services will send email alerts to this address when patient update HL7 messaging errors occur. Email alerts will not contain PII or PHI. For assistance troubleshooting the email alerts, see the VBECS Application Interfaces section.
10. To configure the Logging Configuration group parameter, click or clear the **Log Events and HL7 Messages to Event Log** check box. 📷 Capture a screen shot.	**NOTES** This check box indicates whether to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Application Server. (This is the only way to view VBECS HL7 messages on the VBECS server.)
11. To enable the BCE COTS interface, the **Interface Disabled** check box must be unchecked.	**NOTES** The BCE COTS interface is enabled\disabled via this check box. When enabled the fields on the screen become enabled for the BCE COTS interface. If the BCE interface is disabled through VBECS Admin, no BCE messages will be sent or received from BCE. When the BCE interface is enabled, you will still not send any BCE messages until you stop and start the VBECS Test or Prod Dispatcher service.
12. Click **Save** and **Yes** to confirm the save.	Changes are saved to the VBECS database and VBECS will attempt to restart the VBECS Prod (or Test) HL7 Listener service if the IP or Port Number has changed. If the restart fails, you will receive the following message: **The service failed to restart. Please contact VBECS support to have the service restarted**. If you receive the failure message, please file a support ticket (Service Desk Primary Contact).
13. To close the VBECS – Configure Interfaces dialog, click ☒ in the upper-right corner.	Validates that the data was saved.

Figure 63: Example of Configure Interfaces: BCE COTS



VBECS - Configure Interfaces

Configure Interfaces

Select Interface

- VistALink
- CPRS
- Patient Update
- Patient Merge
- BCE COTS

Configure Interface

Interfaced Application*

Connection Method

○ IP Address

● Domain /HAISHBCE1.vha.med.va.gov

Port Number 19998

Facility ID 589

VHAISHBCE1.vha.med.va.gov

Test Connection ☑ Successful!

VBECS Application*

IP Address 10.3.21.77

Port Number 19824

Facility ID 589A

Message Options

ACK Timeout* 10 secs

Re-Transmit Attempts* 5

Purge Criteria

Completed Messages* 14 days

Messages in Error* 7 days

Interface Failure Alert Recipient

E-mail Address* interface.admin@va.gov

Logging Configuration

Log Events and HL7 Messages to Event Log ☑

□ Interface Disabled

* Required Field

Configure Divisions

The System Administrator configures VBECS as a single division or as multidivisional.

Assumptions

The VistA data conversion is complete.
VBECS-VistA connection parameters are set.
VistALink is installed and running on the associated VistA system.
The user is defined in VistA, and has a DUZ and Access and Verify Codes necessary to establish a VistA connection.
The user has a valid Windows account and is defined as a member of the Active Directory domain group (see Add and Maintain Users in Active Directory).
The IP address of the label printer is known.
The name of the division report printer is known (if multidivisional).
The VBECS database is installed and operational.
User has the VistA secondary menu option VBECS VISTALINK CONTEXT
User has the VistA security key LRBLSUPER and/or LRBLOODBANK

Outcome

One or more divisions are defined in VBECS.
One or more divisions are activated as local facilities in VBECS.
The System Administrator has VBECS login[2] access to all active divisions.

Limitations and Restrictions

All units in a division must be in a final status to allow the division to change from full-service to transfusion-only or from transfusion-only to full-service.

Additional Information

A VBECS Administrator/Supervisor may further configure:

- o VBECS users in Update User Roles.
- o VBECS division parameters in Configure Division, Product Modifications, and Configure Testing.

The user must log onto VistA using Access and Verify Codes.

User Roles with Access to This Option

System Administrator

[2] There is a slight difference in terminology between VistA and VBECS: VistA uses “log on” and “logon,” and VBECS uses “log in” and “login.” Therefore, both terms are used throughout this manual. “Log in” and “login” are used generically when referring to both systems at one time.

Add and Maintain Divisions

The user defines and maintains division attributes.

> *Changes made in the VBECS Administrator option mapping orders to another VBECS division do not affect delivered orders. Orders delivered to a VBECS division must be completed, rejected, or canceled in that division. Resubmit orders after mapping is completed to send an order to another VBECS division.*

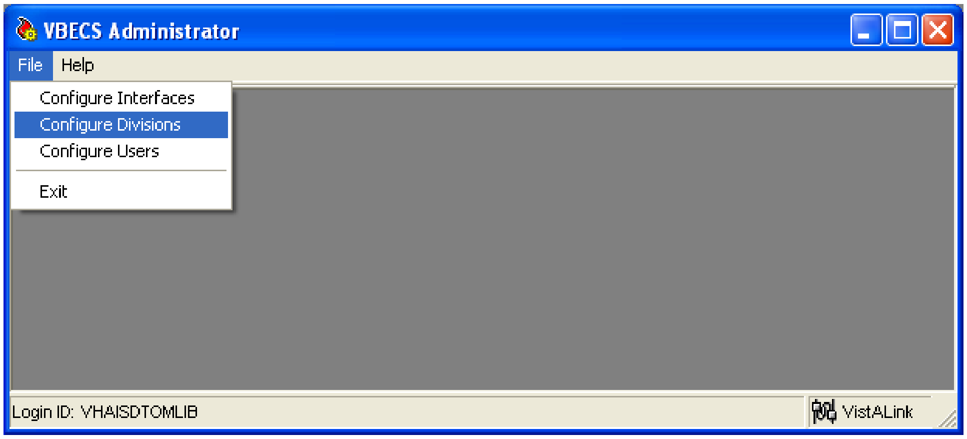
User Action	VBECS Administrator
1. To add and maintain divisions in VBECS, click **File** on the main menu of the VBECS Administrator software.	• Displays the menu options used to configure VBECS.
2. Select **Configure Divisions** (Figure 64).	• Displays the Configure Division dialog and allows entry of division parameters.
3. To edit a defined division, click the **Division Identification** tab (Figure 65). Select a division code or name from the drop-down menu or, to configure a new division, click the **ellipsis** button. Select a division from the list (Figure 66).	**NOTES** The user may not edit the division code or name. A division may be full-service (default) or transfusion-only. When a unit not in a final status exists, a user may not change the type of transfusion service. When a division is transfusion-only, VBECS disables electronic crossmatch. When a division changes from full-service to transfusion-only, units already in inventory are not restricted to patients and must be returned to the blood center. When a division changes from transfusion-only to full-service, inventory units are restricted to patients without ABO/Rh confirmation. The facility must decide how to handle this existing inventory. VBECS prevents the user from changing a division from full-service to transfusion-only or from transfusion-only to full-service when there are open or partially completed worksheets or processes in the division. The Division Name and Division Code are identified in the VistA INSTITUTION file (#4). The Division Name stored in VBECS is the INSTITUTION file NAME field (#.01); the Division Code stored in VBECS is the STATION NUMBER field (#99). When either value change in VistA, rerun these steps to update the VBECS database with the current values from VistA.

User Action	VBECS Administrator
4. To receive orders from VistA Institutions to the selected Division, check the Map orders from VistA institutions check box. Click the Active checkbox for each institution that applies.	**NOTES** Changes made to institution mappings require a restart of the VBECS HL7 Multi Listener service. For more information, see Table 10 in the VBECS Windows Services section. One or more VistA institutions from the list of valid institutions retrieved from VistA may be associated with the selected VBECS division from the list of valid institutions retrieved from VistA. A VistA institution may be associated with only one VBECS division. A VistA institution defined as a VBECS division is not eligible for selection as an associated institution to a different VBECS division. To associate additional institutions, enable an optional VistALink query to retrieve a list of all institutions associated with the VistA site that are currently defined within the VistA database but not in the selected VBECS division. VBECS displays the list to the user for selection.
5. Select the FDA Registered Facility associated with the division or, to search for the facility by name or FDA Registration Number, click the **ellipsis** button (Figure 65).	• Allows the user to associate a division with a facility from the National Facility Table. **NOTES** The user must associate a division with a facility from the National Facility Table. If there is no matching facility, VBECS Administrator asks the user to contact the Service Desk. When this occurs, wait for customer support to respond or, to continue establishing a division, select and configure any facility from the National Facility Table. When the configuration is complete, use the Local Facilities option in VBECS to define the local facility that matches the information missing from the National Facility Table. Return to Configure Divisions to re-associate your division with the newly entered local facility. When a division is configured, VBECS displays, “I certify that the blood products listed were properly maintained, in accordance with the Code of Federal Regulations, while in storage at this institution. Components were inspected when packed for shipment and found to be satisfactory in color and appearance.”
6. Select the VistA Lab Blood Bank Accession Area associated with the selected division from the drop-down menu (Figure 65).	**NOTES** The Lab package uses the Accession Area to track blood bank-related workload for the division. New VA hospitals that require enabling a blood bank must activate and assign a division to an accession area.
7. Enter the desired number of minutes in the Lock Inactivity Timeout field.	• Allows the user to set the lock inactivity timeout period [5 to 15 minutes (default: 5 minutes)].

User Action	VBECS Administrator
	NOTES The lock inactivity timeout period specifies how long a user can be idle and in control of data being edited. VBECS warns the user 60 seconds before the lock inactivity period expires that he will lose priority for the data. When he responds within 60 seconds, VBECS clears the warning and resets the lock activity timer. Otherwise, VBECS informs him that his lock was released and he must reenter his changes. VBECS uses optimistic and pessimistic locking to prevent data corruption. If a user attempts to edit data locked by another user, VBECS alerts him that the record is in use and prevents access (pessimistic locking). If more than one user attempts to change data simultaneously, VBECS accepts only the first update and warns the other users that the record changed (optimistic locking, which is non-configurable and a fail-safe to pessimistic locking).
8. To activate or inactivate the division, click or clear the **Active VBECS Division?** check box (Figure 65). 📷 Capture a screen shot.	• When the user saves a previously active division as inactive, inactivates user roles for that division. **NOTES** The system will not allow the user to activate a division that has orders mapped to another VBECS division. VBECS displays, “Unable to activate. The VBECS division currently has orders mapped to another VBECS division.” The system will not allow the user to inactivate a division that has orders mapped to it. VBECS displays, “Unable to inactivate. This VBECS division currently has orders mapped to it. Release this mapping prior to inactivation,”
9. Click the **Service Type** tab. Click the **Full-Service Facility** or **Transfusion-Only Facility** radio button (Figure 68). 📷 Capture a screen shot.	• Allows the user to identify the facility as full-service or transfusion-only. **NOTES** 🚧 When the division changes from full-service to transfusion-only or from transfusion-only to full-service, information must be in a final state. VBECS does not check for pending orders or active units in inventory, so there is a risk of corrupting information. There is a risk of having unconfirmed units available for transfusion if any are issued.

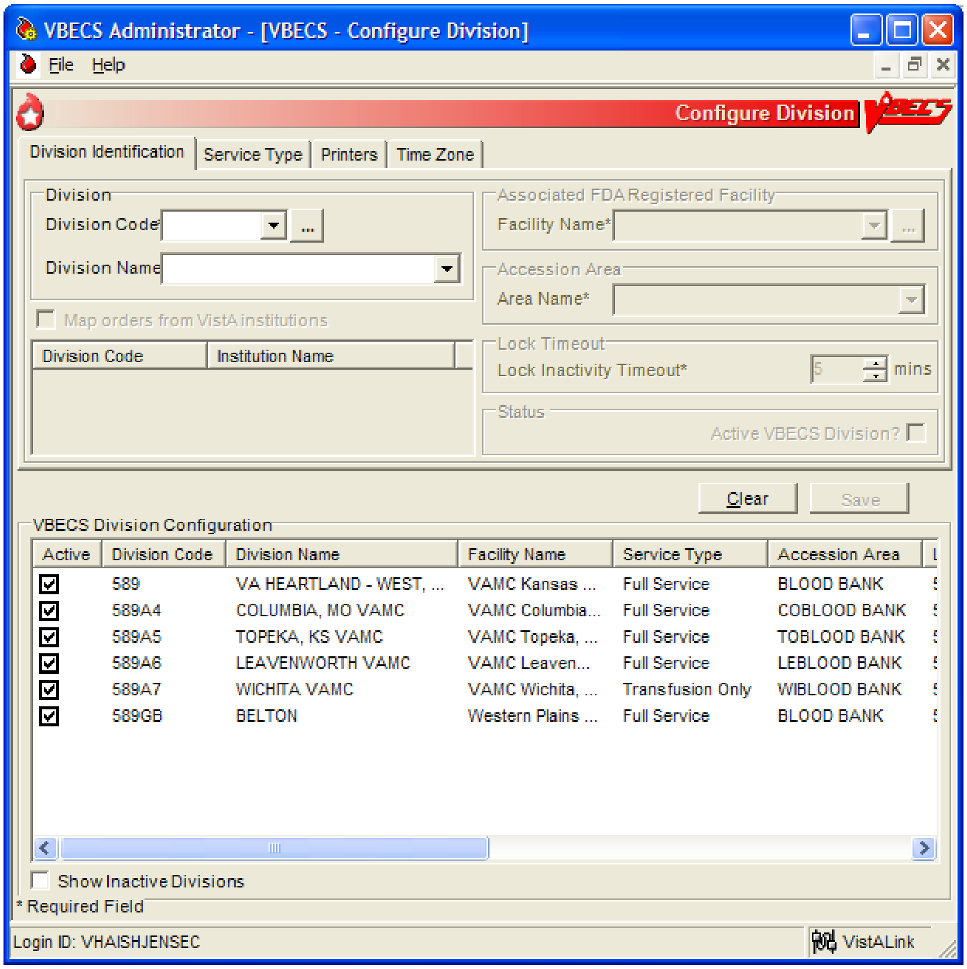
User Action	VBECS Administrator
10. Click the **Printers** tab. Select a Default Report Printer from the list. Clear or click the **Division Uses Label Printer** check box. Edit the COM port number and/or the TCP port number. Enter the IP address (Figure 69). 📷 Capture a screen shot.	• Allows the user to enter the COM and TCP port numbers and the IP address for the label printer. • Allows the user to select the default printer for the division when more than one printer is installed on the system. **NOTES** Standard values for COM and TCP ports: COM = 2 TCP = 9100
11. Click the **Time Zone tab**. Select a time zone. In the Daylight Savings field, select **US Standard DST**, **Do not observe DST**, or **Custom DST**. Enter start and end dates for custom DST (Figure 70). 📷 Capture a screen shot. Click **Save**.	• Allows the user to set the time zone and daylight saving parameters.
12. Click **Save** and **OK** to commit the changes or add the new division to the VBECS database.	• Commits changes and additions to the database. **NOTES** Multidivisional sites must repeat Steps 3 through 11 for each division. The VBECS Administrator/Supervisor who configured the divisions must add himself as a user to all divisions to enable the functionality of canned comments in the VBECS system.
13. To close the **VBECS** – **Configure Divisions** dialog, click ☒ in the upper-right corner.	

Figure 64: Example of Configure Divisions



Login ID: VHAISDTOMLIB

Figure 65: Example of Configure Division: Division Identification

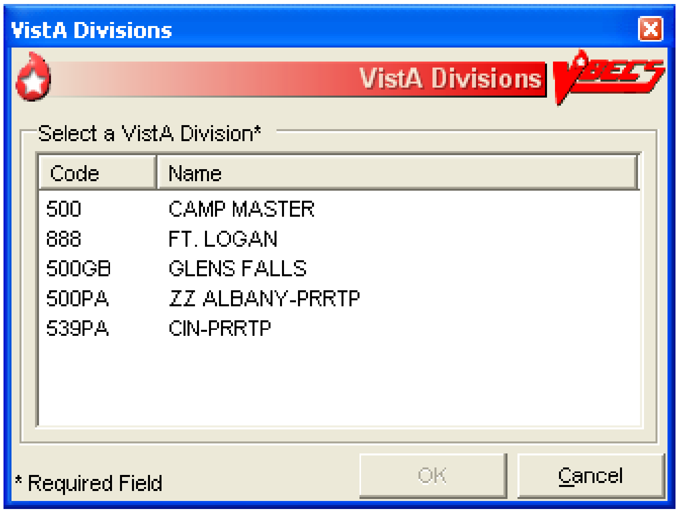


Active	Division Code	Division Name	Facility Name	Service Type	Accession Area	L
☑	589	VA HEARTLAND - WEST, ...	VAMC Kansas ...	Full Service	BLOOD BANK	5
☑	589A4	COLUMBIA, MO VAMC	VAMC Columbia...	Full Service	COBLOOD BANK	5
☑	589A5	TOPEKA, KS VAMC	VAMC Topeka, ...	Full Service	TOBLOOD BANK	5
☑	589A6	LEAVENWORTH VAMC	VAMC Leaven...	Full Service	LEBLOOD BANK	5
☑	589A7	WICHITA VAMC	VAMC Wichita, ...	Transfusion Only	WIBLOOD BANK	5
☑	589GB	BELTON	Western Plains ...	Full Service	BLOOD BANK	5

* Required Field

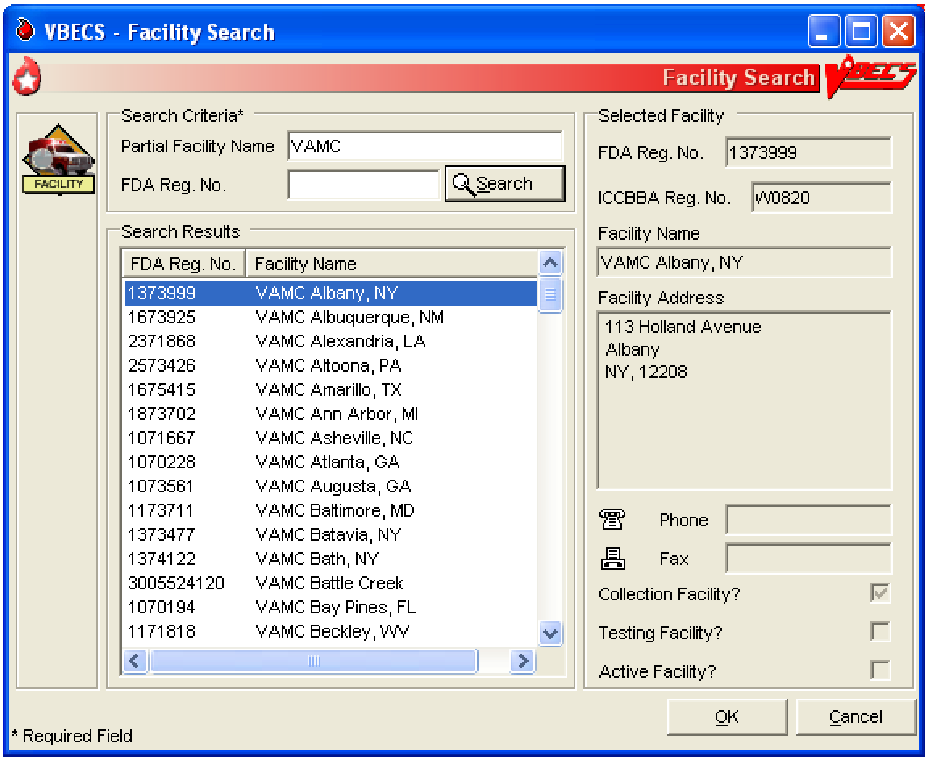
Login ID: VHAISHJENSEC

Figure 66: Example of Select VistA Divisions



Code	Name
500	CAMP MASTER
888	FT. LOGAN
500GB	GLENS FALLS
500PA	ZZ ALBANY-PRRTP
539PA	CIN-PRRTP

Figure 67: Example of Facility Search



Partial Facility Name: VAMC

FDA Reg. No.:

FDA Reg. No.	Facility Name
1373999	VAMC Albany, NY
1673925	VAMC Albuquerque, NM
2371868	VAMC Alexandria, LA
2573426	VAMC Altoona, PA
1675415	VAMC Amarillo, TX
1873702	VAMC Ann Arbor, MI
1071667	VAMC Asheville, NC
1070228	VAMC Atlanta, GA
1073561	VAMC Augusta, GA
1173711	VAMC Baltimore, MD
1373477	VAMC Batavia, NY
1374122	VAMC Bath, NY
3005524120	VAMC Battle Creek
1070194	VAMC Bay Pines, FL
1171818	VAMC Beckley, WV

FDA Reg. No.: 1373999

ICCBBA Reg. No.: W0820

Facility Name: VAMC Albany, NY

Facility Address:
113 Holland Avenue
Albany
NY, 12208

☎ Phone:

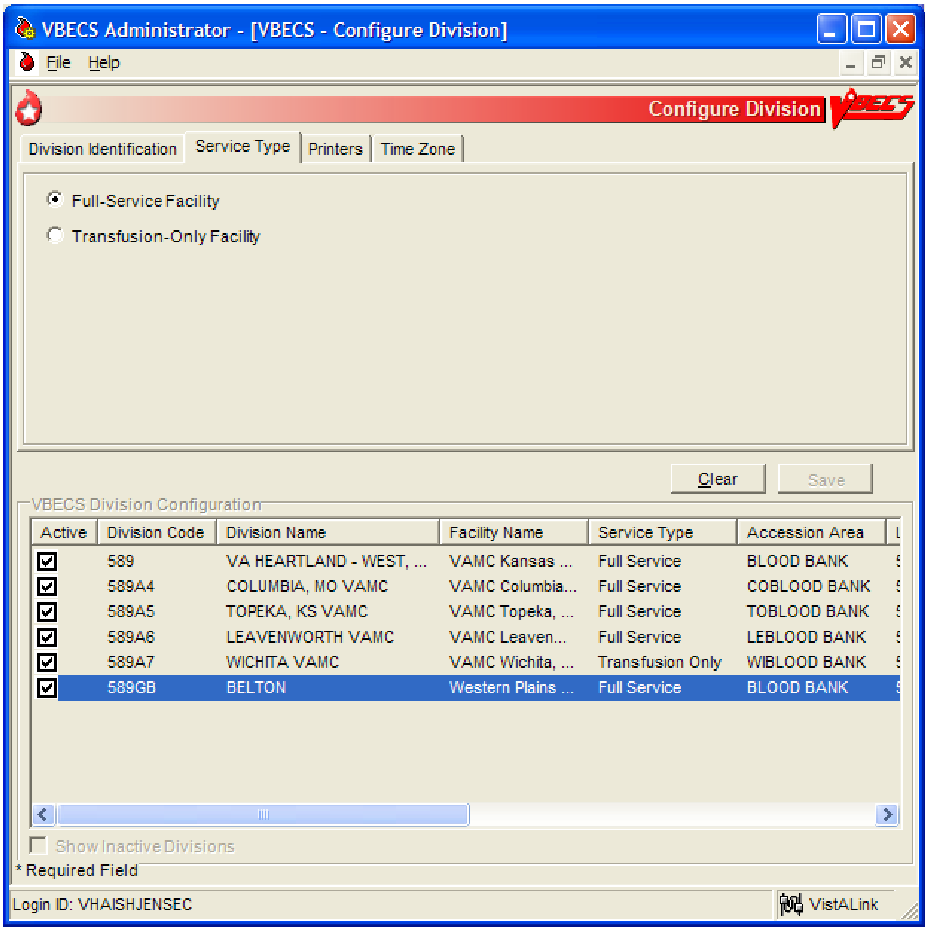
Fax:

Collection Facility? ☑

Testing Facility? □

Active Facility? □

Figure 68: Example of Configure Division: Service Type



● Full-Service Facility

○ Transfusion-Only Facility

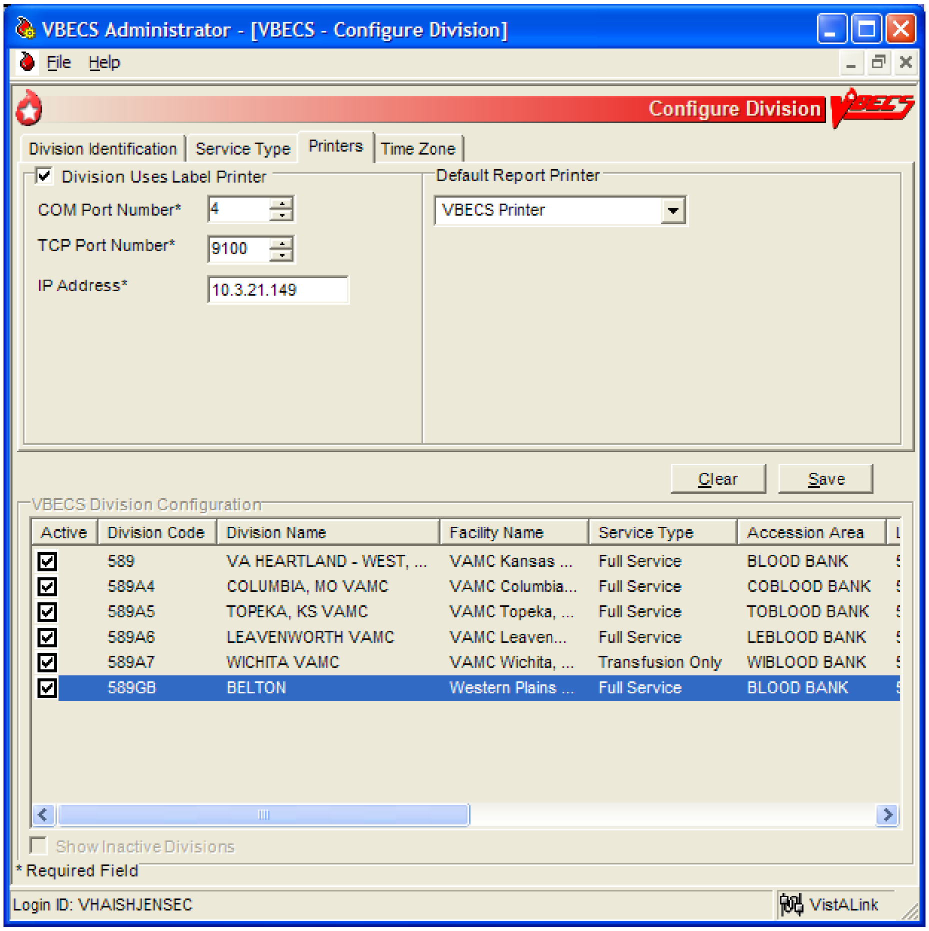
VBECS Division Configuration

Active	Division Code	Division Name	Facility Name	Service Type	Accession Area
☑	589	VA HEARTLAND - WEST, ...	VAMC Kansas ...	Full Service	BLOOD BANK
☑	589A4	COLUMBIA, MO VAMC	VAMC Columbia...	Full Service	COBLOOD BANK
☑	589A5	TOPEKA, KS VAMC	VAMC Topeka, ...	Full Service	TOBLOOD BANK
☑	589A6	LEAVENWORTH VAMC	VAMC Leaven...	Full Service	LEBLOOD BANK
☑	589A7	WICHITA VAMC	VAMC Wichita, ...	Transfusion Only	WIBLOOD BANK
☑	589GB	BELTON	Western Plains ...	Full Service	BLOOD BANK

□ Show Inactive Divisions

* Required Field

Figure 69: Example of Configure Division: Label Printing



☑ Division Uses Label Printer

COM Port Number* 4

TCP Port Number* 9100

IP Address* 10.3.21.149

Default Report Printer: VBECS Printer

VBECS Division Configuration

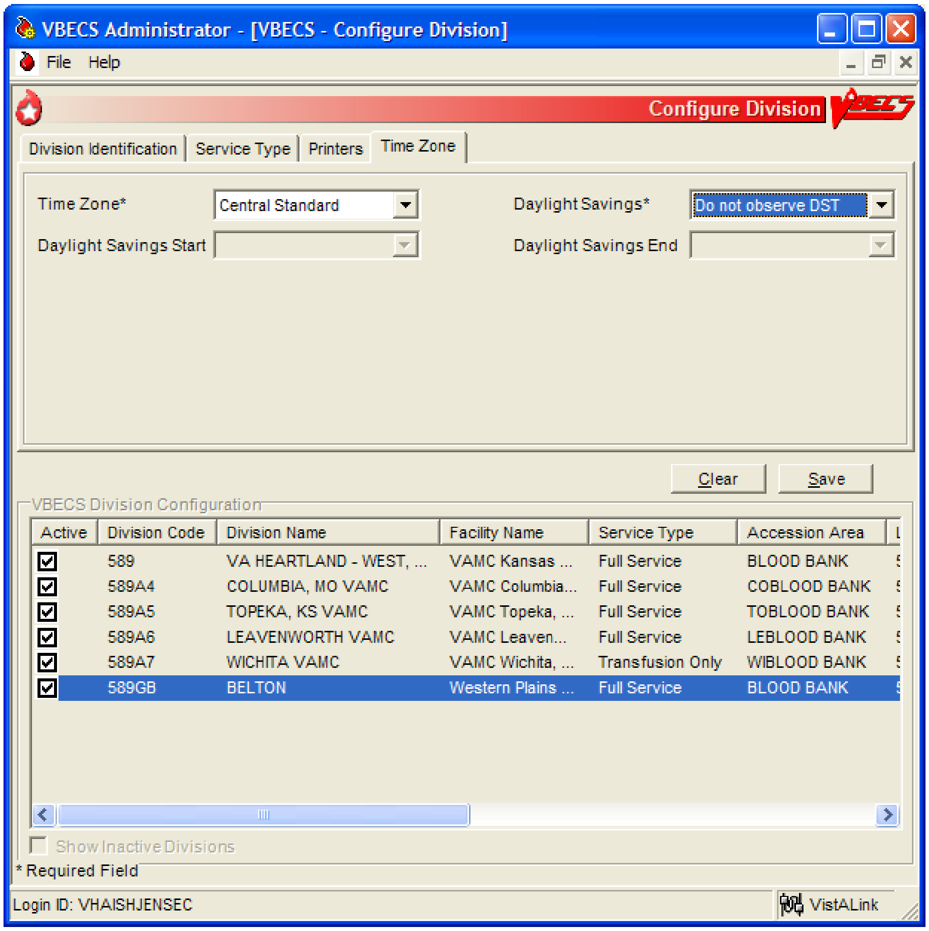
Active	Division Code	Division Name	Facility Name	Service Type	Accession Area	L
☑	589	VA HEARTLAND - WEST, ...	VAMC Kansas ...	Full Service	BLOOD BANK	5
☑	589A4	COLUMBIA, MO VAMC	VAMC Columbia...	Full Service	COBLOOD BANK	5
☑	589A5	TOPEKA, KS VAMC	VAMC Topeka, ...	Full Service	TOBLOOD BANK	5
☑	589A6	LEAVENWORTH VAMC	VAMC Leaven...	Full Service	LEBLOOD BANK	5
☑	589A7	WICHITA VAMC	VAMC Wichita, ...	Transfusion Only	WIBLOOD BANK	5
☑	589GB	BELTON	Western Plains ...	Full Service	BLOOD BANK	5

□ Show Inactive Divisions

* Required Field

Login ID: VHAISHJENSEC

Figure 70: Example of Configure Division: Time Zone



Time Zone* Central Standard

Daylight Savings* Do not observe DST

Daylight Savings Start

Daylight Savings End

Active	Division Code	Division Name	Facility Name	Service Type	Accession Area
☑	589	VA HEARTLAND - WEST, ...	VAMC Kansas ...	Full Service	BLOOD BANK
☑	589A4	COLUMBIA, MO VAMC	VAMC Columbia...	Full Service	COBLOOD BANK
☑	589A5	TOPEKA, KS VAMC	VAMC Topeka, ...	Full Service	TOBLOOD BANK
☑	589A6	LEAVENWORTH VAMC	VAMC Leaven...	Full Service	LEBLOOD BANK
☑	589A7	WICHITA VAMC	VAMC Wichita, ...	Transfusion Only	WIBLOOD BANK
☑	589GB	BELTON	Western Plains ...	Full Service	BLOOD BANK

□ Show Inactive Divisions

* Required Field

Login ID: VHAISHJENSEC

Configure Users

The System Administrator matches VistA users to VBECS users and sets user security levels. If this is a data center site, use the form (Appendix C: Active Directory Change Request) to submit Active Directory modifications and skip the “Add and Maintain Users in Active Directory” section (proceed to the “Configure VBECS Users” section after the data center has completed your request).

Assumptions

The VistA data conversion is complete.
All VBECS users must have the LRBLSUPER and/or LRBLOODBANK security key.
VBECS-VistA connection parameters are set.
VistALink is installed and running on the associated VistA system.
VBECS application configuration files have the correct values for Domain and user group fields.
At least one division in VBECS is configured.
The user is defined in VistA, and has a DUZ and Access and Verify Codes necessary to establish a VistA connection and has signed on to VistA at least once.
All users of the blood bank medical device software are assigned the VBECS VISTALINK CONTEXT option as a secondary option. VistALink uses the VBECS VISTALINK CONTEXT option to provide user context sign-on security to VistA.
The user has a valid Windows login and is defined as a member of the Active Directory domain group.
The System Administrator created Active Directory local groups, as directed in Appendix D: Blood Bank Configuration Checklist, Create Local Groups, in *VistA Blood Establishment Computer Software (VBECS) Installation Guide*.
The VBECS database is installed and operational.
The user must be assigned/belong to an active division in VistA.
The user must have logged into the VistA account successfully at least once.
The user has the XOBV VistALink Tester as a secondary menu (to test the VistALink connection in VBECS Administrator).
The user’s record in VistA File #200 – New Person File, must not have a Termination Date and the DISUSER flag must not be set.

Outcome

VBECS users are defined and able to use VBECS.

Limitations and Restrictions

Each VBECS user must have a unique Windows login ID. If a Windows login ID becomes inactive and is eligible for re-use in Active Directory, do not re-use it for VBECS: it may result in corrupted data in VBECS.
A user must not change their Windows login ID after being configured in VBECS. If the user’s name changes, the name fields in Active Directory can be modified without changing the login ID.

Additional Information

A VBECS Administrator/Supervisor may further configure VBECS users in Update User Roles. The user must log onto VistA using Access and Verify Codes.

User Roles with Access to This Option

System Administrator

Add and Maintain Users in Active Directory

The user adds and inactivates VBECS users.

User Action	Active Directory Users and Computers
1. Install Active Directory tools (on the Administrator's computer only) from the Windows Server 2008 R2 installation CD or as a free download from Microsoft.	
2. Open the Control Panel. Double-click **Administrative Tools**. Double-click **Active Directory Users and Computers** (Figure 71).	• Allows the user to view and add users in Active Directory for VBECS.
3. Navigate to the OU in which your VBECS local groups reside. Double-click the name of the user group (on the right) to which you wish to add the user (Figure 72).	• Displays two user groups in the right panel, one for VBECS Administrator and one for VBECS. • Displays the properties window. **NOTES** The VBECS local groups (V*nnxxx*VbecsUsers and V*nnxxx*VbecsAdministrators, where *nn* is your VISN number and *xxx* is your site identifier) were created in Appendix: Blood Bank Configuration Checklist, Create Local Groups, in *VistA Blood Establishment Computer Software (VBECS) Installation Guide*. • Add a user to either group to allow access to the server through Remote Desktop Connection and to VBECS Administrator or VBECS (depending on the group).
4. Click the **Members** tab (Figure 73). Click **Add** to add a user. To remove a user, select the user name and click **Remove**.	**NOTES** If the Add button is disabled, you do not have access to this group. Contact local active directory personnel to gain access.
5. If the **From this location** field does not display the location of the user to be added, click **Locations** and enter the correct domain (Figure 74).	• Allows the user to enter the domain.
6. In the **Enter the object names to select** field, enter the Windows	**NOTES**

User Action	Active Directory Users and Computers
login ID for the user to be added. Click **OK**.	Click **Check Names** to verify that the login ID is valid.
7. Click **OK**.	• Closes the Properties window.
8. Exit.	

Figure 71: Example of Active Directory Users and Computers

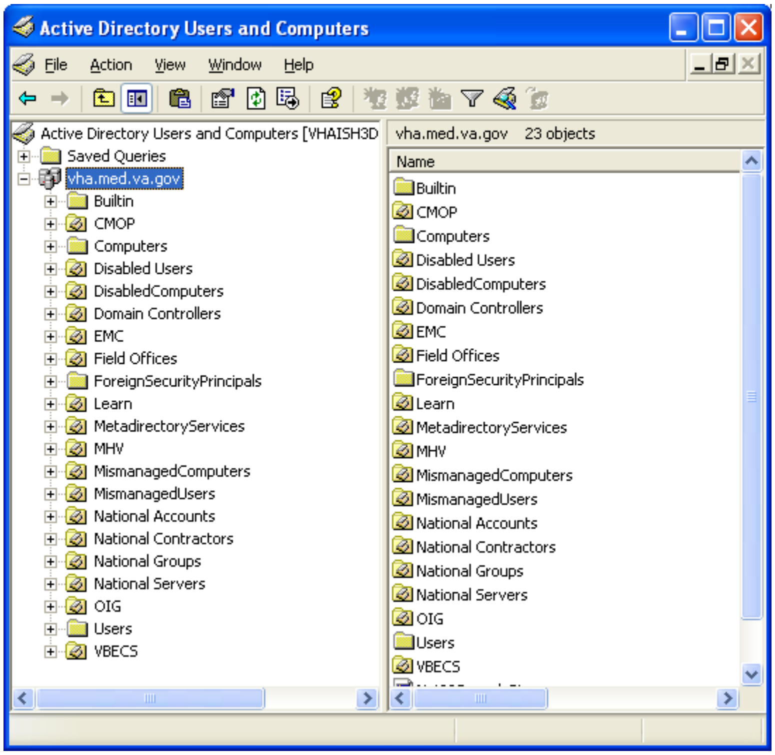
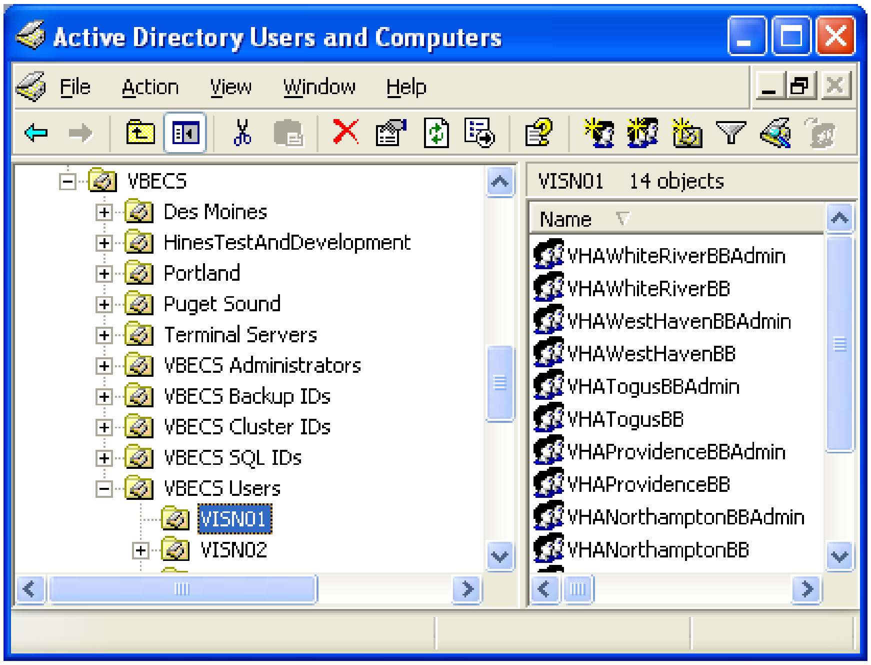


Figure 72: Example of Active Directory Users



- VBECS
  - Des Moines
  - HinesTestAndDevelopment
  - Portland
  - Puget Sound
  - Terminal Servers
  - VBECS Administrators
  - VBECS Backup IDs
  - VBECS Cluster IDs
  - VBECS SQL IDs
  - VBECS Users
    - VISN01
    - VISN02

VHAWhiteRiverBBAdmin
VHAWhiteRiverBB
VHAWestHavenBBAdmin
VHAWestHavenBB
VHATogusBBAdmin
VHATogusBB
VHAProvidenceBBAdmin
VHAProvidenceBB
VHANorthamptonBBAdmin
VHANorthamptonBB

Figure 73: Example of Group Properties

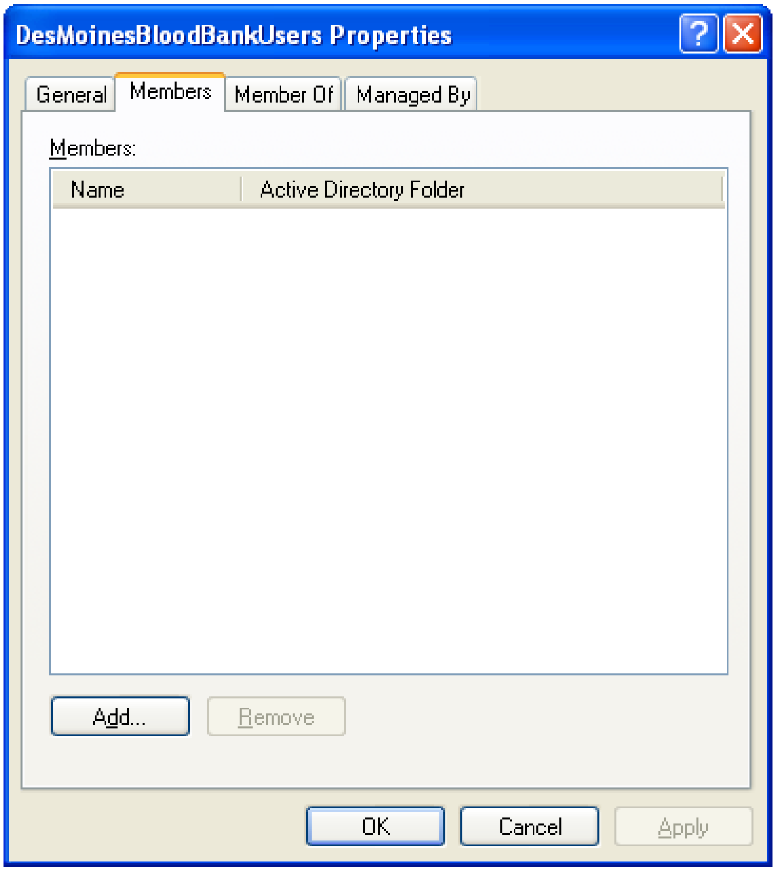
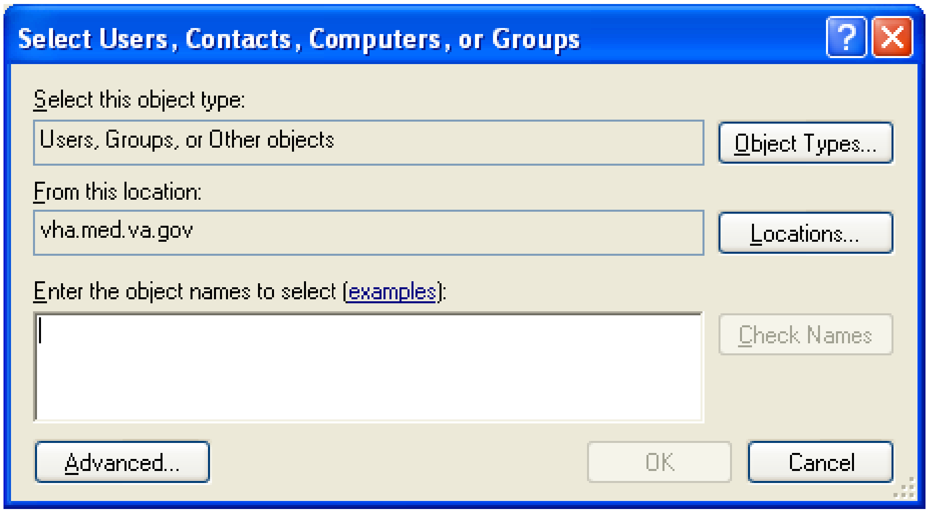


Figure 74: Example of Select Users


Select Users, Contacts, Computers, or Groups
Object Types...
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel

Select this object type:
Users, Groups, or Other objects

From this location:
vha.med.va.gov

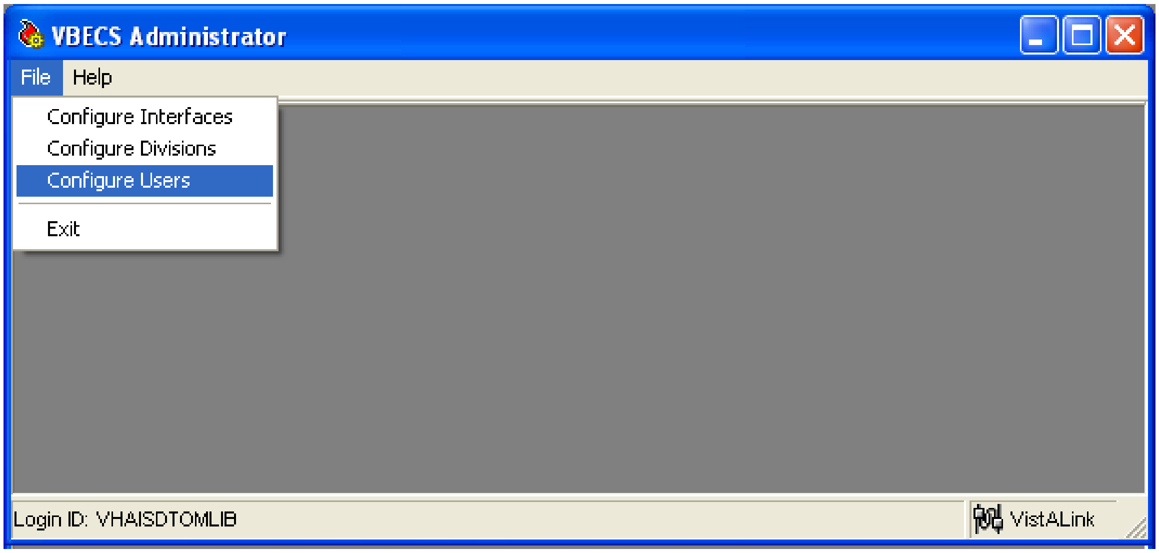
Configure VBECS Users

The Active Directory setup must be completed prior to configuring users in VBECS.

User Action	VBECS Administrator
1. To add and maintain users in VBECS, click **File** on the main menu of the VBECS Administrator software.	• Displays the menu options used to configure VBECS.
2. Select **Configure Users** (Figure 75).	• Allows the user to enter or edit user information.
3. To edit an existing user, select a user ID from the drop-down list (Figure 76) or, to search for a new user ID to add to VBECS, click the **ellipsis** button to the right of the drop-down list (Figure 77). Enter user parameters. For each user, VBECS stores: • VistA DUZ • Windows Login ID • Windows Username • Email Address (optional) • User Initials • Active Status • Division Code • User Role • Division Active Status	• Displays the Windows user ID and name. **NOTES** VistALink lists active VistA Blood Bank users. VistA Blood Bank users are identified by the LRBLOODBANK and LRBLSUPER security keys. When VBECS finds users that are inactive in VistA, it asks whether the user wishes to inactivate them in VBECS. **Yes** inactivates the VBECS users. **No** allows the user to continue without inactivating the users (Figure 80). The user may not edit the VistA DUZ or user name, the Windows login ID or user name, or the division code or name. There is a one-to-one correspondence between Windows and VistA users. A VistA DUZ may be associated with only one Windows login ID and vice versa. The user may: Activate or inactivate but not delete a defined user from VBECS. Rescind a defined user's access privileges at one or more divisions but not delete his record or ID from the database. The user ID stored in VBECS is the user's Windows Logon ID. VBECS displays the data that a user enters in a session. The user may edit and save the data. When a user cancels, VBECS warns that it will not save the data. VBECS closes the form and returns the user to the main menu screen that may include unrelated open windows. VBECS associates the technologist ID, date, time, and division with each process for retrieval by division.
4. To search for a VistA user, click the **ellipsis** button to the right of the VistA DUZ field (Figure 78).	• Allows the user to search for VistA Blood Bank users by name or DUZ. **NOTES** The user may not edit the VistA DUZ or user name, the Windows login ID or user name, or the division code or name.
5. Enter the email address of the user in the E-mail field in the Additional Info group. VistA provides the initials, if available. If	• Allows the user to enter Additional Information about the user for identification. **NOTES**

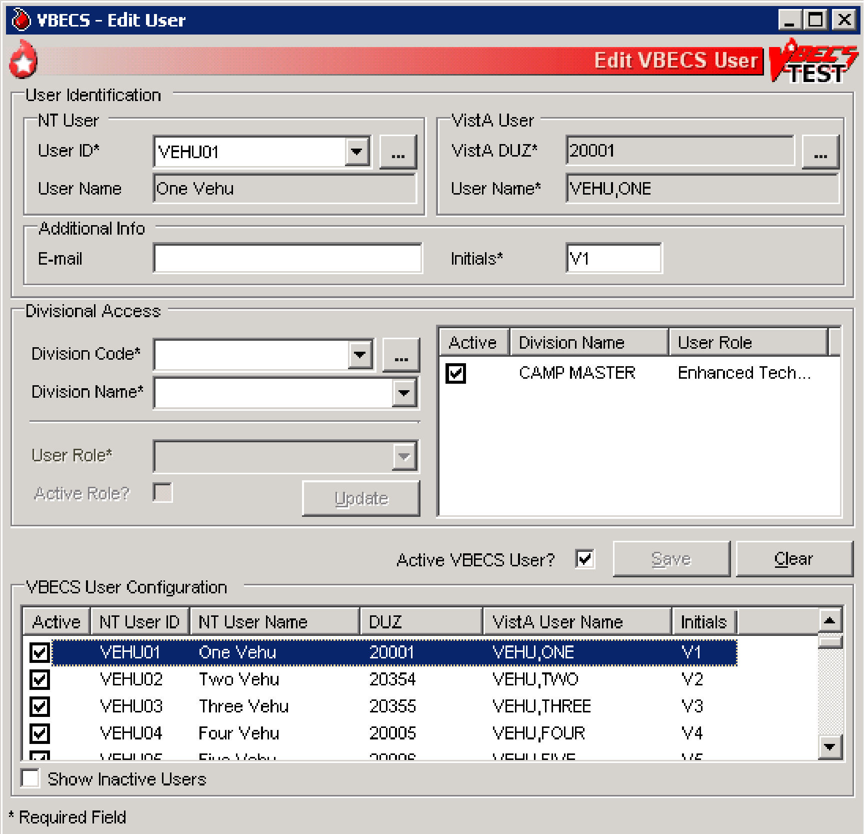
User Action	VBECS Administrator
not, enter them.	User initials may be loaded from VistA. VBECS requires unique user initials for use as the technologist ID.
6. To select a VistA division to associate with the user, click the **ellipsis** button to the right of the Division Code drop-down menu (Figure 79).	• Allows the user to select a division to associate with the user **NOTES** A single user may be associated with multiple divisions.
7. Select a user role from the User Role drop-down menu. Click or clear the **Active Role?** check box to activate or inactivate the role.	• Allows the user to assign security roles to the blood bank user. • If a user was removed from the role of Administrator/Supervisor and was the only Administrator/Supervisor user left for a division, displays "You are trying to remove the last Administrator/Supervisor for your division, which would disallow system configuration in the future. You may not proceed." If all entered data is satisfactory, saves user details and access changes to the file and adds or updates the user information in the list view. **NOTES** One role at a time may be assigned to a user at a division. A user may have only one active user role per division. VBECS allows the assignment of a security level to one or more users at a time. VBECS warns that there must be at least one level 6 VBECS Administrator/Supervisor in the division and does not allow the user to change the last Administrator/Supervisor.
8. Click **Update** and **Save**.	• Displays a confirmation dialog.
9. Click **Yes** to commit changes to the database.	• Click **Yes** to commit changes to the database.
10. To close the Edit Users dialog box, click ☒ in the upper-right corner.	

Figure 75: Example of Configure Users



Login ID: VHAISDTOMLIB

Figure 76: Example of Edit User



User Identification

NT User

User ID* VEHU01

User Name One Vehu

VistA User

VistA DUZ* 20001

User Name* VEHU,ONE

Additional Info

E-mail

Initials* V1

Divisional Access

Division Code*

Division Name*

User Role*

Active Role? □

Active	Division Name	User Role
☑	CAMP MASTER	Enhanced Tech...

Active VBECS User? ☑

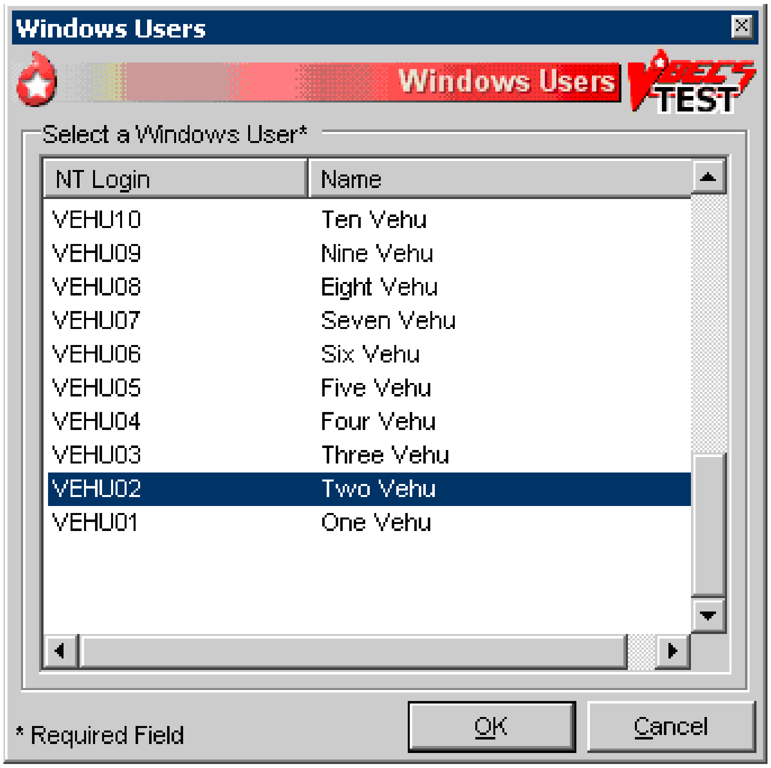
VBECS User Configuration

Active	NT User ID	NT User Name	DUZ	VistA User Name	Initials
☑	VEHU01	One Vehu	20001	VEHU,ONE	V1
☑	VEHU02	Two Vehu	20354	VEHU,TWO	V2
☑	VEHU03	Three Vehu	20355	VEHU,THREE	V3
☑	VEHU04	Four Vehu	20005	VEHU,FOUR	V4
☑	VEHU05	Five Vehu	20006	VEHU,FIVE	V5

□ Show Inactive Users

* Required Field

Figure 77: Example of Windows Users

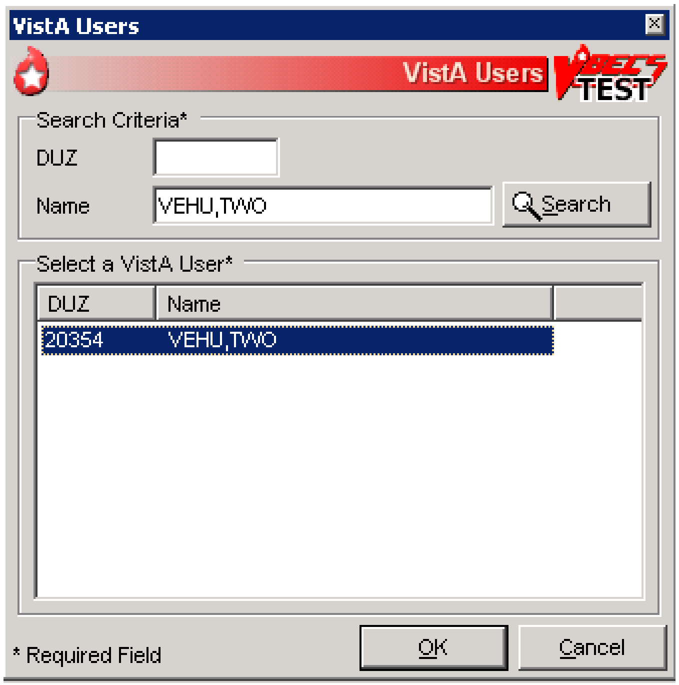


Select a Windows User*

NT Login	Name
VEHU10	Ten Vehu
VEHU09	Nine Vehu
VEHU08	Eight Vehu
VEHU07	Seven Vehu
VEHU06	Six Vehu
VEHU05	Five Vehu
VEHU04	Four Vehu
VEHU03	Three Vehu
VEHU02	Two Vehu
VEHU01	One Vehu

* Required Field

Figure 78: Example of VistA Users



Search Criteria*

DUZ:

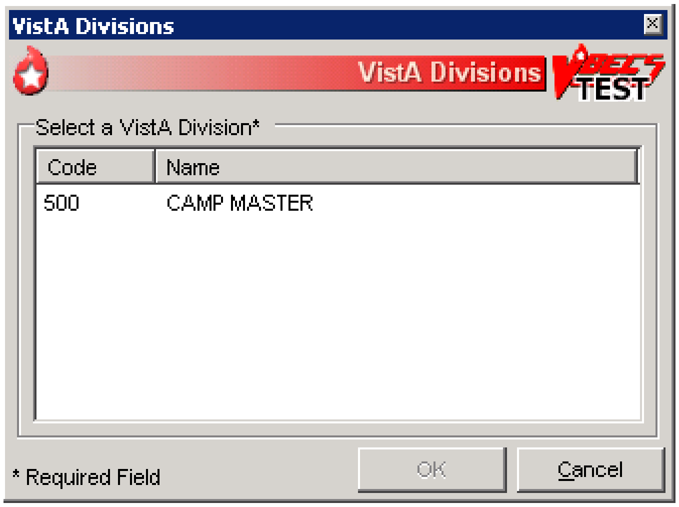
Name: VEHU,TWO

Select a VistA User*

DUZ	Name
20354	VEHU,TWO

* Required Field

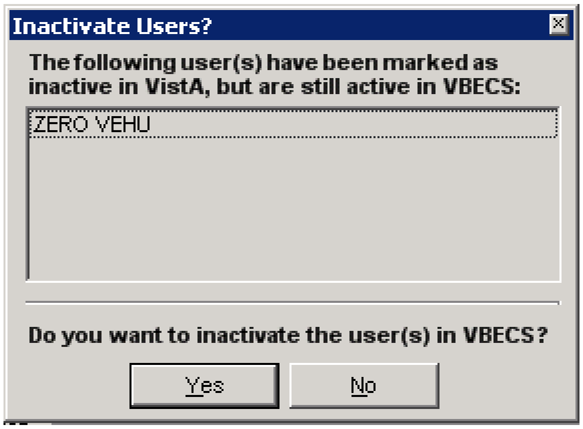
Figure 79: Example of VistA Divisions



Code	Name
500	CAMP MASTER

* Required Field

Figure 80: Example of Inactive Users



The following user(s) have been marked as inactive in VistA, but are still active in VBECS:

ZERO VEHU

Do you want to inactivate the user(s) in VBECS?

Record Workload Data

VBECS workload data is recorded in VBECS when records that qualify as Workload Events are saved in VBECS. This data is transmitted to the VistA Laboratory workload recording system for national and local workload reporting.

Assumptions

Workload codes were assigned to VBECS processes using Workload Codes.
Healthcare Common Procedure Coding System (HCPCS) codes were assigned to blood products using Blood Products.
A record was saved or inactivated immediately preceding workload data collection.
The connection to VistA is active.

Outcome

Information was transmitted to VistA for inclusion in appropriate reports.

Limitations and Restrictions

None

Additional Information

Workload Event data must include information required for Decision Support System (DSS), Patient Care Encounter (PCE), and Billing Awareness. Once in VistA, existing VistA functionality will handle required reporting.

The system accumulates and periodically transmits workload information to the VistA Lab workload recording process. The data is transmitted from VBECS to VistA by the VBECS Workload Capture Remote Procedure called by a nightly Lab background process.

Workload multipliers for all blood bank activities in VistA File #64 must be set to one (1) to avoid excessive Laboratory Management Index Program (LMIP) counts. This allows the workload multiplier set in VBECS to be correctly reflected on VistA reports.

User Roles with Access to This Option

All users

Transmit Workload Data

These steps are associated with the “Save” function within any class that performs a Workload Event such as recording a blood test result or interpretation for a unit or a patient, modifying a unit, and pooling units. VBECS must know which classes perform Workload Events and how to classify the work accomplished for reporting. When the database is updated, the VistA technologist ID of the updater, the division, and the date and time of the update are recorded. In some instances, a mechanism to capture LMIP workload information exists. In addition, for certain events that involve patient processing, the patient location, treating specialty, service, etc., are captured to satisfy PCE or DSS reporting requirements.

These steps address the initial recording of these events.

User Action	VBECS
1. Click **Save** to save a record from an option.	Creates a Workload Event for every process record saved. Recognizes the activity as a new Workload Event. Checks for required reporting properties based on the type of record being saved. Determines the proper workload codes and other related information to be included. **NOTES** One or more workload codes can be collected with each Workload Event saved. A workload code may be multiplied for certain Workload Events.
2. Exit.	

Inactivate a Workload Event

VBECS updates VistA to inactivate the associated workload information (for a patient or a unit) so that PCE and Billing Awareness can be updated to reflect that the transaction is not valid.

User Action	VBECS
1. Inactivate a saved record.	Recognizes the activity performed as an inactivation of an existing Workload Event record. **NOTES**
2. Complete the update and choose to save.	Prompts to confirm the save. Saves workload data. **NOTES** When a previously saved workload-generating event is invalidated (such as in Remove Final Status, Invalidate Test Results, or invalidating previously logged-in units through Edit Unit Information or Invalidate Shipment), VBECS must create and transmit the same Workload Event information to VistA as a negative number.
3. Confirm the save.	Saves workload data. **NOTES** When a saved Workload Event is associated with a patient, VBECS needs to link the Workload Event to the patient for future reports.
4. The option ends when the record is saved.	

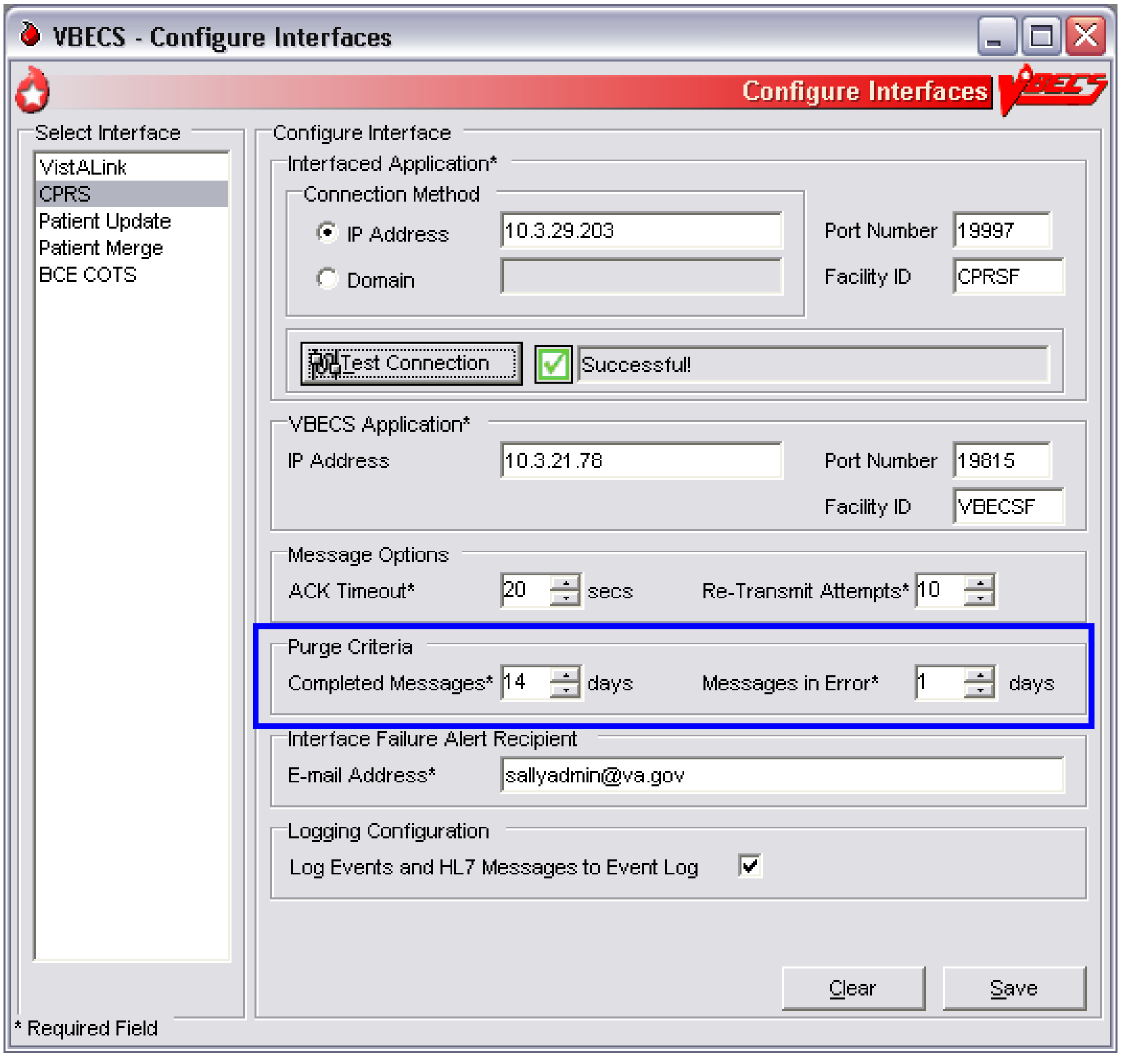
This page intentionally left blank.

External Interfaces

Purging the HL7 Message Log

The purge criteria for HL7 messages stored in VBECS can be set in VBECS Administrator (Figure 81). There are values for completed messages and error messages. When a user logs into VBECS, the current messages in the table are checked against the current criteria and any matching messages are deleted.

Figure 81: Example of VBECS Configure Interfaces HL7 Message Log Purge



Interfaced Application*

Connection Method

● IP Address 10.3.29.203

○ Domain

Port Number 19997

Facility ID CPRSF

✓ Successful!

VBECS Application*

IP Address 10.3.21.78

Port Number 19815

Facility ID VBECSF

Message Options

ACK Timeout* 20 secs

Re-Transmit Attempts* 10

Purge Criteria

Completed Messages* 14 days

Messages in Error* 1 days

Interface Failure Alert Recipient

E-mail Address* sallyadmin@va.gov

Logging Configuration

Log Events and HL7 Messages to Event Log ☑

VistALink Remote Procedure Calls

Remote Procedure Calls (RPCs) provide a method of data exchange through VistALink for VBECS. The VBECS software provides data to or receives data from the VBECS Application Interfacing Support Software (VAISS) located in the VistA M environment through RPCs. This data exchange is controlled through Database Integration Agreements (DBIAs) between the blood bank medical device software and the VAISS VistA M software.

The VAISS software provides a set of M Application Programmer Interfaces (APIs) that call VBECS RPCs through the VBECS VistALink Listener Windows Service and return blood bank data to other VistA applications. The VAISS software also provides a set of VistA RPCs under the VBECS namespace in the Remote Procedure File (#8994) that are called by the VistA VistALink Listener client-server software. These calls are not public utilities and may be subject to change.

Table 9: Remote Procedure Calls

RPC Name	Database Integration Agreement (DBIA)	This RPC:
VBECS Order Entry	4619	Supports order entry of blood bank requests from the blood bank order entry dialog in CPRS
VBECS Patient Available Units	4620	Provides a list of assigned, crossmatched, autologous and directed blood units that are available for a patient
VBECS Patient Transfusion History	4621	Provides a list of past transfusions performed for a patient
VBECS Blood Products	4622	Provides a list of orderable blood products, or component classes, to the VistA Surgery package
VBECS Patient Report	4623	Provides patient specimen testing results, component requests, and available blood units for a patient to be displayed in CPRS
VBECS Patient ABO_RH	4624	Provides the most current ABO Group and Rh Type identified for a patient
VBECS Patient ABID	4625	Provides a list of antibodies identified for a patient
VBECS Patient TRRX	4626	Provides a list of transfusion reactions for a patient
VBECS Workload Capture	4627	Provides blood bank workload data to the VistA Laboratory Service package for workload reporting to national and local entities
VBECS Workload Update Event	4628	Inserts completed workload-related data into the VBECS database after the VistA Laboratory Services package has completed workload-reporting transactions. Upon completion of the insert, the RPC returns an XML response to the VAISS that initiated the communication indicating a successful or unsuccessful transaction.
VBECS Accession Area Lookup	4607	Provides a list of all Laboratory Blood Bank Accession Areas in VistA and their associated divisions to VBECS for workload reporting purposes
VBECS Blood Bank User Lookup	4608	Returns a list of all blood bank users identified in the VistA system to VBECS. Blood bank users are identified by the Security Keys of either LRBLOODBANK or LRBLSUPER.
VBECS Division Lookup	4609	Returns a list of all VAMC divisions associated with a VistA system
VBECS HCPCS Codes Lookup	4610	Returns a list of blood bank related HCPCS codes to be associated with processes, or procedures, performed in VBECS
VBECS Laboratory Test Lookup	4611	Returns a list of VistA Laboratory tests to be associated with blood components in VBECS
VBECS Lab Test Results Lookup	4612	Returns a list of VistA Laboratory test results for a patient
VBECS Medication Profile Lookup	4613	Returns a list of medications for a patient from the VistA Pharmacy package
VBECS Lab Accession UID Lookup	4614	Returns data from the VistA Laboratory Services package based on a Lab order number. The data is used to validate a

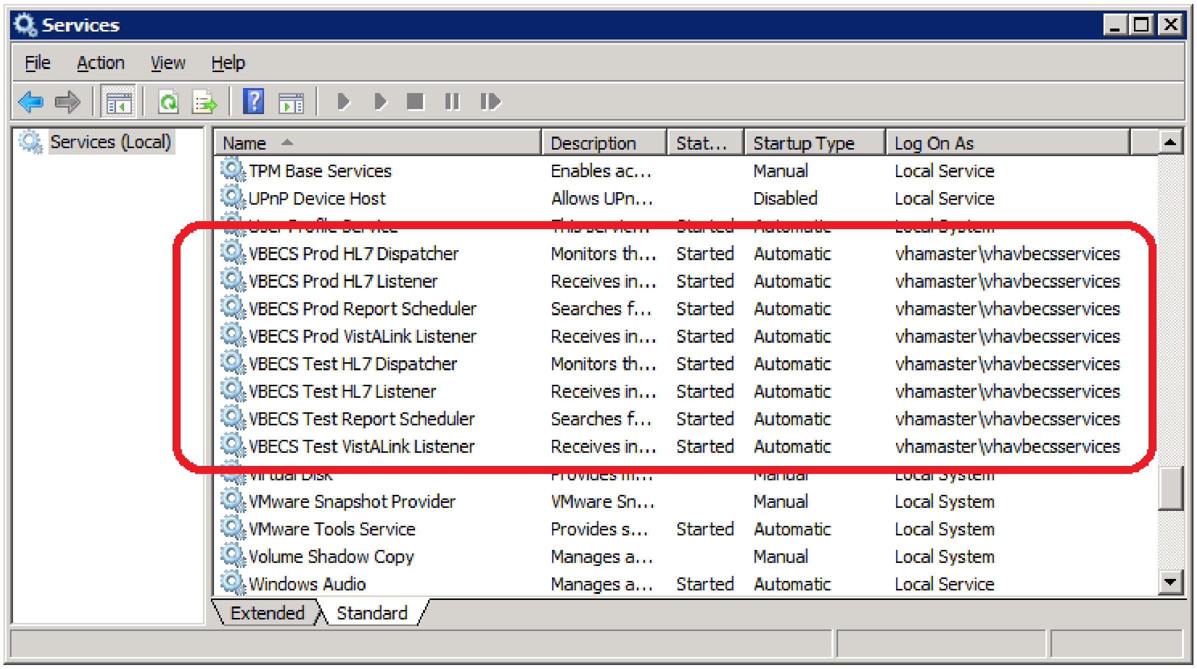
RPC Name	Database Integration Agreement (DBIA)	This RPC:
		VBECS specimen test request for a patient and specimen received in the blood bank for that test.
VBECS Workload Codes Lookup	4615	Returns a list of blood bank related workload related data that is associated with processes in VBECS
VBECS Patient Lookup	4616	Provides a patient lookup function using standard VistA patient lookup criteria. A list of matching patients found in the lookup is returned to VBECS along with required patient identifiers and demographics.
VBECS Provider Lookup	4617	Provides a lookup of VistA users that hold the PROVIDER security key
VBECS Hospital Location Lookup	4618	Returns a list of hospital locations associated with a division in VistA
VBECS Lab Order Lookup by UID	4633	Returns a list of Laboratory Services data related to an order based on a specimen UID
VBECS Dss Extract	4956	Provides BloodBank post-transfusion related data to the VistA DSS Blood Bank Extract application for DSS reporting

VBECS Windows Services

Changes made to individual HL7 listeners must be validated in the test account before using in production.

VBECS uses Microsoft Windows Services (services) to provide minimal downtime and minimal user interaction. These services are installed on each VBECS application server. For details on stopping and starting VBECS services, see the Stopping VBECS Services and Starting VBECS Services sections. All VBECS services start with the VBECS namespace prefix. There are duplicate services for production and test accounts that provide functionality for their respective databases. See Figure 82 for a complete listing of VBECS services.

Figure 82: Example of VBECS Services



Name	Description	Stat...	Startup Type	Log On As
TPM Base Services	Enables ac...		Manual	Local Service
UPnP Device Host	Allows UPn...		Disabled	Local Service
User Profile Service	This service...	Started	Automatic	Local System
VBECS Prod HL7 Dispatcher	Monitors th...	Started	Automatic	vhamaster\vhavbecsservices
VBECS Prod HL7 Listener	Receives in...	Started	Automatic	vhamaster\vhavbecsservices
VBECS Prod Report Scheduler	Searches f...	Started	Automatic	vhamaster\vhavbecsservices
VBECS Prod VistALink Listener	Receives in...	Started	Automatic	vhamaster\vhavbecsservices
VBECS Test HL7 Dispatcher	Monitors th...	Started	Automatic	vhamaster\vhavbecsservices
VBECS Test HL7 Listener	Receives in...	Started	Automatic	vhamaster\vhavbecsservices
VBECS Test Report Scheduler	Searches f...	Started	Automatic	vhamaster\vhavbecsservices
VBECS Test VistALink Listener	Receives in...	Started	Automatic	vhamaster\vhavbecsservices
Virtual Disk	Provides m...		Manual	Local System
VMware Snapshot Provider	VMware Sn...		Manual	Local System
VMware Tools Service	Provides s...	Started	Automatic	Local System
Volume Shadow Copy	Manages a...		Manual	Local System
Windows Audio	Manages a...	Started	Automatic	Local Service

Table 10: VBECS Windows Services

Windows Service Name	Description
VBECS Prod HL7 Dispatcher	The startup type is set to automatic. It polls the VBECS Production database for HL7 messages to be sent to CPRS or BCE in the VistA Production account. If the BCE interface is disabled through our VBECS Admin, no BCE messages will be sent from BCE. When the BCE interface is enabled, you will still not send any BCE messages until you stop and start this service.
VBECS Prod HL7 Listener	The startup type is set to automatic. This is the default HL7 listener service for all Production HL7 interfaces. If the BCE interface is disabled through our VBECS Admin, no BCE messages will be received from BCE. When the BCE interface is enabled, you will still not send any BCE messages until you stop and start this service.
VBECS Prod Report Scheduler	The startup type is set to automatic. It runs scheduled VBECS reports for the Production database.
VBECS Prod VistALink Listener	The startup type is set to automatic. It provides a client-server TCP/IP listener service for VistALink RPC XML messages from the VAISS APIs. It calls VBECS RPCs to provide blood bank data from the VBECS Production database to VistA Production account applications.
VBECS Test HL7 Dispatcher	The startup type is set to automatic. It polls the VBECS Test database for HL7 messages to be sent to CPRS or BCE in the VistA Test account. If the BCE interface is disabled through our VBECS Admin, no BCE messages will be sent or received from BCE. When the BCE interface is enabled, you will still not send any BCE messages until you stop and start this service.
VBECS Test HL7 Listener	The startup type is set to automatic. This is the default HL7 listener service for all Test HL7 interfaces.
VBECS Test Report Scheduler	The startup type is set to automatic. It runs scheduled VBECS reports for the Test database.
VBECS Test VistALink Listener	The startup type is set to automatic. It provides a client-server TCP/IP listener service for VistALink RPC XML messages from the VAISS APIs. It calls VBECS RPCs to provide blood bank data from the VBECS Test database to

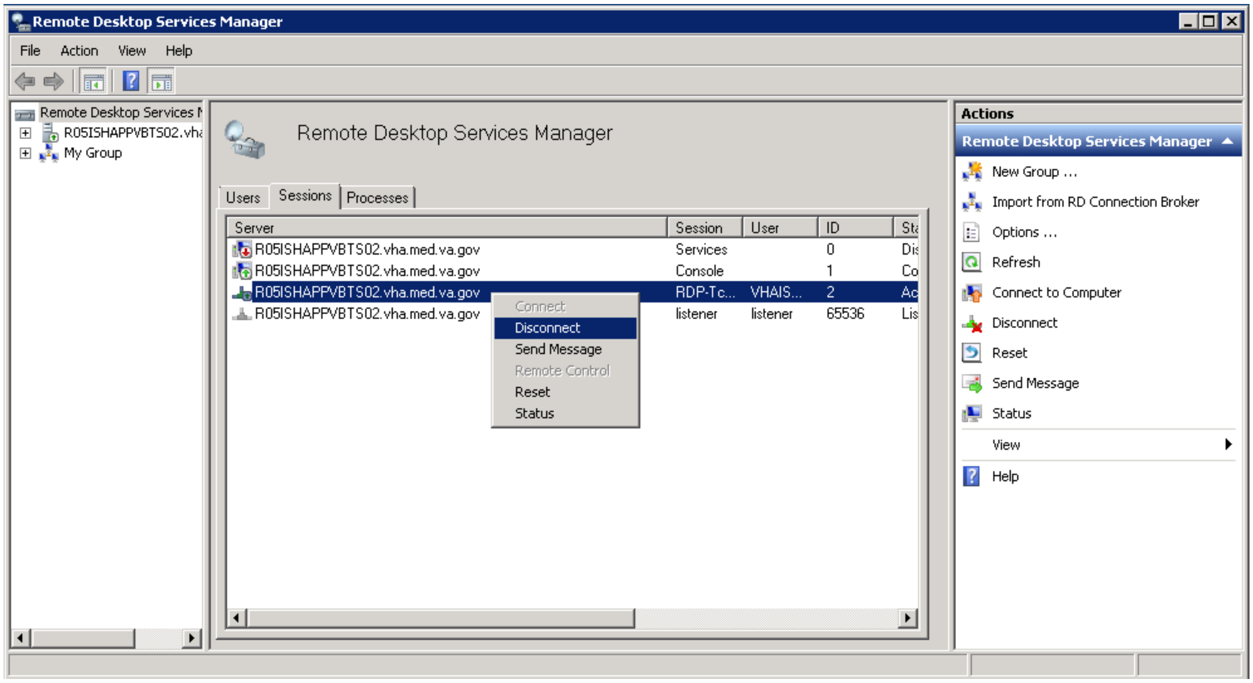
Windows Service Name	Description
	VistA Test account applications.

Troubleshooting

Remote Desktop Session Issues (Enterprise Operations Only)

Occasionally remote desktop sessions require disconnection by an administrator. Sessions may become unresponsive and require disconnection. Additionally if you need to apply a patch such as a window update but sessions remain on the server you may need to force a session to disconnect. To disconnect a remote session navigate to the application or SQL server and click Start, Administrative Tools, Remote Desktop Services, Remote Desktop Services Manager. Locate the session(s) that require disconnection. Right click on the session and select Disconnect (Figure 83).

Figure 83: Example of Remote Desktop Services Manager

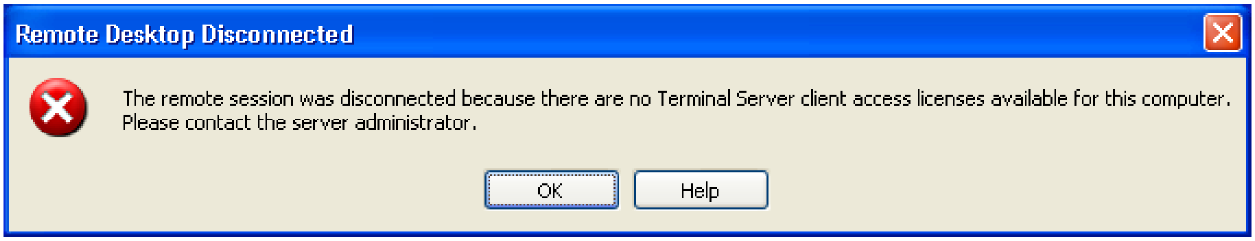


Server	Session	User	ID	Sta
R05ISHAPPVBTS02.vha.med.va.gov	Services		0	Dis
R05ISHAPPVBTS02.vha.med.va.gov	Console		1	Co
R05ISHAPPVBTS02.vha.med.va.gov	RDP-Tc...	VHAIS...	2	Ac
R05ISHAPPVBTS02.vha.med.va.gov	listener	listener	65536	Lis

Remote Desktop Services Licensing Issues

In order to connect to VBECS, a workstation must have a valid license from an active Remote Desktop Services licensing server. A problem may occur when this license has expired on the workstation; the user receives an error message when trying to establish a Remote Desktop Connection (Figure 84). Deleting the Remote Desktop Services license information from the registry will cause the workstation to refresh its license information and restore the ability to connect using remote desktop.

Figure 84: Example of Expired Remote Desktop License



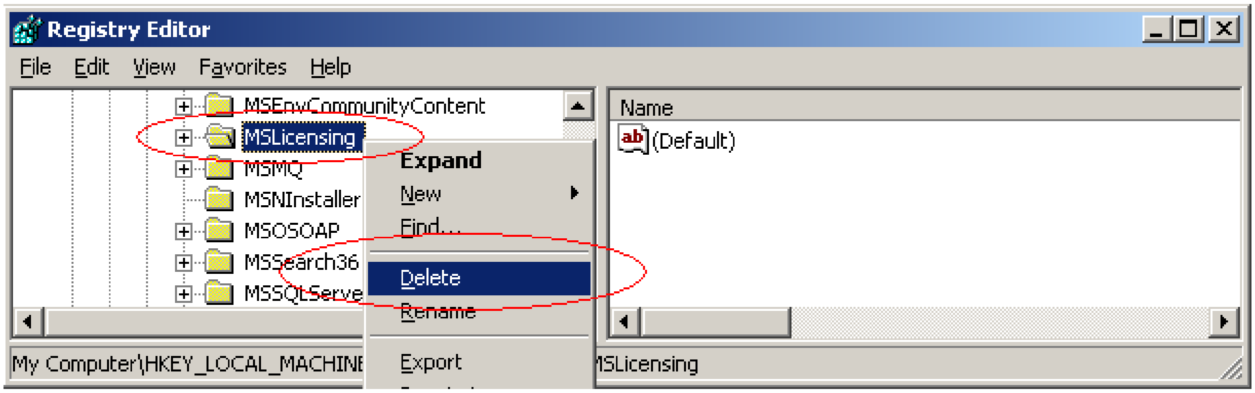
The remote session was disconnected because there are no Terminal Server client access licenses available for this computer. Please contact the server administrator.

Deleting the Remote Desktop Services Licensing Information on a VBECS Workstation

Administrative rights on the workstation are required to perform the following steps.

1) Log into the workstation that is receiving the error (Figure 84) and click **Start, Run…**
2) In the Run window, type **regedit** and click **Enter**.
3) In the Registry Editor window, expand the folders to the following location: **Computer, HKEY_LOCAL_MACHINE, SOFTWARE, Microsoft**.
4) Locate and right-click the **MSLicensing** folder; select **Delete** (Figure 85).

Figure 85: Deleting the MSLicensing Registry Key



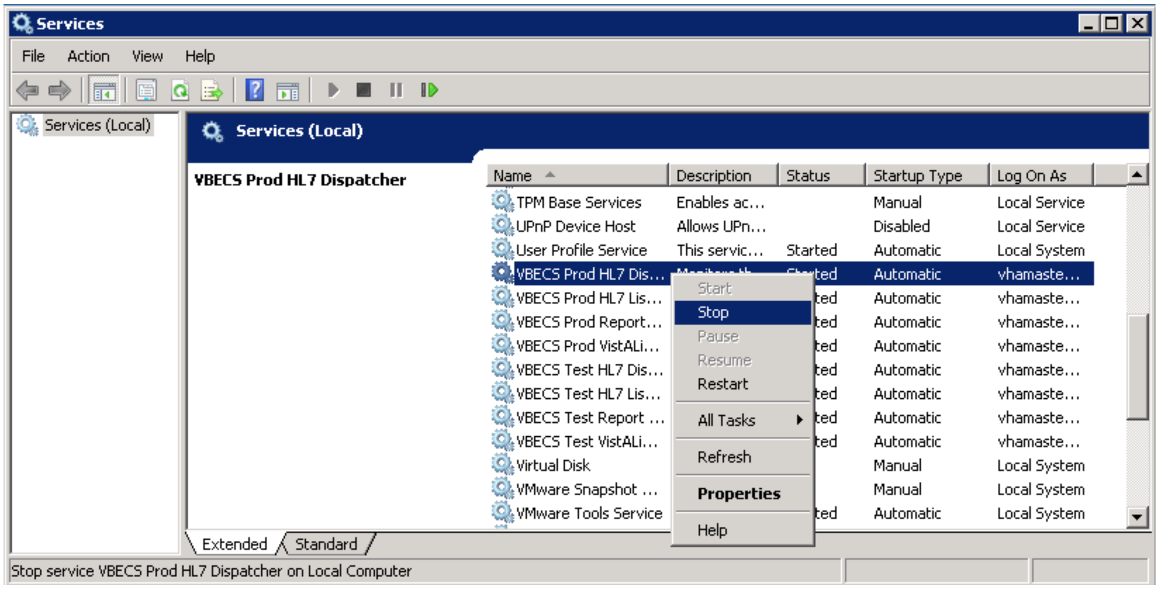
5) Make sure you are at the correct path and click **Yes** to confirm the deletion.
6) Close the Registry Editor.

Stopping and Starting VBECS Services (Enterprise Operations Only)

Stopping VBECS Services

1) Click **Start, Administrative Tools, Services** (Figure 86).
2) Right-click on the service you would like to stop and click **Stop**.

Figure 86: Example of Stopping a VBECS Service



VBECS Prod HL7 Dispatcher

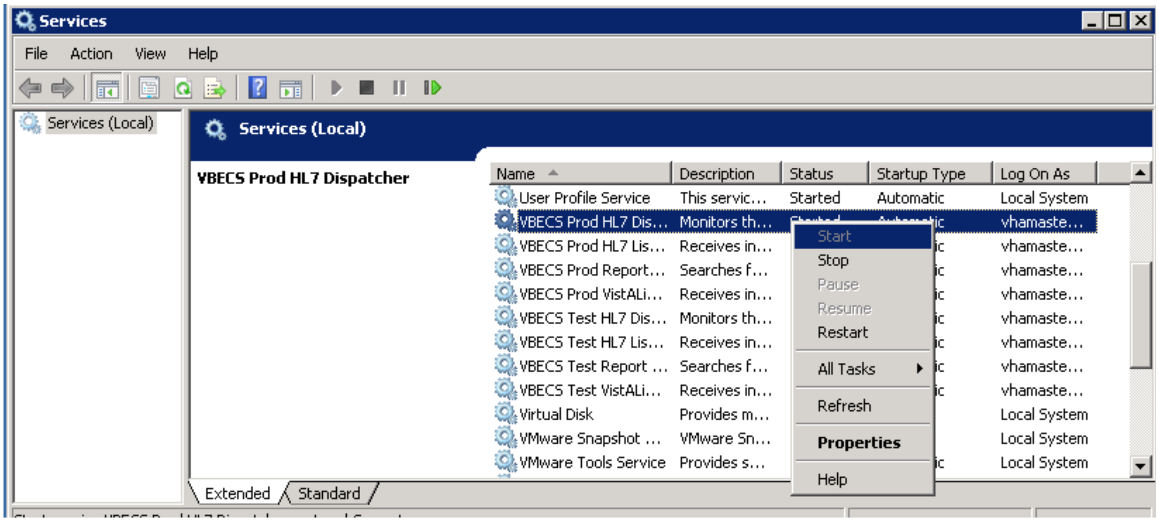
Name	Description	Status	Startup Type	Log On As
TPM Base Services	Enables ac…		Manual	Local Service
UPnP Device Host	Allows UPn…		Disabled	Local Service
User Profile Service	This servic…	Started	Automatic	Local System
VBECS Prod HL7 Dis…	Monitors th…	Started	Automatic	vhamaste…
VBECS Prod HL7 Lis…		ted	Automatic	vhamaste…
VBECS Prod Report…		ted	Automatic	vhamaste…
VBECS Prod VistALi…		ted	Automatic	vhamaste…
VBECS Test HL7 Dis…		ted	Automatic	vhamaste…
VBECS Test HL7 Lis…		ted	Automatic	vhamaste…
VBECS Test Report …		ted	Automatic	vhamaste…
VBECS Test VistALi…		ted	Automatic	vhamaste…
Virtual Disk			Manual	Local System
VMware Snapshot …			Manual	Local System
VMware Tools Service		ted	Automatic	Local System

Stop service VBECS Prod HL7 Dispatcher on Local Computer

Starting VBECS Services

1) Click **Start, Administrative Tools, Services** (Figure 87).
2) Right-click on the service you would like to start and click **Start**

Figure 87: Example of Starting a VBECS Service



VBECS Prod HL7 Dispatcher

Name	Description	Status	Startup Type	Log On As
User Profile Service	This servic…	Started	Automatic	Local System
VBECS Prod HL7 Dis…	Monitors th…	Started	Automatic	vhamaste…
VBECS Prod HL7 Lis…	Receives in…		ic	vhamaste…
VBECS Prod Report…	Searches f…		ic	vhamaste…
VBECS Prod VistALi…	Receives in…		ic	vhamaste…
VBECS Test HL7 Dis…	Monitors th…		ic	vhamaste…
VBECS Test HL7 Lis…	Receives in…		ic	vhamaste…
VBECS Test Report …	Searches f…		ic	vhamaste…
VBECS Test VistALi…	Receives in…		ic	vhamaste…
Virtual Disk	Provides m…			Local System
VMware Snapshot …	VMware Sn…			Local System
VMware Tools Service	Provides s…		ic	Local System

VBECS Exception Logging (Enterprise Operations Only)

VBECS logs all errors that occur in the system in the Application log of Event Viewer on the application server. A user defined as an administrator on the application server can connect to the server through Remote Desktop Connection to view these errors.

- Click **Start**, **Control Panel, Administrative Tools**.
- Open the Event Viewer and open the Windows logs folder, then select Application to view the errors that VBECS logs.
- In the list view on the right side of the screen, click the date column header to sort the errors by date.
- Evaluate “Error” and warning errors that were logged at the same time a VBECS user reported an error. Ignore informational messages. If you require assistance from the VBECS maintenance and maintenance team, file a support ticket (Service Desk Primary Contact).

VBECS Application Interfaces

When the HL7 Listener service encounters an error parsing an HL7 message it generates an event description like the following:

```
VBECS Patient Update HL7 Parser: Error processing HL7 message:
Missing or invalid content in HL7 message:
ERR^MSH~1~12~203~
```

Upon troubleshooting an email message regarding an HL7 message, file a ticket with the Service Desk and include the contents of the email for a description so that Health Product Support can assist in identifying the patient associated with the failed HL7 message. Due to PII and HIPAA contraints, patient information will not be sent over email. Product support will have access to the event viewer and be able to identify the appropriate patient information.Table 11 describes the ERR codes (e.g., 203 like in the above example) descriptions.

Table 11: Troubleshooting Rejected VBECS HL7 Messages

Error Code	Description of Problem
100	Segment Sequence Error
101	Required Field Missing
102	Data Type Error
103	Table Value Not Found
200	Unsupported Message Type
201	Unsupported Event Code
202	Unsupported Processing ID
203	Unsupported Version Id See Table 12: VBECS HL7 Versions
204	Unknown Key Identifier
205	Duplicate Key Identifier
206	Application Record Locked
207	Application Internal Error
208	Conflicting Processing Id

Table 12: VBECS HL7 Versions

HL7 Interface	HL7 Version

VistA CPRS- Order Update – CPRS OERR	2.4
VistA PIMS Patient ADT Update – VAFC ADT	2.3
VistA MPI/PD PatientMerge – MPI TRIGGER	2.4
BCE COTS – Patient Blood Product Transfusion Verification	2.5

Table 13: Troubleshooting VBECS Application Interfaces

Source	Description of Problem	Possible Cause	Solution
VBECS: Order Alerts and Pending Order List	New orders or cancellations of existing orders in CPRS are not showing up in VBECS.	The OERR-VBECS Logical Link is not running on the VistA system.	Start the OERR-VBECS Logical Link.
		The VBECS <Prod or Test> HL7 Listener Windows Service is not running or is locked on the application server.	Start or restart the VBECS <Prod or Test> HL7 Listener Windows Service.
		Network connectivity issue	Contact local system support.
		The HL7 message is missing patient last or first name or one or more name components length(s) exceed(s) the VBECS maximum supported value.	VBECS responds to the new order request with an application reject (AR) acknowledgement message indicating Patient Name(s) not found in HL7 Message or Patient's Name(s) field size(s) exceed(s) VBECS maximum supported value. Rejected patient order messages due to invalid patient name message content are recorded on the Windows Event Log and an email message containing the MSH segment of the rejected HL7 message.
VBECS Admin: Configure Division	New orders are not showing up in VBECS.	Order mappings to institutions within a division’s configuration were changed.	Stop and restart the VBECS <Prod or Test> HL7 Listener Service.
VBECS: Patient Update Alerts	VistA patient updates are not showing up in VBECS.	The patient being updated in VistA is not in the VBECS Patient table and is, therefore, not a blood bank patient.	No action is required.
		The fields that were updated in VistA are not stored in VBECS; therefore, no data will be updated.	No action is required.
		The Taskman scheduled option VAFC BATCH UPDATE is not scheduled to run or has not reached the time limit in the schedule.	Schedule the VAFC BATCH UPDATE option to run at the desired increment or use the option “One-time Option Queue” in the Taskman Management Options to start the task.
		The VBECSPTU Logical Link is not running on the VistA system.	Start the VBECSPTU Logical Link.

Source	Description of Problem	Possible Cause	Solution
		The VBECS <Prod or Test> HL7 Listener Windows Service is not running or is locked on the application server.	Start or restart the VBECS <Prod or Test> HL7 Listener Windows Service.
		Network connectivity issue	Contact local system support.
		The HL7 message is missing patient last or first name or one or more name components length(s) exceed(s) the VBECS maximum supported value.	VBECS responds to the patient update request with an application reject (AR) acknowledgement message indicating Patient Name(s) not found in HL7 Message or Patient's Name(s) field size(s) exceed(s) VBECS maximum supported value. Rejected patient update messages due to invalid patient name message content are recorded on the Windows Event Log and an email message containing the MSH segment of the rejected HL7 message as a means to identify the message in the server event log is sent to the interface failure alert recipient set in VBECS Administrator for immediate action.
VBECS: Patient Merge Alerts	VistA Patient Merge events are not showing up in VBECS.	The two patient identifiers in the merge do not exist in VBECS and, therefore, cannot be merged.	No action is required.
		The VBECPTM Logical Link is not running on the VistA system.	Start the VBECSPTM Logical Link.
		The VBECS <Prod or Test> HL7 Listener Windows Service is not running or is locked on the application server.	Start or restart the VBECS <Prod or Test> HL7 Listener Windows Service.
		Network connectivity issue	Contact local system support.
		The HL7 message is missing patient last or first name or one or more name components length(s) exceed(s) the VBECS maximum supported value.	Failed patient merge messages due to invalid patient name message content are recorded on the Windows Event Log and an email message containing the MSH segment of the rejected HL7 message as a means to identify the message in the server event log is sent to the interface failure alert recipient set in VBECS Administrator for immediate action.

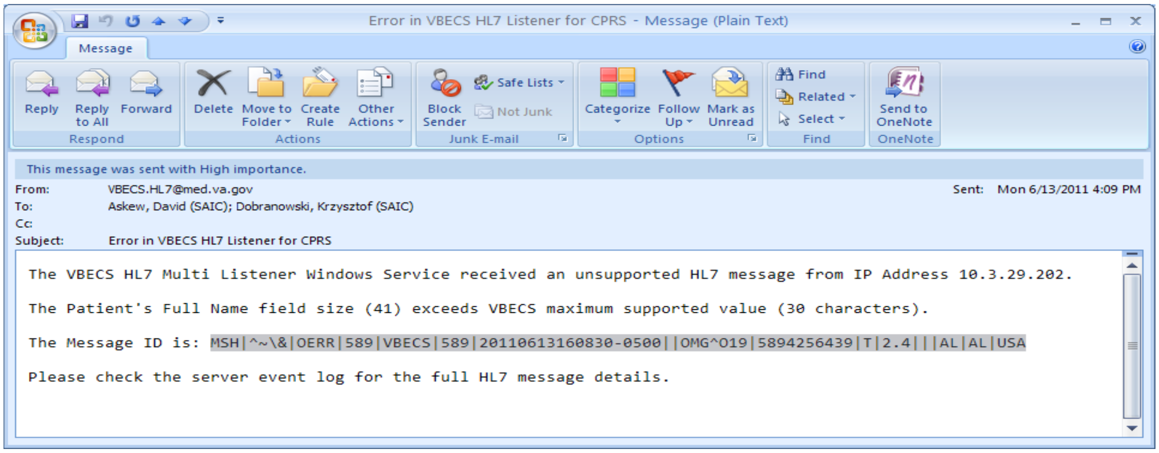
Source	Description of Problem	Possible Cause	Solution
VistA: HL7 System Link Monitor	The VistA HL7 System Link Monitor shows more MESSAGES TO SEND than MESSAGES SENT for the OERR-VBECS Logical Link and is hung in an “Open” state.	The VBECS <Prod or Test> HL7 Listener Windows Service is not running or is locked on the VBECS Application server.	Start or restart the VBECS <Prod or Test> HL7 Listener Windows Service.
		Network connectivity issue	Contact local system support.
	The VistA HL7 System Link Monitor shows more MESSAGES TO SEND than MESSAGES SENT for the VBECSPTU Logical Link and is hung in an “Open” state.	The VBECS <Prod or Test> HL7 Listener Windows Service is not running or is locked on the VBECS Application server.	Start or restart the VBECS <Prod or Test> HL7 Listener Windows Service.
		Network connectivity issue.	Contact local system support.
	The VistA HL7 System Link Monitor shows more MESSAGES TO SEND than MESSAGES SENT for the VBECSPTM Logical Link and is hung in an “Open” state.	The VBECS <Prod or Test> HL7 Listener Windows Service is not running or is locked on the application server.	Start or restart the VBECS <Prod or Test> HL7 Listener Windows Service.
		Network connectivity issue.	Contact local system support.
CPRS: Orders Tab	CPRS does not display the correct status of a blood bank order after it was updated in VBECS.	The VBECS <Prod or Test> HL7 Dispatcher Windows Service is not running or is locked on the application server.	Start or restart the VBECS <Prod or Test> HL7 Dispatcher Windows Service.
		The VBECS-OERR Logical Link is not running.	Start the VBECS-OERR Logical Link in Background mode.
		Network connectivity issue	Contact local system support.
CPRS: Blood Bank Order Dialog	CPRS displays “Not able to open port” message in Patient Information screen in Blood Bank Order Dialog.	The VBECS <Prod or Test> VistALink Listener Service is not running or is locked on the VBECS Application server.	Start or restart the VBECS <Prod or Test> VistALink Listener Service.
		Network connectivity issue	Contact local system support.
CPRS: Reports Tab, Blood Bank Report	CPRS displays “----BLOOD BANK REPORT IS UNAVAILABLE----“	The VBECS <Prod or Test> VistALink Listener is not running or is locked on the VBECS Application server.	Start or restart the VBECS <Prod or Test> VistALink Listener Service.
		Network connectivity issue.	Contact local system support.
		Incorrect parameters file	Verify settings are pointing to the correct VBECS application server and port.
CPRS: Blood Bank Order Dialog: Signing an Order	CPRS displays an “Error Saving Order” dialog screen with the text “The error, One or more orders to the VBECS system failed and are queued for later delivery.”	An error occurred in the VBECS <Prod or Test> HL7 Listener Windows Service, which caused a failure to respond to CPRS with acceptance.	Log onto the application server and review the System Application Event Log for error details.
		Network connectivity issue.	Contact local system support.

Source	Description of Problem	Possible Cause	Solution
VBECS Application Server Application Event Log: Source is VBECS SimpleListener	An application error has been logged to the Event Log where the Message under Exception Information is “Could not access ‘CDO.Message’ object.”	The VBECS <Prod or Test> HL7 Listener Windows Service has encountered an error trying to send an email message to the Interface Administrator.	Disable port 25 blocking in McAfee. Open the VirusScan Console and select Access Protection. Click the Task menu option, the Properties. Uncheck Prevent mass mailing worms from sending mail, port 25 under Ports to block.
	An application warning was logged in the Event Log with the description stating, “An unsupported HL7 message was received from IP Address *[IP address]*.” The IP address in the description of the error will indicate where the message is coming from.	If the IP address is associated with the local VistA system, the HL7 Application Parameters in VistA were not set up correctly for the supported protocols.	Refer to the VBECS Application Interfacing Support Software Installation and User Configuration Guide for HL7 setup procedures in VistA.
		If the IP address is not from the local VistA system, a rogue HL7 system is sending messages to the VBECS server.	Contact IRM to identify the location of the server with which the IP address is associated. Notify the site that the message is coming from the problem so that the messages can be routed to the correct location.
VBECS Application Server Application Event Log: Source is VBECS HL7 MailServer	An application error was logged in the Event Log with the source of VBECS HL7 MailServer where the Message under Exception Information is, “Could not access ‘CDO.Message’ object.”	The VBECS <Prod or Test> HL7 Listener Windows Service encountered an error trying to send an email message to the Interface Administrator.	Disable port 25 blocking in McAfee. Open the VirusScan Console and select Access Protection. Click the Task menu option, Properties. Uncheck Prevent mass mailing worms from sending mail, port 25 under Ports to block.
VBECS Application Server Application Event Log: Source is CPRS HL7 Parser	An HL7 message sent from CPRS to VBECS was rejected. The description in the Event Log is “Exception message: Division [*division]* is not supported by this instance of VBECS.”	An invalid or unsupported division associated with the Patient Location was selected in CPRS when the order was created.	The order must be created in CPRS again with a valid Patient Location associated with a VBECS-supported division.
	An HL7 message sent from CPRS to VBECS was rejected. The description in the Event Log is “Exception message: Unable to find valid Associated Institutions information. Please check configuration in VBECS Admin.”	Clinician logs into VistA with a division that is not mapped to VBECS.	The order must be created in CPRS again with a division that is mapped to VBECS.

Finding Application Log Entries from Email Alerts (Enterprise Operations Only)

1) When HL7 message patient last or first name components length(s) exceed(s) the VBECS maximum supported value of 30, an email will be received (Figure 88). See the Configure CPRS HL7 Interface Parameters for email configuration.

Figure 88: Example of Error in VBECS HL7 Listener for CPRS



This message was sent with High importance.

From: VBECS.HL7@med.va.gov

Sent: Mon 6/13/2011 4:09 PM

To: Askew, David (SAIC); Dobranowski, Krzysztof (SAIC)

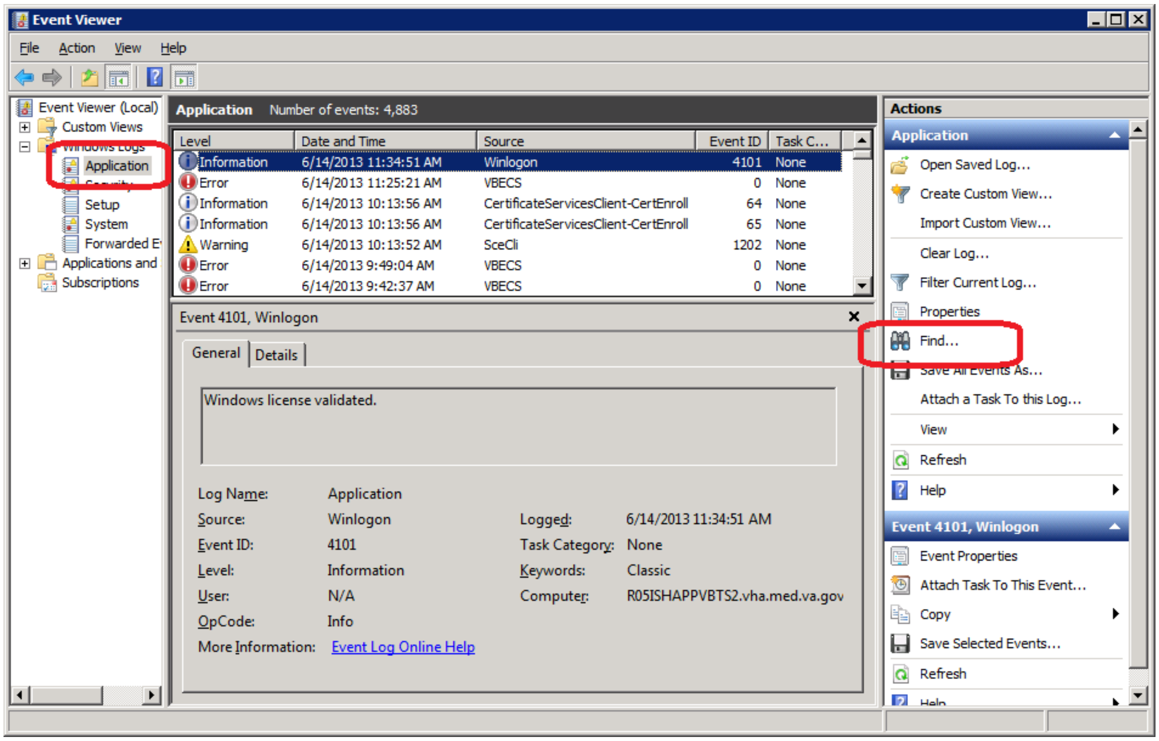
Cc:

Subject: Error in VBECS HL7 Listener for CPRS

```
The VBECS HL7 Multi Listener Windows Service received an unsupported HL7 message from IP Address 10.3.29.202.

The Patient's Full Name field size (41) exceeds VBECS maximum supported value (30 characters).

The Message ID is: MSH|^~\&|OERR|589|VBECS|589|20110613160830-0500||OMG^O19|5894256439|T|2.4|||AL|AL|USA

Please check the server event log for the full HL7 message details.
```

2) On the Application Server, click **Start, Administrative Tools, Event Viewer**.
3) On the Event Viewer Window, expand the **Windows Logs** and click on **Application** in the left-hand tree; click the top event in the log table, then click **Find** on the right side of the window (Figure 89).

Figure 89: Example of Event Viewer



Application Number of events: 4,883

Level	Date and Time	Source	Event ID	Task C…
Information	6/14/2013 11:34:51 AM	Winlogon	4101	None
Error	6/14/2013 11:25:21 AM	VBECS	0	None
Information	6/14/2013 10:13:56 AM	CertificateServicesClient-CertEnroll	64	None
Information	6/14/2013 10:13:56 AM	CertificateServicesClient-CertEnroll	65	None
Warning	6/14/2013 10:13:52 AM	SceCli	1202	None
Error	6/14/2013 9:49:04 AM	VBECS	0	None
Error	6/14/2013 9:42:37 AM	VBECS	0	None

Event 4101, Winlogon

General | Details

Windows license validated.

Log Name: Application

Source: Winlogon

Logged: 6/14/2013 11:34:51 AM

Event ID: 4101

Task Category: None

Level: Information

Keywords: Classic

User: N/A

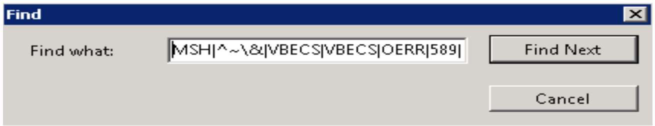
Computer: R05ISHAPPVBTS2.vha.med.va.gov

OpCode: Info

More Information: Event Log Online Help

4) Paste the **MessageID** highlighted in the email received (Figure 88) in the **Find What** text box. Click **Find Next** (Figure 90).

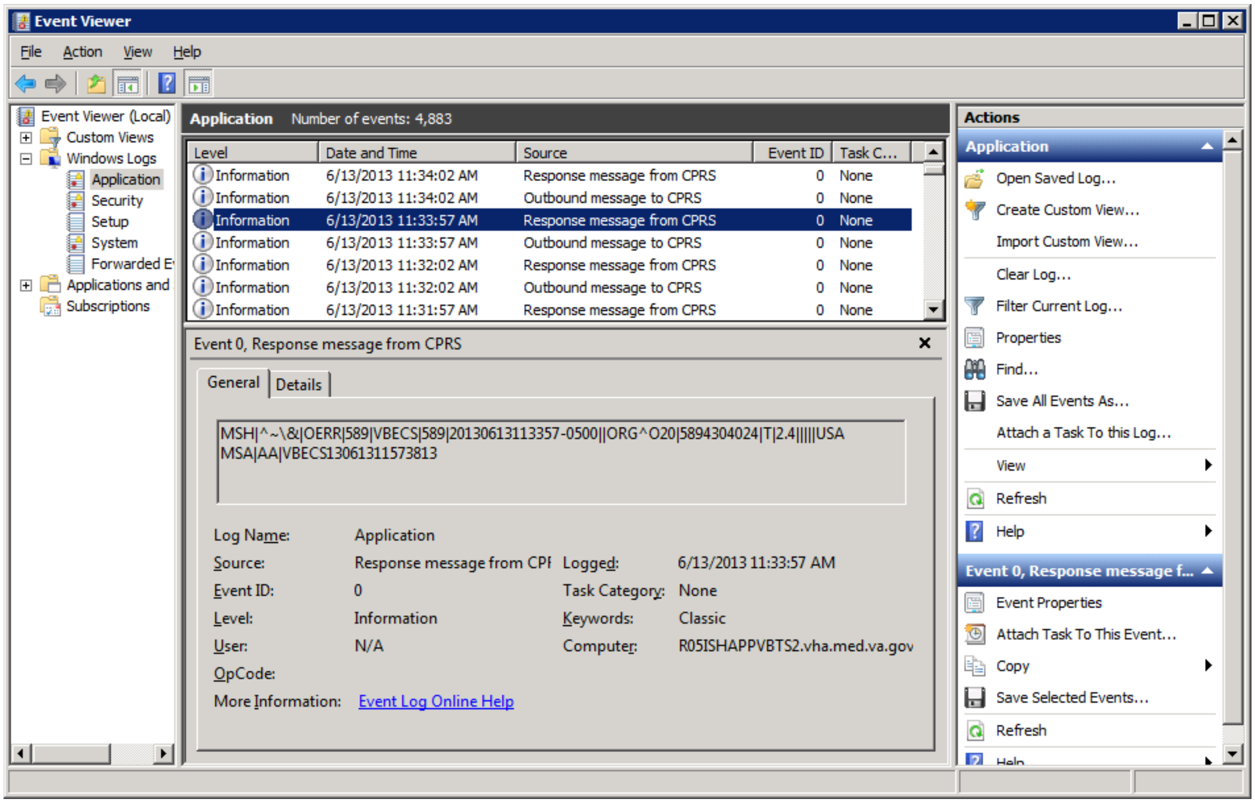
Figure 90: Example of Find in Local Application



Find what: MSH|^~\&|VBECS|VBECS|OERR|589|

5) When the event record has been found, the row will be highlighted (Figure 91).

Figure 91: Example of Message ID Located in Event Log



Application Number of events: 4,883

Level	Date and Time	Source	Event ID	Task C...
Information	6/13/2013 11:34:02 AM	Response message from CPRS	0	None
Information	6/13/2013 11:34:02 AM	Outbound message to CPRS	0	None
Information	6/13/2013 11:33:57 AM	Response message from CPRS	0	None
Information	6/13/2013 11:33:57 AM	Outbound message to CPRS	0	None
Information	6/13/2013 11:32:02 AM	Response message from CPRS	0	None
Information	6/13/2013 11:32:02 AM	Outbound message to CPRS	0	None
Information	6/13/2013 11:31:57 AM	Response message from CPRS	0	None

Event 0, Response message from CPRS

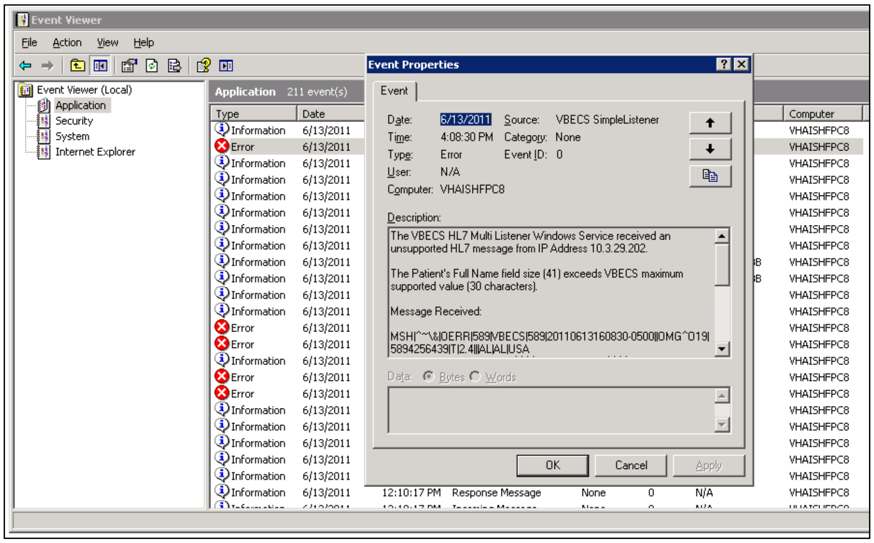
```
MSH|^~\&|OERR|589|VBECS|589|20130613113357-0500||ORG^O20|5894304024|T|2.4|||||USA
MSA|AA|VBECS13061311573813
```

Log Name:	Application		
Source:	Response message from CPI	Logged:	6/13/2013 11:33:57 AM
Event ID:	0	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	R05ISHAPPVBTS2.vha.med.va.gov
OpCode:			
More Information:	Event Log Online Help		

6) Click **Cancel** to close the Find window (Figure 90). The screen will now be display the found event.

7) Double-click on the highlighted row (Figure 92).

Figure 92: Example of Event Properties



Type	Date						Computer
Information	6/13/2011						VHAISHFPC8
Error	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Error	6/13/2011						VHAISHFPC8
Error	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Error	6/13/2011						VHAISHFPC8
Error	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011						VHAISHFPC8
Information	6/13/2011	12:10:17 PM	Response Message	None	0	N/A	VHAISHFPC8

Date: 6/13/2011 Source: VBECS SimpleListener
Time: 4:08:30 PM Category: None
Type: Error Event ID: 0
User: N/A
Computer: VHAISHFPC8

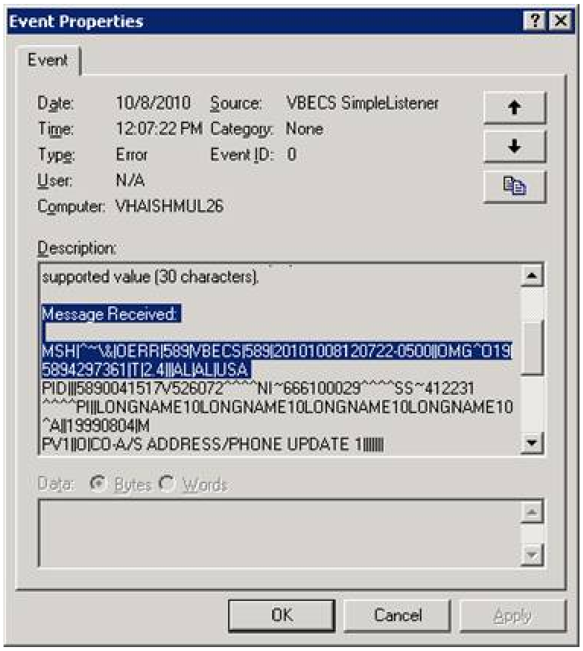
Description:

```
The VBECS HL7 Multi Listener Windows Service received an
unsupported HL7 message from IP Address 10.3.29.202.

The Patient's Full Name field size (41) exceeds VBECS maximum
supported value (30 characters).

Message Received:

MSH|^~\&|OERR|589|VBECS|589|20110613160830-0500||OMG^O19|
5894256439|T|2.4|||AL|AL|USA
```

Data: ● Bytes ○ Words

8) If the **Message ID** in the email is part of the Message Receive information in the Event Properties, analyze the detail message to identify the Patient Information causing the error (Figure 93).

Figure 93: Example of Analyzing Event Properties



Date: 10/8/2010 Source: VBECS SimpleListener
Time: 12:07:22 PM Category: None
Type: Error Event ID: 0
User: N/A
Computer: VHAISHMUL26

Description:

```
supported value (30 characters).

Message Received:

MSH|^~\&|OERR|589|VBECS|589|20101008120722-0500||OMG^O19|
5894297361|T|2.4|||AL|AL|USA
PID|||5890041517V526072^^^^^NI~666100029^^^^^SS~412231
^^^^^PI||LONGNAME10LONGNAME10LONGNAME10LONGNAME10
^A||19990804|M
PV1||O|C0-A/S ADDRESS/PHONE UPDATE 1|||||||
```

Data: ● Bytes ○ Words

9) If the Message ID in the email is not found in the Message Received, proceed to the next error by repeating Steps 3 through 7.

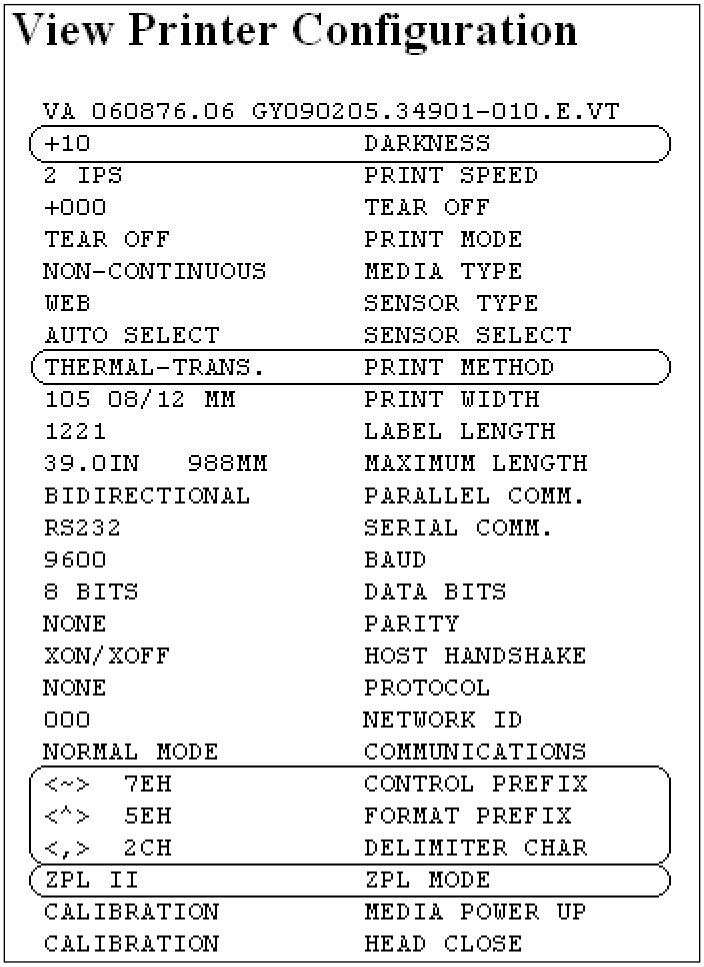
Zebra Printer Problems

Problem: The printer prints, but there is no text on the label or text is too light.

Probable Cause: The printer is out of ribbon or the DARKNESS setting is too light (Figure 94).

Solution: Increase the DARKNESS setting after verifying printer has ribbon.

Figure 94: Example Zebra Printer Settings



View Printer Configuration

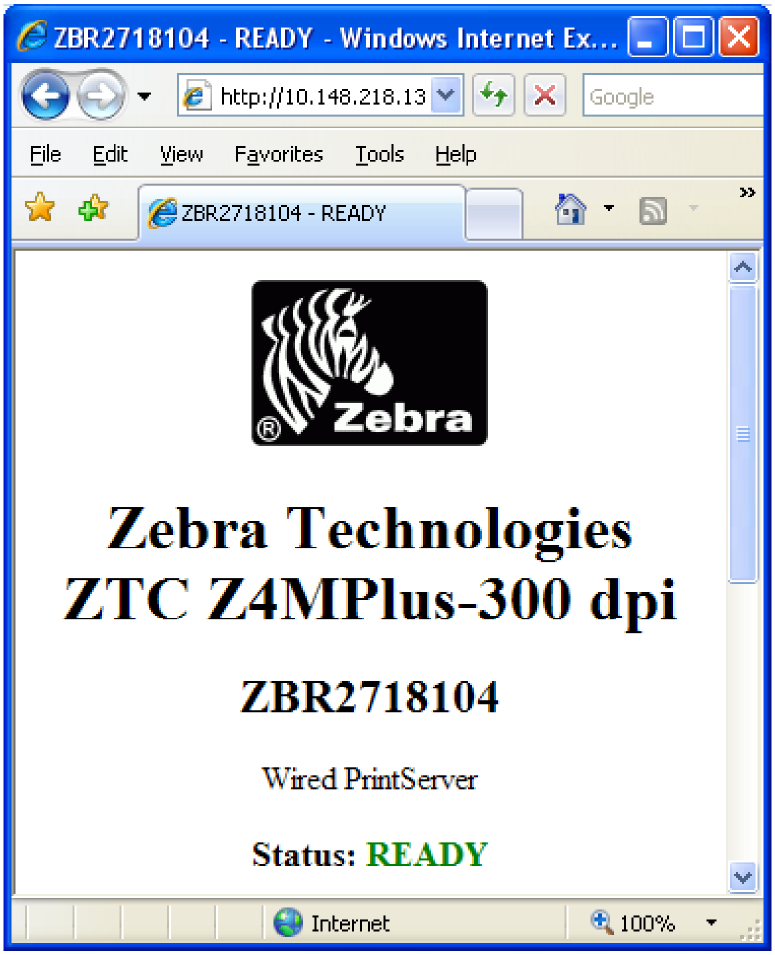
```
VA 060876.06 GY090205.34901-010.E.VT
+10                   DARKNESS
2 IPS                 PRINT SPEED
+000                  TEAR OFF
TEAR OFF              PRINT MODE
NON-CONTINUOUS        MEDIA TYPE
WEB                   SENSOR TYPE
AUTO SELECT           SENSOR SELECT
THERMAL-TRANS.        PRINT METHOD
105 08/12 MM          PRINT WIDTH
1221                  LABEL LENGTH
39.0IN   988MM        MAXIMUM LENGTH
BIDIRECTIONAL         PARALLEL COMM.
RS232                 SERIAL COMM.
9600                  BAUD
8 BITS                DATA BITS
NONE                  PARITY
XON/XOFF              HOST HANDSHAKE
NONE                  PROTOCOL
000                   NETWORK ID
NORMAL MODE           COMMUNICATIONS
<~>  7EH              CONTROL PREFIX
<^>  5EH              FORMAT PREFIX
<,>  2CH              DELIMITER CHAR
ZPL II                ZPL MODE
CALIBRATION           MEDIA POWER UP
CALIBRATION           HEAD CLOSE
```

Problem: The printer does not print. It also cannot be pinged or be seen in a web browser (Figure 95).

Probable Cause: Network settings are not correct on the printer

Solution: Correct the printer's network settings (see the section titled "Set the IP Address on the Printer").

Figure 95: Example of Zebra Printer Web Console



Zebra Technologies
ZTC Z4MPlus-300 dpi

ZBR2718104

Wired PrintServer

Status: READY

Problem: The printer does not print and network settings have been verified (see previous).

Probable Cause: One or more settings are incorrect.

Solution: Verify that the PRINT METHOD, CONTROL PREFIX, FORMAT PREFIX, DELIMITER CHAR and ZPL MODE match the settings in Figure 94.

Scanner Problems

Problem: When scanning, a **`** character appears at the start of the scan.

Probable Cause: The **Caps Lock** is on.

Solution: Turn the **Caps Lock** off.

Problem: When scanning, characters appear in the field that do not match the label being scanned. Often, the bad characters are not alphanumeric.

Probable Causes: Remote Desktop setting or network latency causes data to become corrupted.

Solution #1: First, try adjusting the keyboard settings in Remote Desktop Connection. Change the **Keyboard** setting to **On the local computer** (Figure 8). If this does not work, try solution #2.

Solution #2: The lab supervisor will program an inter-character delay into the scanner to fix the issue. This puts a small time-delay between each character as it is sent over the network, which results in slightly slower scan speeds.

Figure 96 through Figure 103 are configuration barcodes arranged from a 10-millisecond inter-character delay all the way up to an 80-millisecond delay respectively. We suggest that you start with the 10-millisecond delay. If that does not resolve the problem, proceed with larger delays until the problem is corrected.

Note that these barcodes include all of the configuration information for the scanners. There is no need to scan any additional barcodes to configure the scanner.

Figure 96: 10 milliseconds

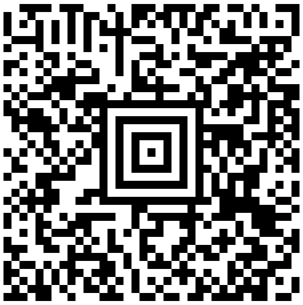


Figure 97: 20 milliseconds

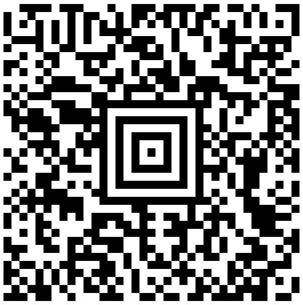


Figure 98: 30 milliseconds

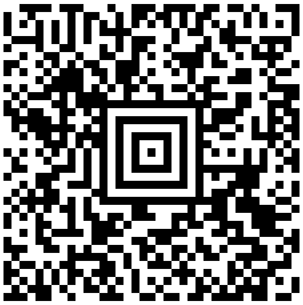


Figure 99: 40 milliseconds

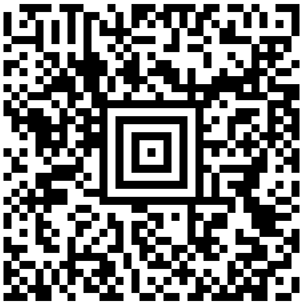


Figure 100: 50 milliseconds

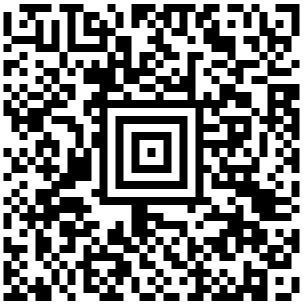


Figure 101: 60 milliseconds

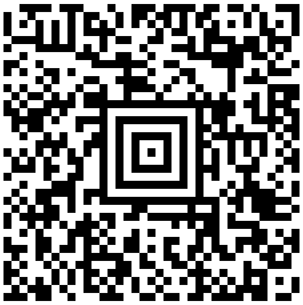


Figure 102: 70 milliseconds

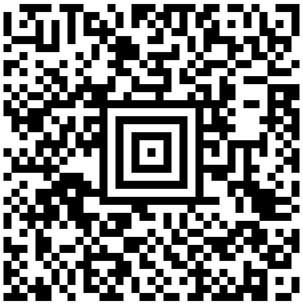
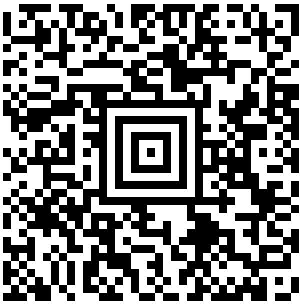


Figure 103: 80 milliseconds



VBECS FTP Download Issues

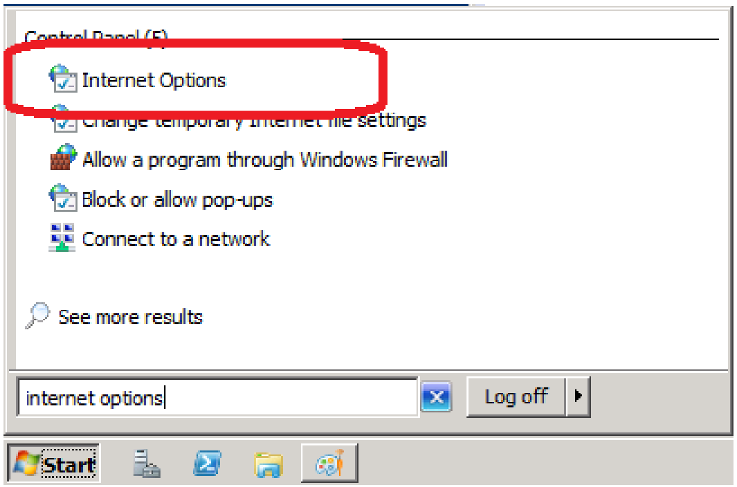
Problem: VBECS FTP Download Security Alert with message 'Your current settings do not allow you do download files from this location'

Probable Cause: FTP site is not part of Trusted Sites in Internet Explorer.

Solution: Add the VBECS FTP site to the Trusted Sites in Internet Explorer by doing the following steps:

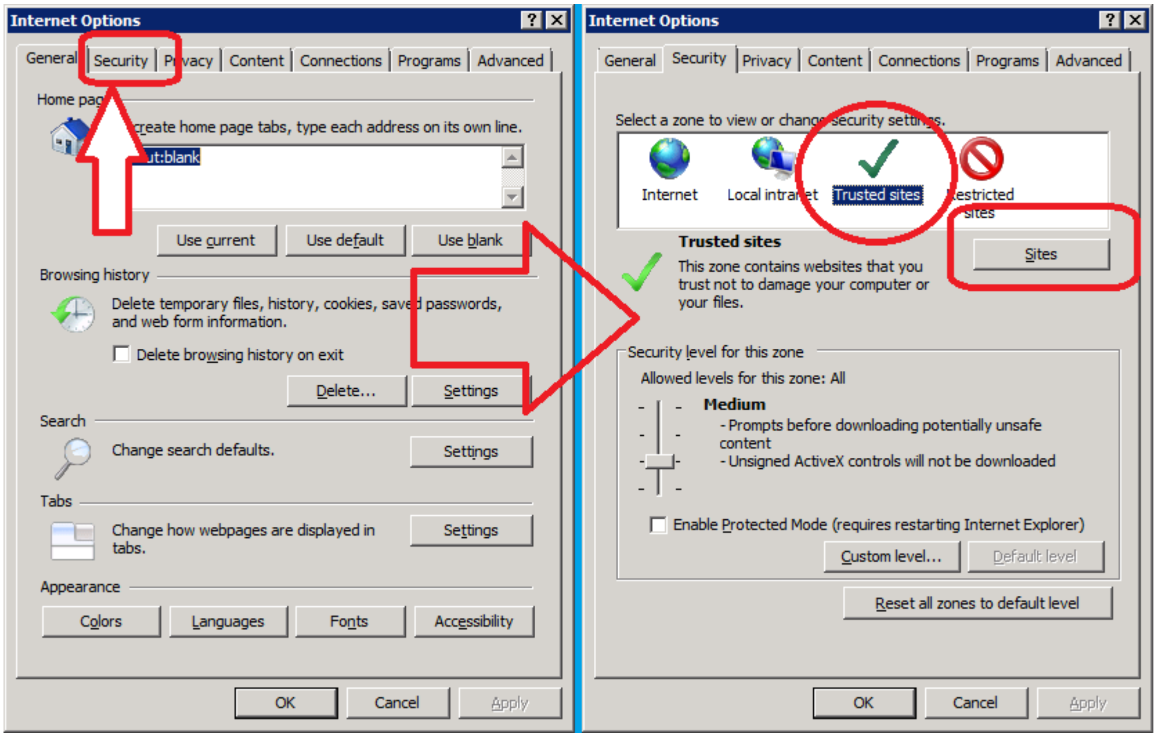
1) Click **Start**: type internet options and select the top menu item that displays (Figure 104).

Figure 104: Example of Internet Explorer Window



2) Select the **Security** tab: select **Trusted sites** and click **Sites** (Figure 105).

Figure 105: Example of Internet Explorer Internet Options Security tab



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Home pag

reate home page tabs, type each address on its own line.

ut:blank

Use current | Use default | Use blank

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Delete... | Settings

Search

Change search defaults. | Settings

Tabs

Change how webpages are displayed in tabs. | Settings

Appearance

Colors | Languages | Fonts | Accessibility

OK | Cancel | Apply

Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

Sites

Security level for this zone

Allowed levels for this zone: All

Medium

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

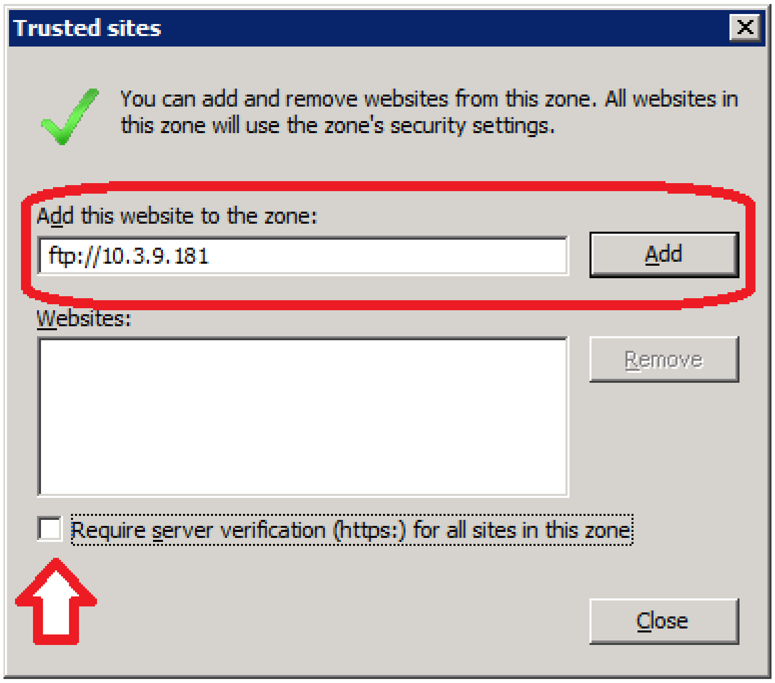
Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply

3) Make sure **Require server verification…** is unchecked. Enter **ftp://10.3.9.181** and click the **Add** button (Figure 106).

Figure 106: Adding VBECS FTP to the Trusted Sites



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

ftp://10.3.9.181

□ Require server verification (https:) for all sites in this zone

4) Close the Internet Options windows.

This page intentionally left blank.

Archiving and Recovery (Enterprise Operations Only)

The VBECS database will be backed up once daily and the backup to tape can be taken any time after 1:00 AM (CST).

Assumptions

The SQL Server job that backs up the database is running correctly.
Replacement hardware will have a tape drive that is compatible with the one lost in the disaster.

Outcome

VBECS data is successfully recovered.

Limitations and Restrictions

None

Additional Information

None

Restore the Databases

If you find the need to perform a database restore and require assistance, file a support ticket (Service Desk Primary Contact) for the VBECS Maintenance Team.

Service Desk Primary Contact

For Information Technology (IT) support, call the Service Desk (VASD), 888-596-HELP (4357) toll free, 24 hours per day, 7 days per week.

National Service Desk Alternate Contacts

- Web site: http://vaww.itsupportservices.va.gov/vasd_home.asp (National Service Desk Tuscaloosa).
- Email : vhacionhd@va.gov

This page intentionally left blank.

Failover

VBECS does not have a seamless failover mechanism. If an application server fails, the user will receive a message that the remote connection was lost. VBECS will lose information entered since the last save. The user must reopen a Remote Desktop Connection session. The user will have to reenter all information that was lost since the last save.

The connection between VBECS and VistA can be lost for a number of reasons:

An application server can fail or the VistA server can fail. When this connection is lost, no messages can be exchanged. When the connection between VBECS and VistA is lost due to a failure of VBECS, the messages are queued on the VistA side. Orders placed during this downtime will remain in the queue. Once the VBECS system recovers and a connection is reestablished with VistA, the messages come across. The order alerts icon located in the VBECS status bar will display the orders that were in the queue at the time of failure.

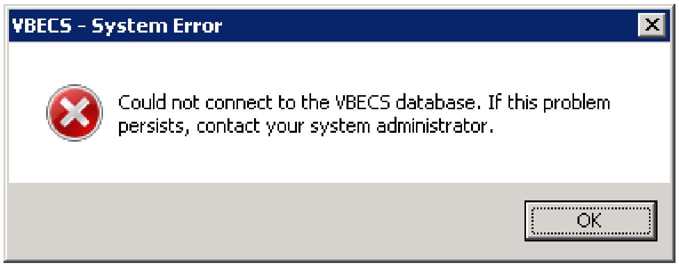
An application server can fail because of a vSphere failure. If the underlying physical host that VBECS resides on fails, the VBECS servers will fail too. vSphere clustering will restore the server on another host.

If a user's client workstation fails in the middle of a VBECS session, the session remains active on the server for a period set by the server administrator. The standard session time-out is 15 minutes. If the user resolves the issues with the client workstation and reconnects to the VBECS server through Remote Desktop Connection before the session times out, the session will remain as it was when the client failed.

VBECS uses a feature within Microsoft SQL Server 2012 called AlwaysOn. SQL Server AlwaysOn provides both High Availability (HA) and Disaster Recovery for VBECS databases. HA is implemented within one datacenter through synchronous replication. If a primary SQL server should fail, the VBECS application is automatically directed to use the databases on the HA SQL server. This is a seamless failover and occurs automatically with no intervention needed. The previously defined HA server becomes the new primary server and when the original primary server recovers, it becomes the new HA server. This will occur during normal maintenance of the servers during Windows update deployment on a monthly basis as those servers are rebooted. Using the same AlwaysOn technology, disaster recovery is implemented through asynchronous replication between the primary data center and a disaster recovery data center. Unlike the HA configuration, activating a disaster recovery server requires manual intervention.

If the VBECS user is in the process of performing a query at the exact second a synchronous failover takes place, they are presented with the message shown in Figure 107:

Figure 107: Synchronous Failover Message



VBECS - System Error

Could not connect to the VBECS database. If this problem persists, contact your system administrator.

Once the VBECS user clicks OK, any open child dialogs automatically close to preserve data integrity. They may proceed to use VBECS and will not see this message again. This message could present itself in the event of a disaster recovery failover as well. In that case, the system will not recover automatically and the VBECS user continues to see this message every time they try to query the database. Manual failover recovery to the disaster recovery server takes place through written instructions defined in the Disaster Recovery Plan and requires the intervention and expertise of the datacenter and VBECS maintenance teams.

Performance

VBECS may delay a critical function such as patient transfusion if the network suffers latency issues. File a support ticket (Service Desk Primary Contact) per local procedures when latency issues arise.

VBECS was re-factored after performance testing results showed latency issues for VistA queries. As a result, many queries are cached in the VBECS database. Due to the criticality of having correct and current patient data, patient lookups cannot be cached.

Locking

VBECS is designed with pessimistic locking controlled within the application code: if one user selects a record for edit, the record is locked by that user. If another user tries to edit that record, a message will tell him that the record is locked and who has the record. The second user is not granted access to the record. Locks have a timeout period defined in the configure division portion of the VBECS Administrator application. When a lock times out or is released by a user completing his edit, another user can edit that record.

If the application code fails due to a logic bug, optimistic locking is in place to prevent data corruption. When a record is retrieved, a row version is also retrieved. When a record is saved, the row in the database gets an updated row version; before the save takes place, the save routine checks that the row version supplied matches the row version in the table. If it does not match, the routine notifies the caller that another user changed the data. The save does not complete; the user must retrieve the updated record and start his edits again.

If VBECS had an application error resulting in the application terminating, locks may have to be manually deleted. File a ticket (Service Desk Primary Contact).

This page intentionally left blank.

Security

VBECS contains sensitive data and performs a critical function, so it is critical to secure the system. It is important to secure the server from both users and malicious attacks from an individual who is trying to gain access to the system. This information section describes the measures taken to secure VBECS.

Active Directory

Access to the VBECS servers is controlled through AD. Each VBECS site will have two groups set up in AD, one for normal VBECS users and one for VBECS Administrators (this is not a server administrator). Unless the user is a server administrator, he must be a member of one of these two groups to gain access to the server. Users will use their normal Windows user names to log in.

These groups also play a role in application level security. Even if a user were able to access the server, he would not be able to access VBECS.

Group Policy

Group policy controls the user experience (what the user sees and has access to on the VBECS server). To configure this correctly, the recommendations in “*Windows Server 2008 R2 Security Guide*” (Microsoft Web site) were followed to establish a baseline for group policy.

Group policy can be applied to user accounts or to the servers directly. In the case of VBECS, group policy is applied to the servers (it is easier to manage). It is also undesirable to have group policy associated with the user, which may inhibit his use of other systems. Enabling loopback processing applies the policy to any user that logs into the server.

In some cases, group policy also enables VBECS to perform actions on the Windows operating system. For example, there is a group policy setting that allows the VBECS services to be restarted after a configuration change in VBECS Administrator.

System Center Operations Manager

SCOM is a proactive monitoring tool. SCOM will constantly monitor each server for system abnormalities. If SCOM detects a problem, an email will be sent to the system administrator defined during the SCOM installation process. SCOM will monitor these high-level categories:

Windows Server 2008 R2 Operating System
CPU health and usage
Network interface cards
SQL Server (SQL Clustering and SQL AlwaysOn)
Memory usage
Hard-disk health and usage
VBECS files and services
Windows Services

Application-Wide Exceptions

Table 14 explains system exceptions to aid VA Health Product Support in determining the cause and resolving system issues.

Table 14: Application-Wide Exceptions

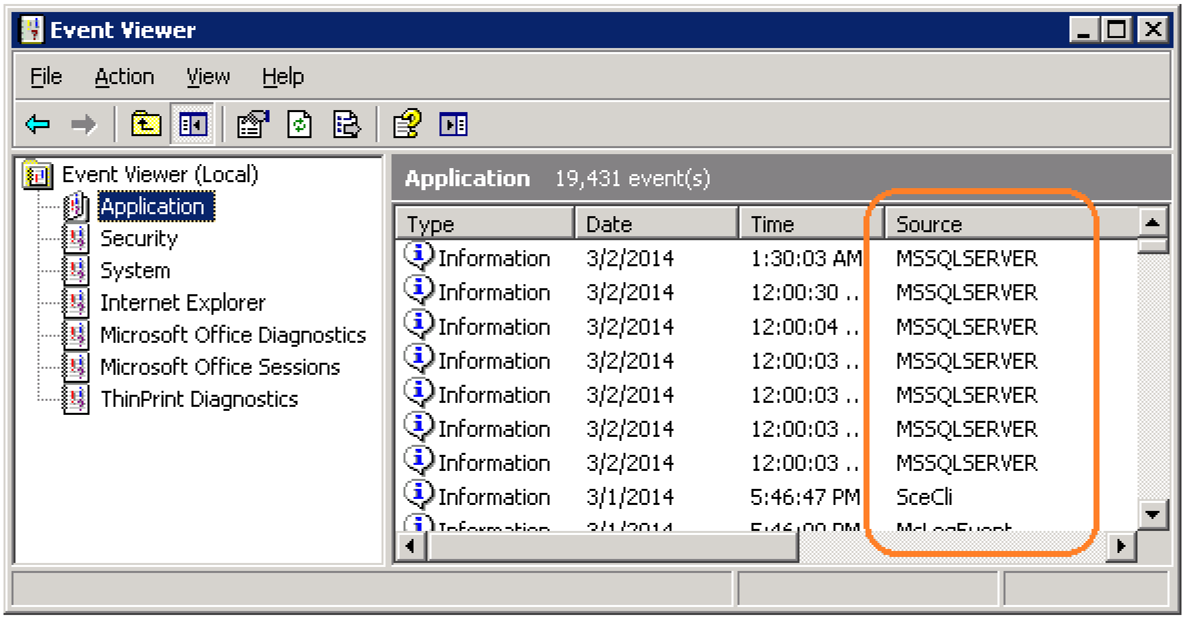
System Exceptions	Description
ArgumentException	Base class for all argument exceptions
ArgumentNullException	Thrown by methods that do not allow an argument to be null
ArgumentOutOfRangeException	Thrown by methods that verify that arguments are in a given range
ComException	Exception encapsulating COM HRESULT information
Exception	Base class for all exceptions
ExternalException	Base class for exceptions that occur or are targeted at environments outside the runtime
IndexOutOfRangeException	Thrown by the runtime only when an array is indexed improperly
InvalidOperationException	Thrown by methods when in an invalid state
NullReferenceException	Thrown by the runtime only when a null object is referenced.
SEHException	Exception encapsulating Win32 structured exception handling information
System.ArithmeticException	A base class for exceptions that occur during arithmetic operations, such as System.DivideByZeroException and System.OverflowException
System.ArrayTypeMismatchException	Thrown when a store into an array fails because the actual type of the stored element is incompatible with the actual type of the array
System.DivideByZeroException	Thrown when an attempt to divide an integral value by zero occurs
System.IndexOutOfRangeException	Thrown when an attempt to index an array via an index that is less than zero or outside the bounds of the array
System.InvalidCastException	Thrown when an explicit conversion from a base type or interface to a derived type fails at run time
System.NullReferenceException	Thrown when a null reference is used in a way that causes the referenced object to be required
System.OutOfMemoryException	Thrown when an attempt to allocate memory (via new) fails
System.OverflowException	Thrown when an arithmetic operation in a checked context overflows
System.StackOverflowException	Thrown when the execution stack is exhausted by having too many pending method calls; typically indicative of very deep or unbounded recursion
System.TypeInitializationException	Thrown when a static constructor throws an exception, and no catch clauses exist to catch it
SystemException	Base class for all runtime-generated errors

Table 15 explains the event sources that VBECS uses to write to the Application log in Event Viewer (**Finding Application Log Entries from Email Alerts (Enterprise Operations Only)**).

Table 15: Event Sources

Event Source	Description
VBECS Exception	A VBECS system crash
VBECS Prod	VBECS Production
VBECS Test	VBECS Test
VBECS Admin Prod	VBECS Administrator Production
VBECS Admin Test	VBECS Administrator Test
HL7Dispatcher Prod	VBECS Services
HL7Dispatcher Test	
HL7Service Prod	
HL7Service Test	
ReportScheduler Prod	
ReportScheduler Test	
VistaLinkService Prod	
VistaLinkService Test	

Figure 108: Event Sources



Application 19,431 event(s)

Type	Date	Time	Source
Information	3/2/2014	1:30:03 AM	MSSQLSERVER
Information	3/2/2014	12:00:30 ..	MSSQLSERVER
Information	3/2/2014	12:00:04 ..	MSSQLSERVER
Information	3/2/2014	12:00:03 ..	MSSQLSERVER
Information	3/2/2014	12:00:03 ..	MSSQLSERVER
Information	3/2/2014	12:00:03 ..	MSSQLSERVER
Information	3/2/2014	12:00:03 ..	MSSQLSERVER
Information	3/1/2014	5:46:47 PM	SceCli
Information	3/1/2014	5:46:00 PM	McLogEvent

Health Product Support Access

Health Product Support has access to the App Server. While members of the support team do not have full administrative privileges, they have access to the following:

- Printer status and settings
- View status of VBECS services
- View the Application and System event logs
- View Task Manager

This page intentionally left blank.

Configuring the App Server and Lab Workstations for VBECS 2.0.0

After the App Server is deployed, additional configuration will need to be performed on it and on the lab workstations. On the server, install the printer, configure permissions and create the Report share. On the workstation, create a shortcut to the report share.

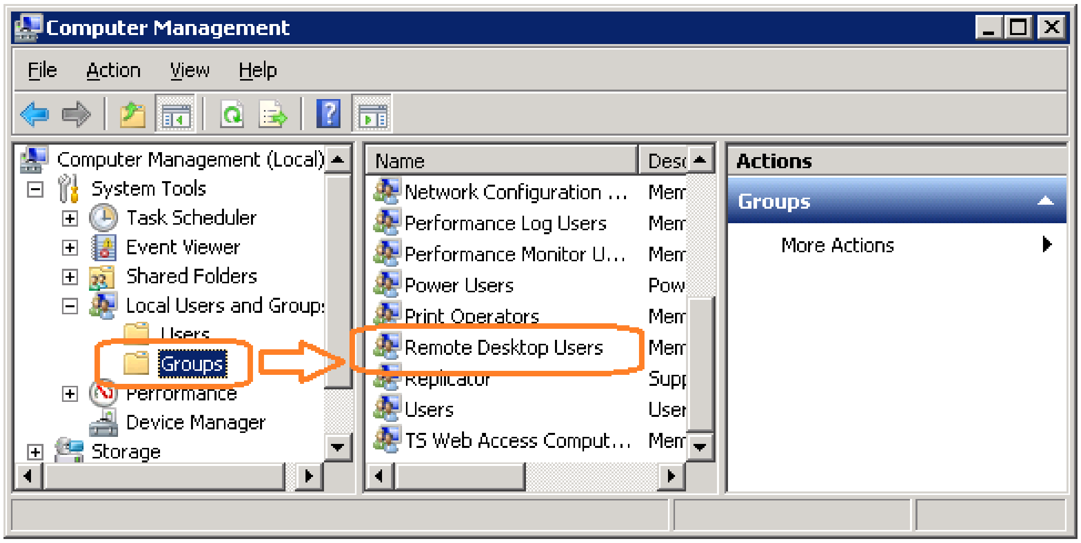
Server Tasks (Enterprise Operations Only)

Perform the following tasks on the App Server only.

Grant User Permissions

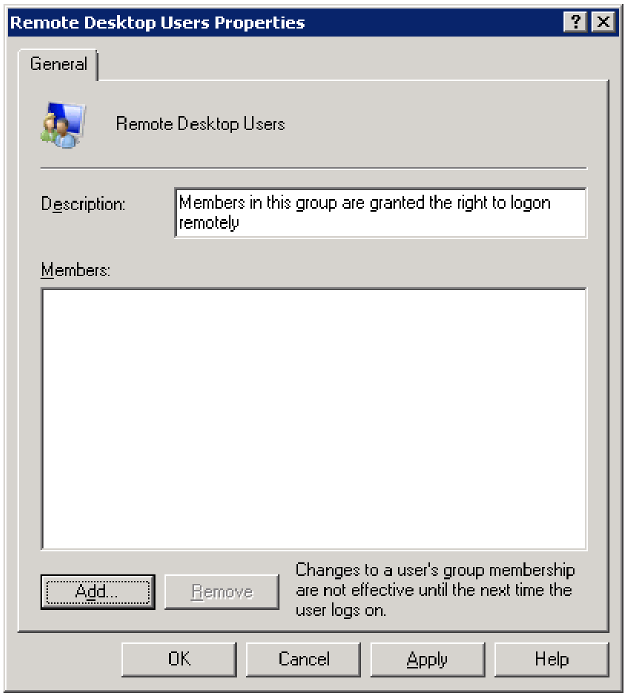
1) Open a remote desktop connection to the VBECS App Server and login with server administrator privileges.
2) Click **Start**, **Administrative Tools**, **Computer Management**. Expand **Local Users and Groups**. Select **Groups** and double-click **Remote Desktop Users** (Figure 109).

Figure 109: Computer Management



3) Click **Add** (Figure 110).

Figure 110: Remote Desktop Users Properties



Description: Members in this group are granted the right to logon remotely

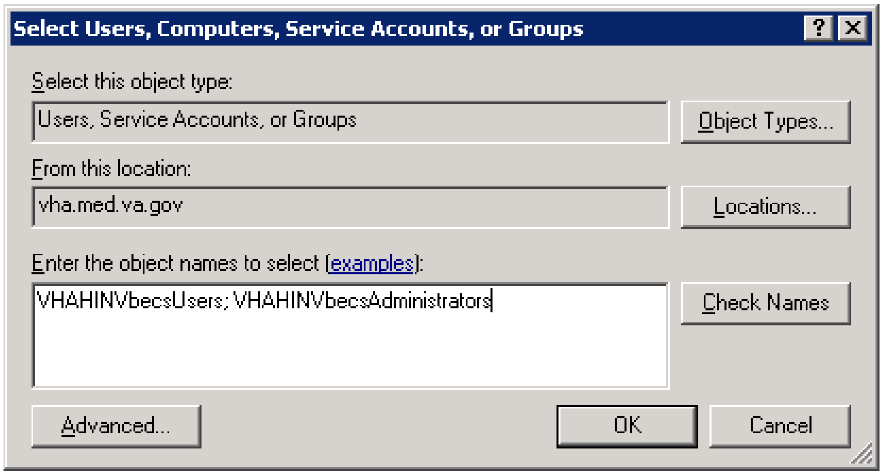
Members:

Changes to a user's group membership are not effective until the next time the user logs on.

4) Specify the VBECS Users and VBECS Administrators group (Figure 111). Note that groups typically follow this naming convention (substitute the 3-letter site code for sss):
   - VBECS Users: *VHAsssVbecsUsers*
   - VBECS Administrators: *VHAsssVbecsAdministrators*

   Click **OK** to close the window. Click **OK** again to close the **Properties** window.

Figure 111: Example of Select Users, Computers...



Select this object type: Users, Service Accounts, or Groups

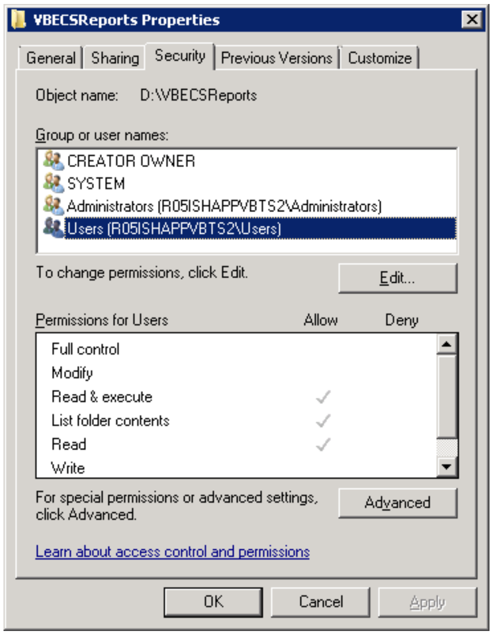
From this location: vha.med.va.gov

Enter the object names to select (examples): VHAHINVbecsUsers; VHAHINVbecsAdministrators

Configure the Report Share

1) Open a remote desktop connection to the VBECS App Server and login with server administrator privileges.
2) Open Windows Explorer and navigate to the **D** drive.
3) Right-click on **VBECSReports** and click **Properties**. Select the **Security** tab and click **Edit** (Figure 112).

Figure 112: Example of VBECSReports Properties



Object name: D:\VBECSReports

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (R05ISHAPPVBTS2\Administrators)
- Users (R05ISHAPPVBTS2\Users)

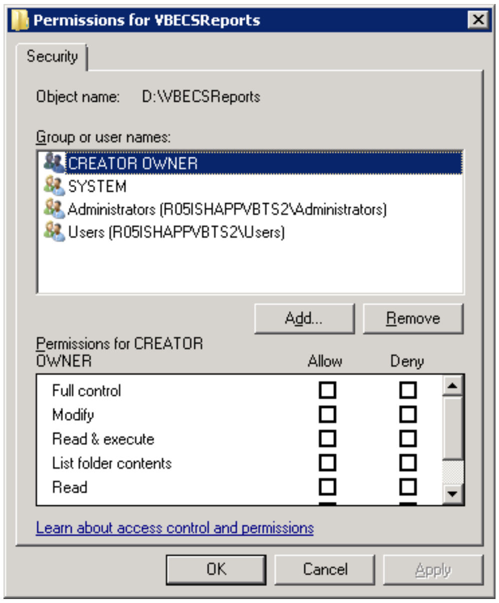
To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

4) Click **Add** (Figure 113).

Figure 113: Example of Permissions



Permissions for VBECSReports

Security

Object name: D:\VBECSReports

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (R05ISHAPPVBTS2\Administrators)
- Users (R05ISHAPPVBTS2\Users)

Permissions for CREATOR OWNER

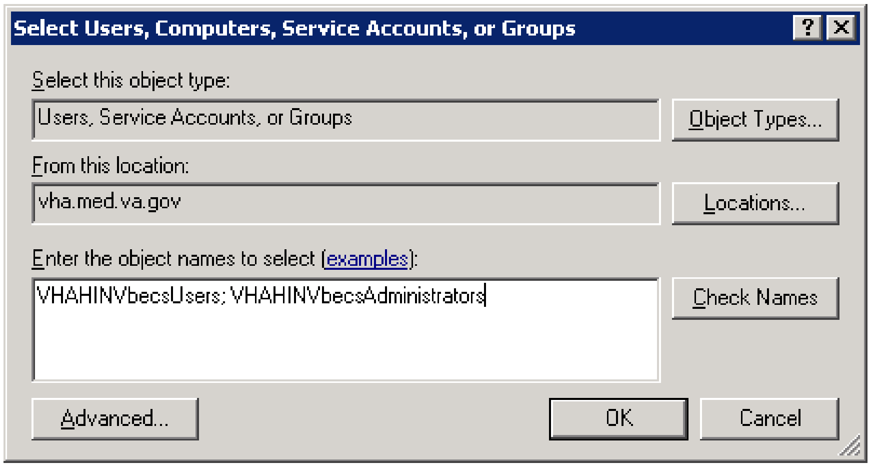
	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

5) Specify the VBECS Users and VBECS Administrators group (Figure 114). Note that groups typically follow this naming convention (substitute the 3-letter site code for sss):

- VBECS Users: *VHAsssVbecsUsers*
- VBECS Administrators: *VHAsssVbecsAdministrators*

Click **OK** to close the window.

Figure 114: Example of Select Users, Computers...



Select Users, Computers, Service Accounts, or Groups

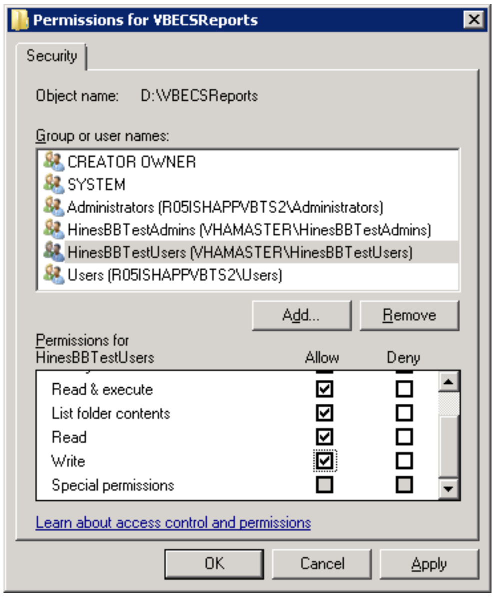
Select this object type: Users, Service Accounts, or Groups

From this location: vha.med.va.gov

Enter the object names to select (examples): VHAHINVbecsUsers; VHAHINVbecsAdministrators

6) In the **Permissions** window, assign **Write** access to both groups in addition to the rights granted by default. Click **OK**.

Figure 115: Example of Permissions


Permissions for VBECSReports
Security
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

Object name: D:\VBECSReports

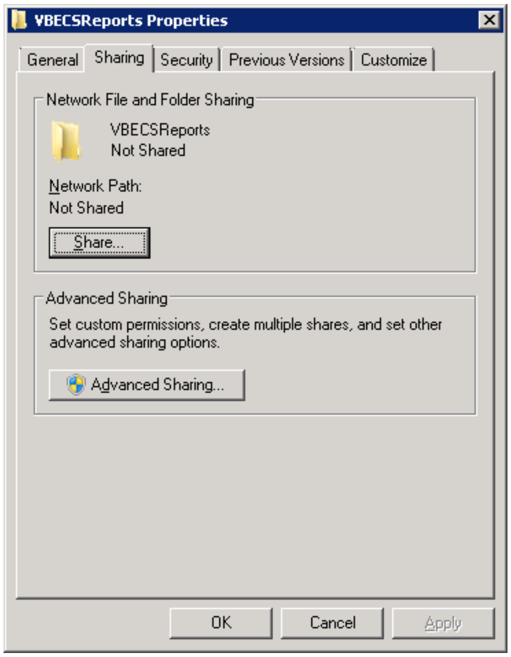
Group or user names:

CREATOR OWNER
SYSTEM
Administrators (R05ISHAPPVBTS2\Administrators)
HinesBBTestAdmins (VHAMASTER\HinesBBTestAdmins)
HinesBBTestUsers (VHAMASTER\HinesBBTestUsers)
Users (R05ISHAPPVBTS2\Users)

Permissions for HinesBBTestUsers	Allow	Deny
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	☑	□
Special permissions	□	□

7) Select the **Sharing** tab and click **Advanced Sharing** (Figure 116).

Figure 116: VBECSReports Properties



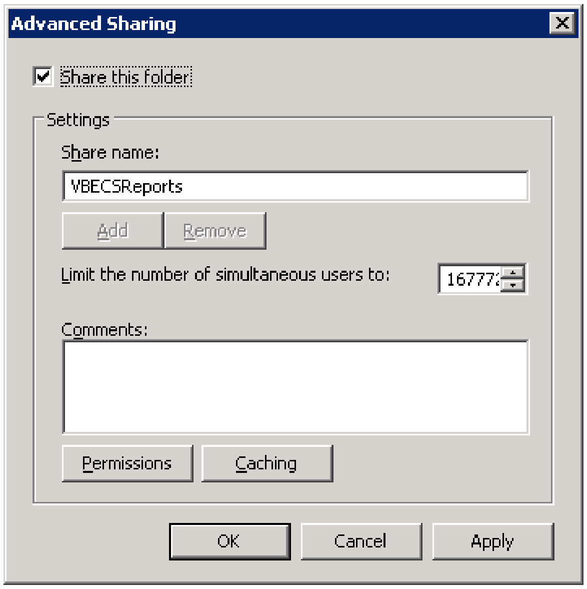
VBECSReports
Not Shared

Network Path:
Not Shared

Set custom permissions, create multiple shares, and set other advanced sharing options.

8) Click **Share this folder** and then **Permissions** (Figure 117).

Figure 117: Advanced Sharing



Advanced Sharing

☑ Share this folder

Settings

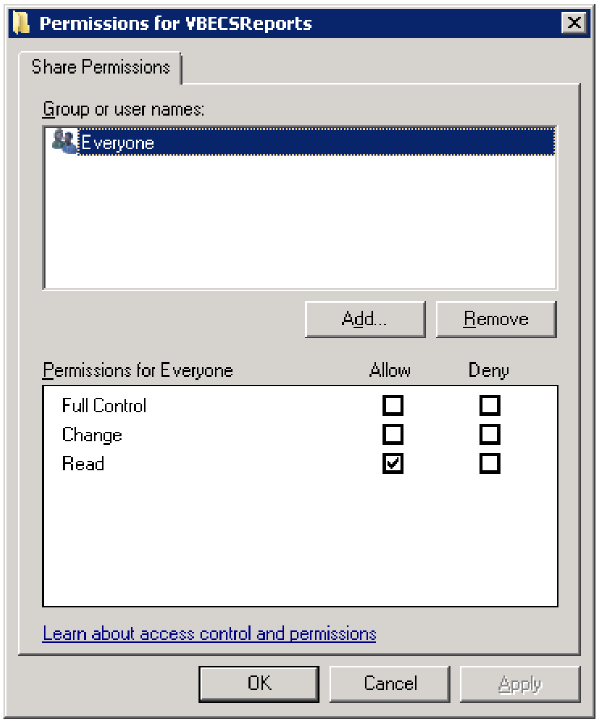
Share name: VBECSReports

Limit the number of simultaneous users to: 16777

Comments:

9) Click **Add** (Figure 118).

Figure 118: Permissions



Permissions for VBECSReports
Share Permissions
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

Group or user names:
Everyone

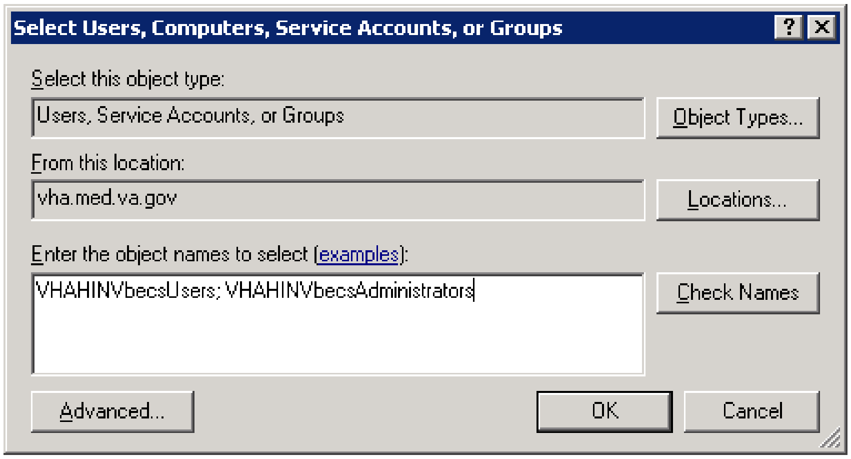
Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

10) Specify the VBECS Users and VBECS Administrators group (Figure 119). Note that groups typically follow this naming convention (substitute the 3-letter site code for sss):

- VBECS Users: *VHAsssVbecsUsers*
- VBECS Administrators: *VHAsssVbecsAdministrators*

Click **OK** and **OK** again to close all windows.

Figure 119: Select Users...



Select this object type:
Users, Service Accounts, or Groups

From this location:
vha.med.va.gov

Enter the object names to select (examples):
VHAHINVbecsUsers; VHAHINVbecsAdministrators

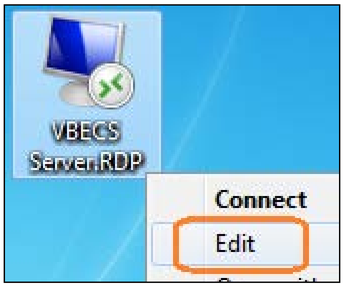
Workstation Tasks

Update the RDP shortcut and create the report share on each lab workstation.

Update the RDP Shortcut

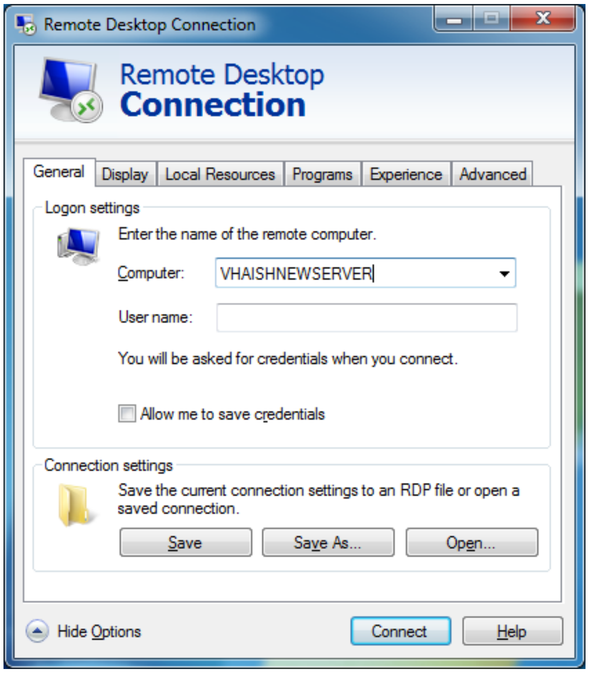
1) Find the IP address of your new App Server in the VBECS Server Planning Sheet on the VBECS 2.0.0 SharePoint.
2) Log into the lab workstation with administrator privileges.
3) Right-click on the VBECs remote desktop shortcut and click **Edit** (Figure 120).

Figure 120: Edit shortcut



4) In the **Computer** field, enter the IP address of the new app server (Figure 121). Click **Save**.

Figure 121: Remote Desktop Connection



Logon settings

Enter the name of the remote computer.

Computer: VHAISHNEWSERVER

User name:

You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

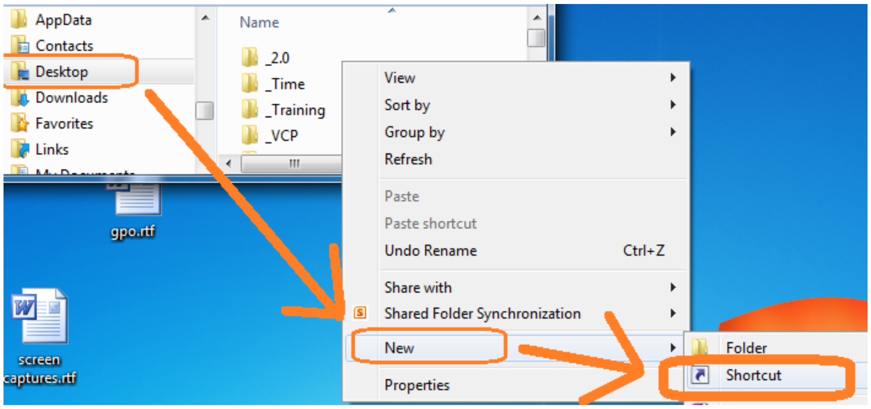
Save the current connection settings to an RDP file or open a saved connection.

Configure a Shortcut to the Report Share

The report share section (Configure the Report Share) must have been executed before proceeding with this section. The report share contains patient identifiable information, so the shortcut must only be accessible by authorized laboratory personnel. If the workstation will only be used by laboratory personnel, the shortcut may be placed in the **Public Desktop** folder. Otherwise, create it separately in each user's folder.

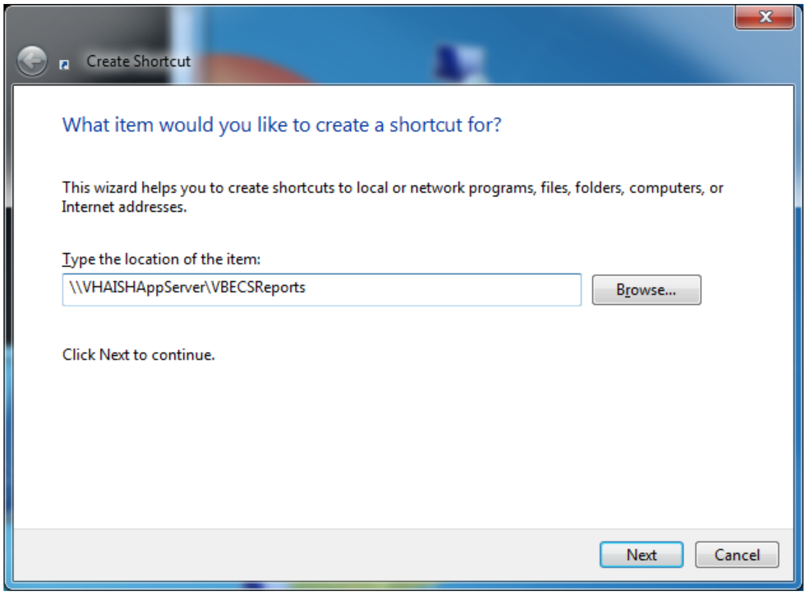
1) Log into the lab workstation with administrator privileges. Navigate to the user's desktop folder (C:\Users\Public\Public Desktop), right-click on the **Desktop** folder and select **New**, **Shortcut** (Figure 122). Note: If you cannot see the Public Desktop folder in the tree view type (C:\Users\Public\Public Desktop) in the address bar and hit enter.

Figure 122: Example of New Shortcut



2) Enter the share name (\\<VBECS application server name>\VBECSReports) and click **Next** (Figure 123).

Figure 123: Example of Report Share



Create Shortcut

What item would you like to create a shortcut for?

This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

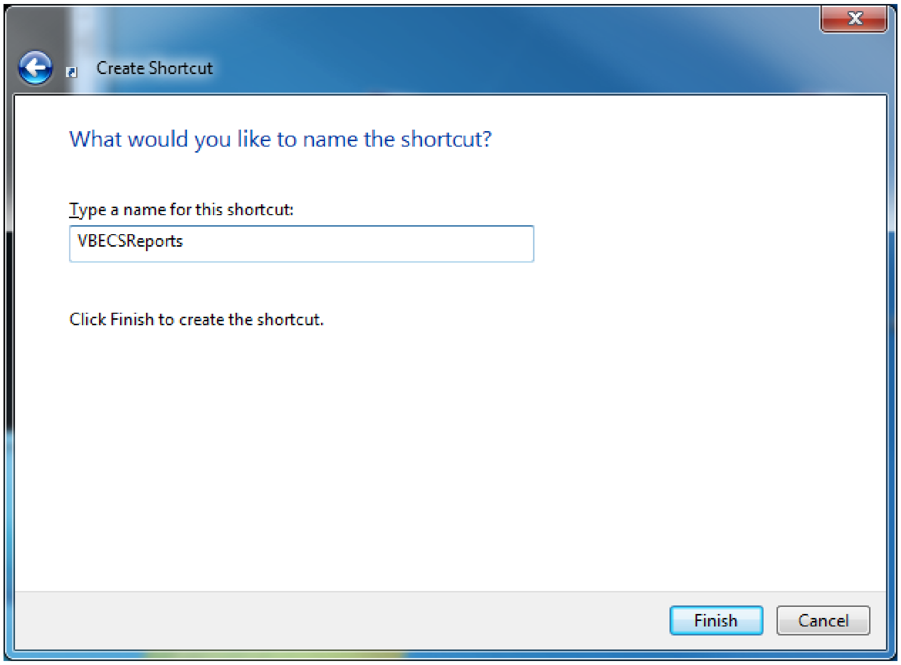
Type the location of the item:

\\VHAISHAppServer\VBECSReports

Click Next to continue.

3) Name the shortcut **VBECSReports**. Click **Finish** (Figure 124).

Figure 124: Create Shortcut



Create Shortcut

What would you like to name the shortcut?

Type a name for this shortcut:

VBECSReports

Click Finish to create the shortcut.

Glossary

Acronym, Term	Definition
ABO	A group for classifying human blood, based on the presence or absence of specific antigens in the blood, which contains four blood types: A, B, AB, and O. The ABO group is the most critical of the human blood systems. It is used to determine general compatibility of donor units to a recipient.
Access Code	A field in the VistA New Person file used to uniquely identify a user on the VistA system.
Active Directory (AD)	A hierarchical directory service built on the Internet's Domain Naming System (DNS).
ADPAC	Automated Data Processing Application Coordinator.
AG	Availability Group.
ANR	Automated Notification Report.
API	Application Programmer Interface.
AITC	Austin Information Technology Center.
BCE	Bar Code Expansion.
CPRS	Computerized Patient Record System.
DBIA	Database Integration Agreement.
DR	Disaster Recovery.
DSS	Decision Support System.
DUZ	Designated User.
EO	Enterprise Operations.
HA	High Availability.
HCPCS	Healthcare Common Procedure Coding System.
HL7	Health Level Seven.
LAN	Local Area Network.
LLP	Lower Layer Protocol.
LMIP	Laboratory Management Index Program.
PCE	Patient Care Encounter.
PIV	Personal Identification Verification.
RDP	Remote Desktop Protocol.
RPC	Remote Procedure Call.
SQL	Structured Query Language.
SSMS	SQL Server Management Studio.
SCOM	System Center Operations Manager.
TCP/IP	Transmission Control Protocol/Internet Protocol.
VAISS	VBECS Application Interfacing Support Software.
VBECS	VistA Blood Establishment Computer Software.
VDL	VA Software Document Library.

Acronym, Term	Definition
Verify Code	A field in the VistA New Person file used to verify the identity of a user associated with an Access Code.
VISN	Veterans Integrated Service Network.
XML	Extensible Markup Language.

Appendices

Appendix A: Instructions for Capturing Screen Shots

Throughout the technical manual-security guide, the Administrator is asked to capture screen shots to document configuration options. To capture a screen shot:

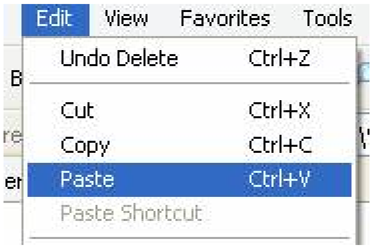
- Open a blank document (for example, in Microsoft Word) and save it as (click **File**, **Save As**) “mmyydd Technical-Security Validation Record,” or another easily identified file name.

> *If you wish to place a document on the server for ease of copying and pasting, assign file names similar to “mmyydd Technical-Security Validation Record Server1” and “mmyydd Technical-Security Validation Record Server2.”*

When the screen you wish to capture is displayed, press the **Print Screen** key.
In the Technical-Security Validation Record document, place the cursor where you want to insert the picture.

Click (the paste icon) or select **Edit**, **Paste (**Figure 125**)**.

Figure 125: Paste



Label the screen shot within the document with the technical manual-security guide step, page number, and server on which the picture was taken.

This page intentionally left blank.

Appendix B: Known Defects and Anomalies

Copies of *Known Defects and Anomalies* may be obtained from the VA Software Document Library (VDL) Web site (http://www.va.gov/vdl/application.asp?appid=182.).

This page intentionally left blank.

Appendix C: Active Directory Change Request

Follow your local site procedures for requesting and documenting changes in Active Directory for user additions or deletions from VBECS Active Directory groups. Contact the Implementation Team to verify your data center contact, if necessary.

This page intentionally left blank.

Appendix D: Data Center Instructions (Enterprise Operations only)

Purpose

This appendix describes the server configuration as well as the tasks that must be completed by the data center for a successful VBECS installation:

- Initial Setup Tasks: These tasks must be completed prior to installation of any VBECS systems.
- Ongoing Tasks: These are continual maintenance tasks.

Server Configuration

The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations.

VBECS is a medical device; all updates and changes to it must be tested and documented. This will be centrally managed. The VBECS servers must be added to site exclusion lists so they are not part of local update mechanisms. Ensure that login scripts do not run on VBECS servers as they may attempt to install unauthorized software. Do not install the ePolicy agent *on the VBECS systems: exclude them from* Systems Management Server *(SMS) updates. Install Windows updates* only *after approval is granted.*

App and Database Server Virtual Machine Configurations

Table 16 and Table 17 describe the configurations of the App and Database Server virtual machines respectively.

These configurations are designed to promote 24/7 availability and use of the application. At an App Server level, replication provides high availability. At the Database Server level, AlwaysOn cluster configuration provides near immediate failover in case the primary server fails.

Table 16: App Server Virtual Machine Configuration

App Server Specifications	
Processor	2 virtual CPUs (vCPUs) with a speed of 2.67GHz
Memory	6 gigabyte (GB) main storage (RAM)
Storage	80GB system drive (C) with a 10GB (D) drive to host configuration and reports
Operating System	Microsoft Windows Server 2008 Server Enterprise Edition R2 (x64)
Network Controller	Two 10/100 network cards; one for network configuration and another for backups.
Backup	Servers are replicated at the disaster recovery site.

Table 17: Database Server Virtual Machine Configuration

Database Server Specifications	
Processor	4 vCPUs: Xeon(R) X5650 @ 2.67GHz

Memory	32GB main storage (RAM)
Storage	**Server**: 80GB system drive (C) with a 10GB drive to host configuration and reports **Shared storage**: 4 x 980GB drives* ((E Data) with a 20 GB drive, (F Logs) with a 20GB drive, (G TempDB) with a 20GB drive, (H Backup) with a 20 GB drive)
Operating System	Microsoft Windows Server 2008 Server Enterprise Edition R2 (x64)
Network Controller	Two 10/100 network cards; one for network configuration and another for backups.
Backup	Data is replicated to the disaster recovery site via SQL AlwaysOn.

*The drives used in the test servers will be scaled down.

Physical Host Configurations

Table 18 describes the requirements of the hosting hardware. Input/Output Operations per Second (IOPS) is a storage benchmark. The Storage Totals row describes the total amount of storage that each region must provide.

Table 18: App Server Virtual Machine Configuration

Specification		R01	R02	R03	R04
IOPS	Read (Avg/ Max)	654/ 5,265	658/ 5,326	985/ 7,959	646/ 5,143
	Write (Avg/ Max)	2,435/ 10,435	2,445/ 10,543	3,663/ 15,761	2,418/ 10,220
Storage Totals		31.16 TB	31.32 TB	46.9 TB	30.84 TB

Initial Setup Tasks

Execute the tasks in this section prior to installation.

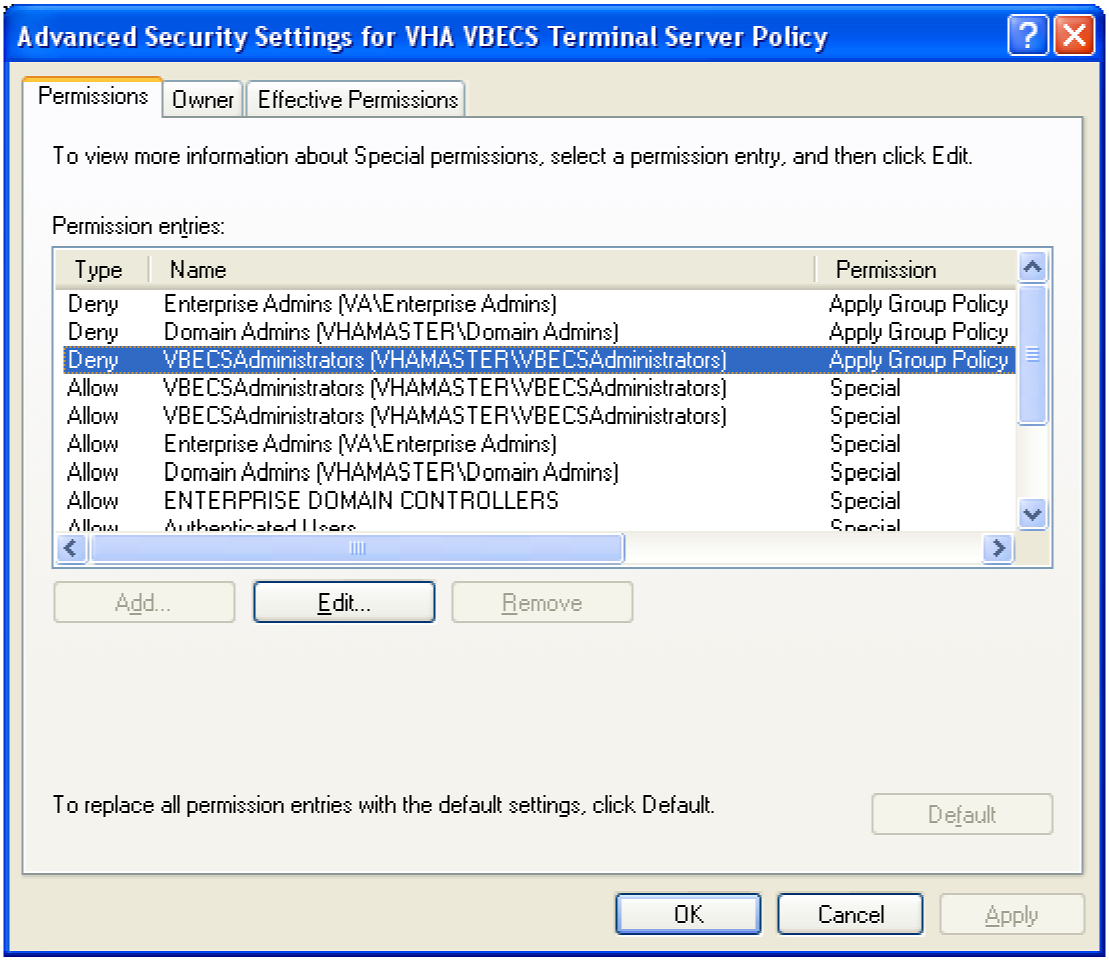
Group Policy

For Group Policy purposes, VBECS servers will reside in their own OU, which will contain only VBECS servers. You may also create OUs under the main OU for organizational purposes. For more information, see the Group Policy section.

Import the *VHA VBECS Terminal Server Policy* from the VHAMASTER domain. Place the group policy in the top-level server OU. For more information about OUs and server organization, see the Active Directory section.

Configure the policy so that it is not applied to the R*xx*VbecsServerAdmins Active Directory group. See the example in Figure 126.

Figure 126: Example of a Group Policy Not Applied to VBECSAdministrators Group



Advanced Security Settings for VHA VBECS Terminal Server Policy
Permissions
Owner
Effective Permissions

To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission
Deny	Enterprise Admins (VA\Enterprise Admins)	Apply Group Policy
Deny	Domain Admins (VHAMASTER\Domain Admins)	Apply Group Policy
Deny	VBECSAdministrators (VHAMASTER\VBECSAdministrators)	Apply Group Policy
Allow	VBECSAdministrators (VHAMASTER\VBECSAdministrators)	Special
Allow	VBECSAdministrators (VHAMASTER\VBECSAdministrators)	Special
Allow	Enterprise Admins (VA\Enterprise Admins)	Special
Allow	Domain Admins (VHAMASTER\Domain Admins)	Special
Allow	ENTERPRISE DOMAIN CONTROLLERS	Special
Allow	Authenticated Users	Special

To replace all permission entries with the default settings, click Default.

RDP Server

VBECS is a RDP Server application and requires a license. Specify the license server in the group policy at the following location:

- Computer Configuration, Policies, Administrative Templates, Windows Components, Remote Desktop Services, Remote Desktop Session Host, Licensing, Use the specified Remote Desktop license servers (**Enabled**), License servers to use: **tslicense.va.gov**

Remote desktop is critical to VBECS. Failure to connect to a license server will result in widespread outages. If you see errors related to Terminal Server licensing, contact the Enterprise Engineering group immediately: ***VA IT Engineering CIS IDM***.

Ongoing Tasks

Execute the tasks in this section continually.

1) Back Up the VBECS Database

Back up the VBECS databases nightly (1am CST):

- Back up all folders and files in the <Primary Server> H:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup and <Secondary (HA) Server> H:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup directories.
- Database backups are maintained for at least seven days on the Primary and Secondary (HA) servers.

2) VBECS Updates

When the VBECS maintenance team releases a VBECS patch, install the patch in accordance with instructions supplied by the VBECS maintenance team.

3) Windows Updates

The VBECS maintenance team tests every Microsoft Windows update. Once the VBECS maintenance team certifies the Microsoft Windows update, EO staff at the AITC install the updates during the monthly maintenance periods defined for the test and production servers. Refer to *Applying Windows Updates* section for details.

Appendix E: Services Allowed to Run on VBECS Servers

If you are using an alternate backup solution such as CommVault, the list of services may be different.

The following services are permitted to run on VBECS application servers:

- ActivIndentity Shared Store Service
- Application Host Helper Service
- Background Intelligent Transfer Service
- Base Filtering Engine
- Certificate Propagation
- CNG Key Isolation
- COM+ Event System
- COM+ System Application
- Cryptographic Services
- DCOM Server Process Launcher
- Desktop Window Manager Session Manager
- DHCP Client
- Diagnostic Policy Service
- Distributed Link Tracking Client
- Distributed Transaction Coordinator
- DNS Client
- Function Discovery Provider Host
- Group Policy Client
- IKE and AuthIP IPsec Keying Modules
- IP Helper
- IPSEC Policy Agent
- McAfee Engine Service
- McAfee Framework Service
- McAfee Host Intrusion Prevention Ipc Service
- McAfee Host Intrusion Prevention Service
- McAfee McShield
- McAfee Task Manager
- McAfee Validation Trust Protection Service
- Net.Pipe Listener Adapter
- Net.Tcp Listener Adapter
- Net.Tcp Port Sharing Service
- Netlogon
- Network Connections
- Network List Service
- Network Location Awareness (NLA)
- Network Store Interface Service
- Plug and Play
- Power

- Print Spooler
- Remote Desktop Configuration
- Remote Desktop Services
- Remote Desktop Services UserMode Port Redirector
- Remote Procedure Call (RPC)
- Remote Registry
- RPC Endpoint Manager
- SCOM
- Security Accounts Manager
- Server
- Shell Hardware Detection
- SMS Agent Host
- Software Protection
- SPP Notification Service
- System Event Notification Service
- Task Scheduler
- TCP/IP NetBIOS Helper
- User Profile Service
- VMware Tools
- VBECS Prod HL7 Dispatcher
- VBECS Prod HL7 Listener
- VBECS Prod Report Scheduler
- VBECS Prod VistALink Listener
- VBECS Test HL7 Dispatcher
- VBECS Test HL7 Listener
- VBECS Test Report Scheduler
- VBECS Test VistALink Listener
- Windows Event Log
- Windows Font Cache Service
- Windows Management Instrumentation
- Windows Process Activation Service
- Windows Remote Management (WS-Management)
- Windows Time
- Windows Update
- Workstation
- World Wide Web Publishing Service

The following services are permitted to run on VBECS SQL servers:

- ActivIndentity Shared Store Service
- Application Host Helper Service
- Background Intelligent Transfer Service
- Base Filtering Engine
- Certificate Propagation
- Cluster Service
- CNG Key Isolation
- COM+ Event System
- COM+ System Application
- Cryptographic Services
- DCOM Server Process Launcher
- Desktop Window Manager Session Manager
- DHCP Client
- Diagnostic Policy Service
- Distributed Link Tracking Client
- Distributed Transaction Coordinator
- DNS Client
- Encrypting File System (EFS)
- Function Discovery Provider Host
- Group Policy Client
- IKE and AuthIP IPsec Keying Modules
- IP Helper
- IPSEC Policy Agent
- McAfee Engine Service
- McAfee Framework Service
- McAfee Host Intrusion Prevention Ipc Service
- McAfee Host Intrusion Prevention Service
- McAfee McShield
- McAfee Task Manager
- McAfee Validation Trust Protection Service
- Net.Pipe Listener Adapter
- Net.Tcp Listener Adapter
- Net.Tcp Port Sharing Service
- Netlogon
- Network Connections
- Network List Service
- Network Location Awareness
- Network Store Interface Service
- Plug and Play
- Power
- Print Spooler
- Remote Desktop Configuration
- Remote Desktop Services
- Remote Desktop Services UserMode Port Redirector

- Remote Procedure Call (RPC)
- Remote Registry
- RPC Endpoint Manager
- SCOM
- Security Accounts Manager
- Server
- Shell Hardware Detection
- SMS Agent Host
- SQL Server (MSSQLSERVER)
- SQL Server Agent (MSSQLSERVER)
- SQL Server VSS Writer
- System Event Notification Service
- Task Scheduler
- TCP/IP NetBIOS Helper
- User Profile Service
- VMware Tools
- Windows Event Log
- Window Font Cache Service
- Windows Management Instrumentation
- Windows Modules Installer
- Windows Process Activation Service
- Windows Remote Management (WS-Management)
- Windows Time
- Windows Update
- Workstation
- World Wide Web Publishing Service

Appendix F: Auditing on VBECS Servers

The following events are audited on VBECS servers. These events may be viewed in Event Viewer logs (under Administrative Tools):

- Account logon events (Success, Failure)
- Account management (Success, Failure)
- Directory service access (Success, Failure)
- Logon events (Success, Failure)
- Object access (Success, Failure)
- Policy Change (Success, Failure)
- System events (Success, Failure)

This page intentionally left blank.

Appendix G: VBECS Production Site Codes

Region	Installation	Site Code	VISN
1	Albuquerque, NM	ABQ	18
1	Amarillo, TX	AMA	18
1	Big Spring, TX	BIG	18
1	Cheyenne, WY	CHY	18
1	Phoenix, AZ	PHO	18
1	Prescott, AZ	PRE	18
1	Tucson, AZ	TUC	18
1	Denver, CO	DEN	19
1	Fort Harrison, MT	FHM	19
1	Grand Junction, CO	GRJ	19
1	Salt Lake City, UT	SLC	19
1	Boise, ID	BOI	20
1	Portland, OR	POR	20
1	Puget Sound, WA	PUG	20
1	Roseburg, OR	ROS	20
1	Spokane, WA	SPO	20
1	Fresno, CA	FRE	21
1	Martinez, CA	MAC	21
1	Palo Alto, CA	PAL	21
1	Reno, NV	REN	21
1	San Francisco, CA	SFC	21
1	Greater LA, CA	GLA	22
1	Las Vegas, NV	LAS	22
1	Loma Linda, CA	LOM	22
1	Long Beach, CA	LON	22
1	San Diego, CA	SDC	22
2	Chicago (West), IL	CHS	12
2	Hines, IL	HIN	12
2	Iron Mountain, MI	IRO	12
2	Madison, WI	MAD	12
2	Milwaukee, WI	MIW	12
2	North Chicago, IL	NCH	12
2	Tomah, WI	TOM	12
2	Kansas City, KS	KAN	15
2	St. Louis, MO	STL	15
2	Alexandria, VA	ALX	16
2	Biloxi, MS	BIL	16
2	Fayetteville, AR	FAV	16
2	Houston, TX	HOU	16
2	Jackson, MS	JAC	16

Region	Installation	Site Code	VISN
2	Little Rock, AR	LIT	16
2	Muskogee, OK	MUS	16
2	Oklahoma, OK	OKL	16
2	Shreveport, LA	SHR	16
2	Central Texas, TX	CTX	17
2	Dallas, TX	DAL	17
2	South Texas, TX	STX	17
2	Black Hills, MN	BHH	23
2	Fargo, ND	FAR	23
2	Minneapolis, MN	MIN	23
2	Omaha, NE	OMA	23
2	St. Cloud, MN	STC	23
2	Sioux Falls, SD	SUX	23
3	Asheville, NC	ASH	6
3	Beckley, WV	BEC	6
3	Durham, NC	DUR	6
3	Fayetteville, NC	FNC	6
3	Hampton, VA	HAM	6
3	Richmond, VA	RIC	6
3	Salem, VA	SAM	6
3	Salisbury, NC	SBY	6
3	Augusta, GA	AUG	7
3	Birmingham, AL	BIR	7
3	Central Alabama, AL	CAV	7
3	Charleston, SC	CHA	7
3	Columbia, SC	CMS	7
3	Dublin, GA	DUB	7
3	Atlanta, GA	ATG	8
3	Bay Pines, FL	BAY	8
3	Miami, FL	MIA	8
3	North Florida, FL	NFL	8
3	Orlando, FL	ORL	8
3	San Juan, PR	SAJ	8
3	Tampa, FL	TAM	8
3	West Palm Beach, FL	WPB	8
3	Huntington, WV	HUN	9
3	Lexington, KY	LEX	9
3	Louisville, KY	LOU	9
3	Memphis, TN	MEM	9
3	Mountain Home, TN	MOU	9
3	Nashville, TN	TVH	9
3	Cincinnati, OH	CIN	10

Region	Installation	Site Code	VISN
3	Cleveland, OH	CLE	10
3	Chillicothe, OH	CLL	10
3	Columbus, OH	COS	10
3	Dayton, OH	DAY	10
3	Ann Arbor, MI	ANN	11
3	Battle Creek, MI	BAC	11
3	Danville, IN	DAN	11
3	Detroit, MI	DET	11
3	Indianapolis, IN	IND	11
3	Northern Indiana, IN	NIN	11
3	Saginaw, MI	SAG	11
4	Boston, MA	BHS	1
4	Connecticut HCS, CT	CON	1
4	Manchester, NH	MAN	1
4	Providence, RI	PRO	1
4	Togus, ME	TOG	1
4	White River Junction, VT	WRJ	1
4	Albany, Bath, Buffalo, NY	UNY	2
4	Bronx, NY	BRX	3
4	Hudson Valley HCS, NY	HVH	3
4	New Jersey HCS, NJ	NJH	3
4	Northport, NY	NOP	3
4	New York Harbor, NY	NYH	3
4	Altoona, PA	ALT	4
4	Clarksburg, WV	CLA	4
4	Coatesville, PA	COA	4
4	Erie, PA	ERI	4
4	Lebanon, PA	LEB	4
4	Philadelphia, PA	PHI	4
4	Pittsburgh, PA	PTH	4
4	Westboro, PA	WBP	4
4	Wilmington, DE	WIM	4
4	Maryland HCS, MD	BAL	5
4	Martinsburg, WV	MWV	5
4	Washington, DC	WAS	5

This page intentionally left blank.

Index

This is the last page of the *VistA Blood Establishment Computer Software (VBECS) 2.0.0 Technical Manual-Security Guide*.