VistA Blood Establishment Computer Software (VBECS) Version 2.3.1

Technical Manual-Security Guide

March 2019

Department of Veterans Affairs
Enterprise Project Management Office

This page intentionally left blank.

Table of Contents

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.

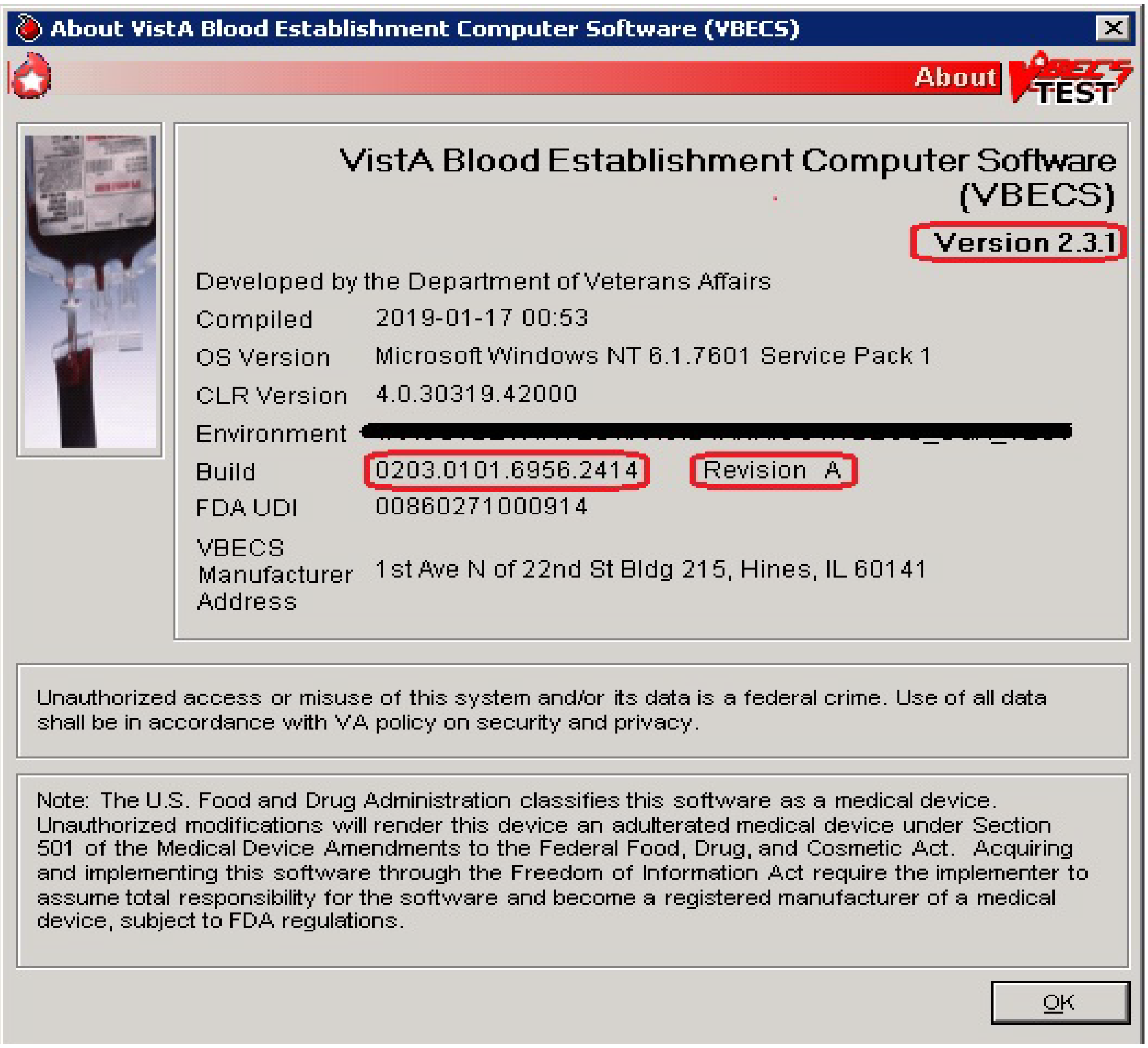
VBECS Version Numbers

In previous VBECS patch releases, the user documentation referred to the VBECS version in a 4-digit format (e.g., 2.1.0.2 – where 2.1.0 represents the patch version and the last digit (2) is the patch build number).

The VBECS version (Figure 1) is now represented with only the first three digits (e.g., 2.1.0) and appears that way in all user documentation to simplify readability

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 is revision A, but the version customers receive can be revision A, B or a higher revision letter.

Figure 1: Example of Help, About VBECS



VistA Blood Establishment Computer Software (VBECS)

Version 2.3.1

Developed by the Department of Veterans Affairs

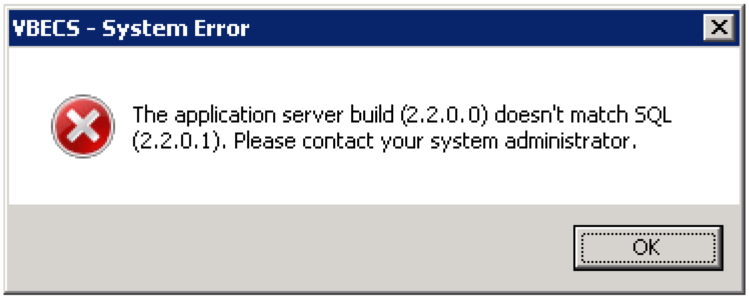
Compiled	2019-01-17 00:53
OS Version	Microsoft Windows NT 6.1.7601 Service Pack 1
CLR Version	4.0.30319.42000
Environment	[redacted]
Build	0203.0101.6956.2414 Revision A
FDA UDI	00860271000914
VBECS Manufacturer Address	1st Ave N of 22nd St Bldg 215, Hines, IL 60141

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



The application server build (2.2.0.0) doesn't match SQL (2.2.0.1). Please contact your system administrator.

Related Manuals and Reference Materials

HL7 V2.3.1 Implementation Guide
*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
Health Product Support Release of Products and Patches Guide V2.3 Updated: February 2014
VistA Blood Establishment Computer Software (VBECS) 2.3.1 User Guide
VistA Blood Establishment Computer Software (VBECS) 2.3.1 Administrator User Guide
VistA Blood Establishment Computer Software (VBECS) – <instrument> Configuration and Setup Guide
VistALink Version 1.5 Developer-System Manager Manual, Chapter 6: Security Management, pp. 34–35
Windows Server 2008R2 Security Guide, Microsoft Corporation

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.

Data Center Tasks

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

Appendices

The appendices contain reference materials.

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.

.

This page intentionally left blank.

Remote Desktop Configuration (Windows)

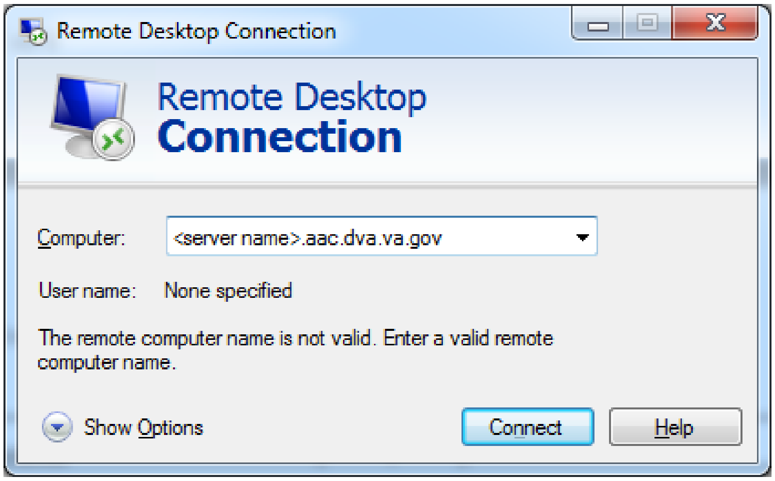
Configure the screen resolution, sound, and connection speed, and create a Remote Desktop Connection shortcut on each VBECS workstation.

Server Name and Screen Resolution

To set the screen resolution:

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

Figure 3: Example of Remote Desktop Connection Options



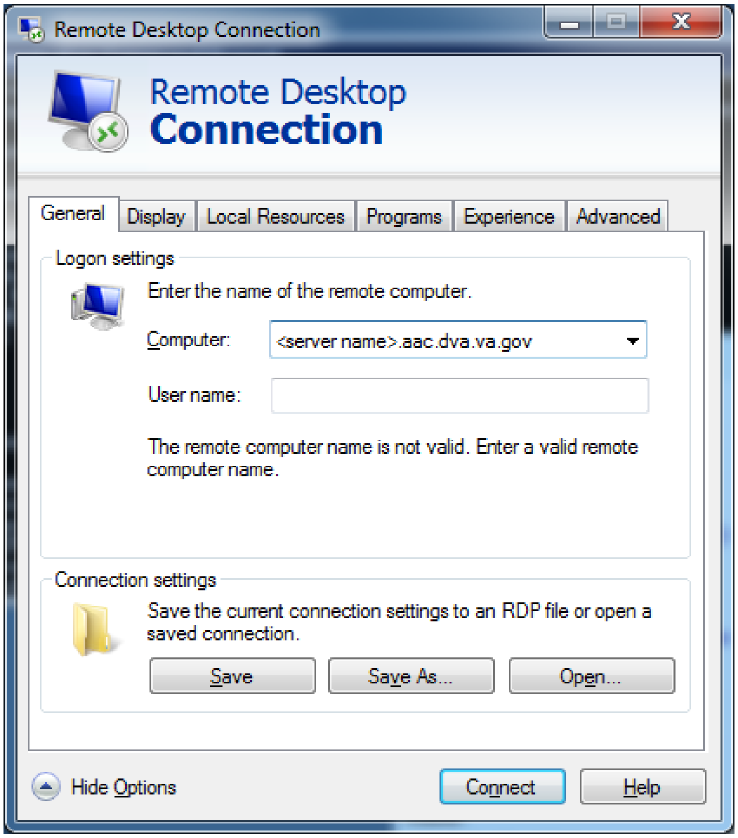
Computer: <server name>.aac.dva.va.gov

User name: None specified

The remote computer name is not valid. Enter a valid remote computer name.

3) Click the **General** tab (Figure 4).
4) Enter the VBECS application server's fully qualified domain name (FQDN) in the **Computer** field. The name will always be your server name followed by **.aac.dva.va.gov**

Figure 4: Example of General Tab Computer and Domain



Enter the name of the remote computer.

Computer: <server name>.aac.dva.va.gov

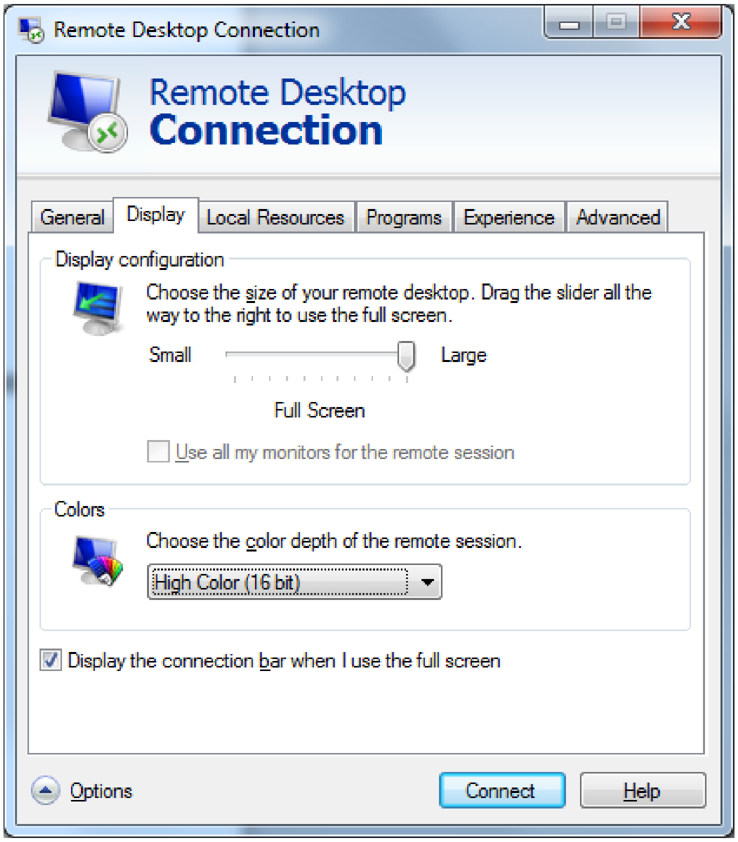
User name:

The remote computer name is not valid. Enter a valid remote computer name.

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

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

Figure 5: Example of Display Tab



Display configuration

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

Colors

Choose the color depth of the remote session.

High Color (16 bit)

☑ Display the connection bar when I use the full screen

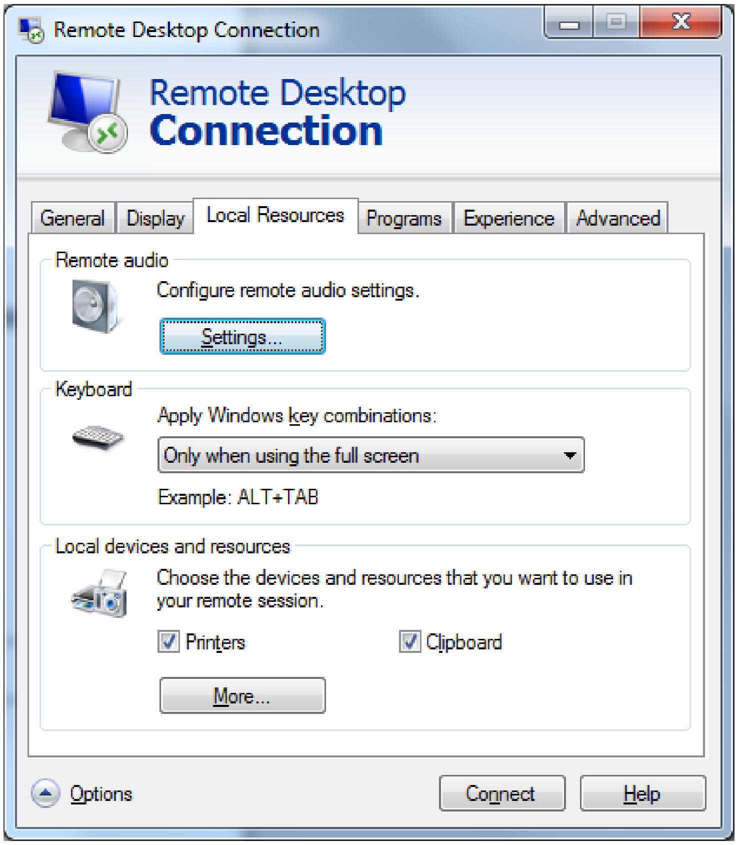
Sound

To enable sound:

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

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

Figure 6: Example of Remote Computer Sound



Configure remote audio settings.

Apply Windows key combinations: Only when using the full screen

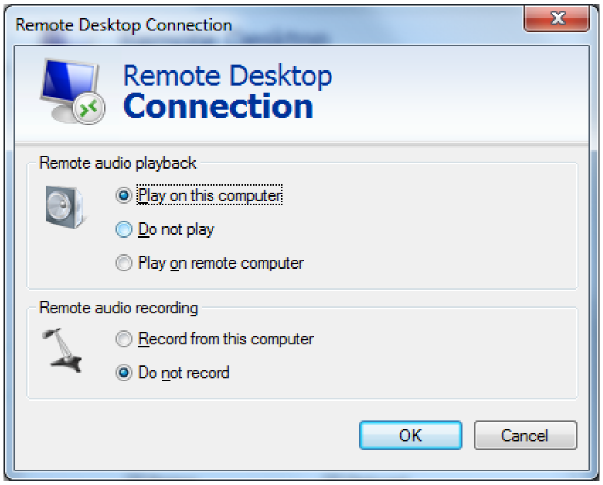
Example: ALT+TAB

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

☑ Printers ☑ Clipboard

9) Select **Play on this computer** (Figure 7) from the Remote audio playback section.
10) 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

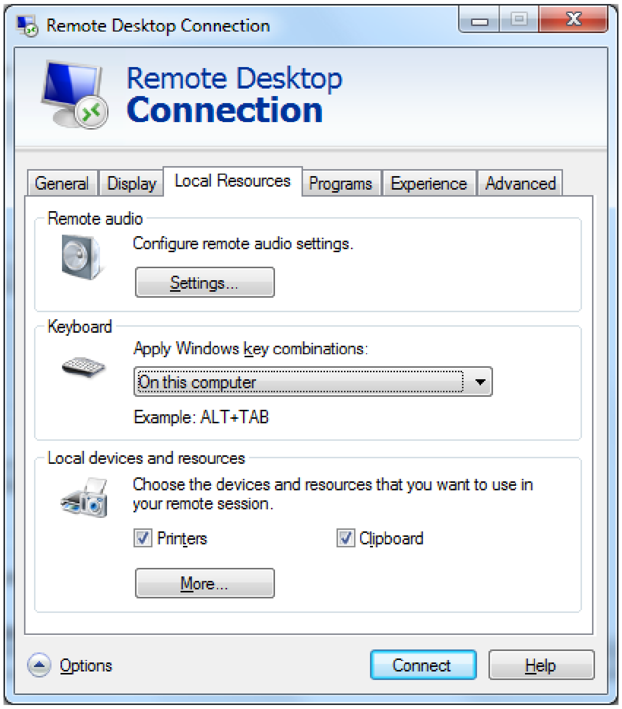
○ Record from this computer
● Do not record

Keyboard

To configure keyboard settings:

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

Figure 8: Example of Remote Computer Keyboard



Remote Desktop Connection

Remote Desktop Connection

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

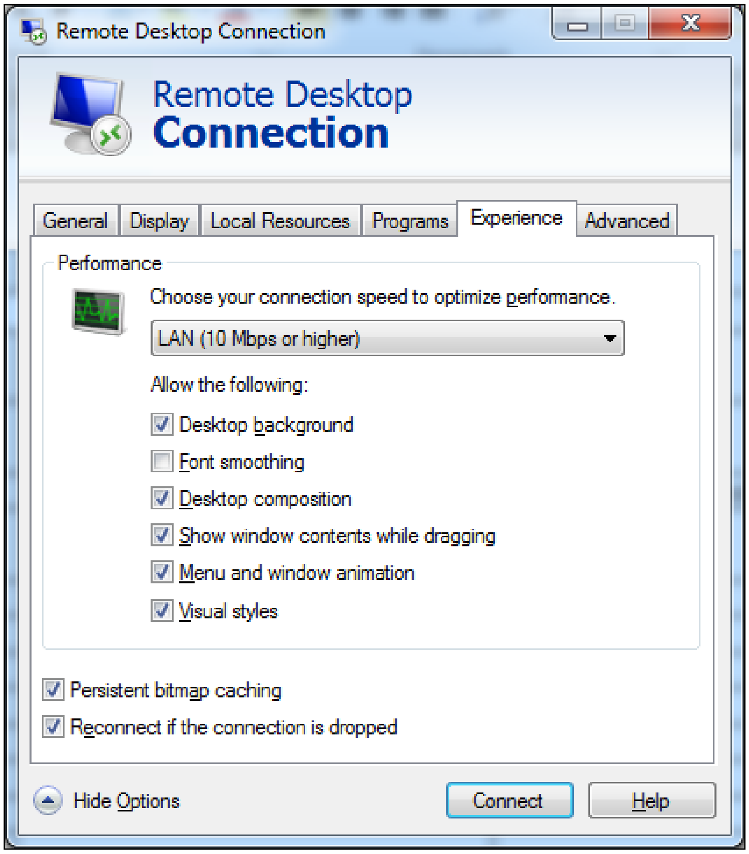
Connection Speed

To set the connection speed:

13) Click the **Experience** tab (Figure 9).

14) Select **LAN (10 Mbps or higher)** from the **Choose your connection speed to optimize performance** drop-down list. Deselect **Font smoothing**.

Figure 9: Example of Connection Speed



Performance

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

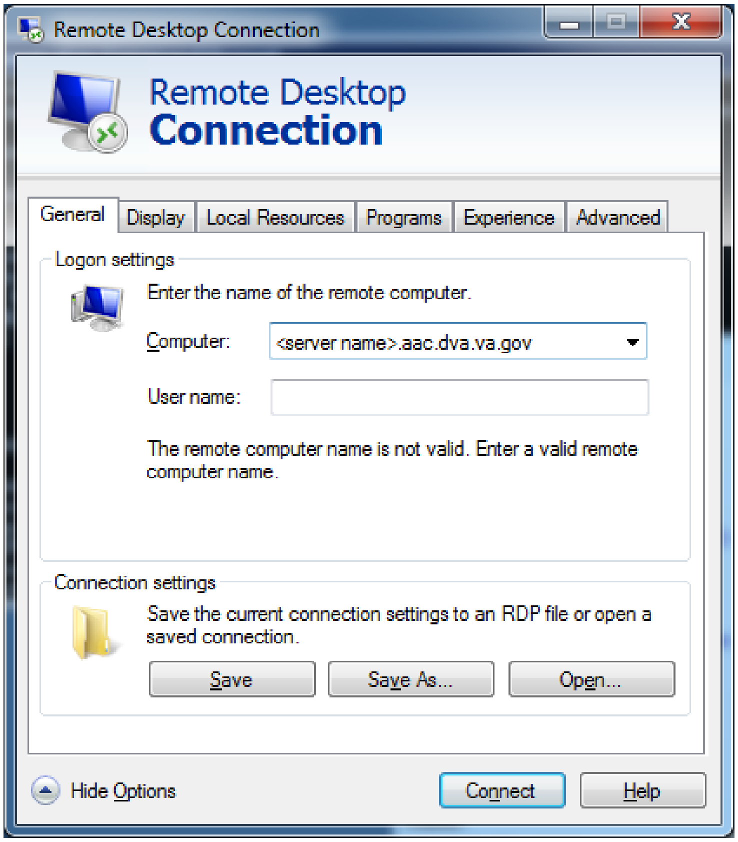
☑ Reconnect if the connection is dropped

Save Settings

To save the settings:

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

Figure 10: Example of General Tab Save As



Enter the name of the remote computer.

Computer: <server name>.aac.dva.va.gov

User name:

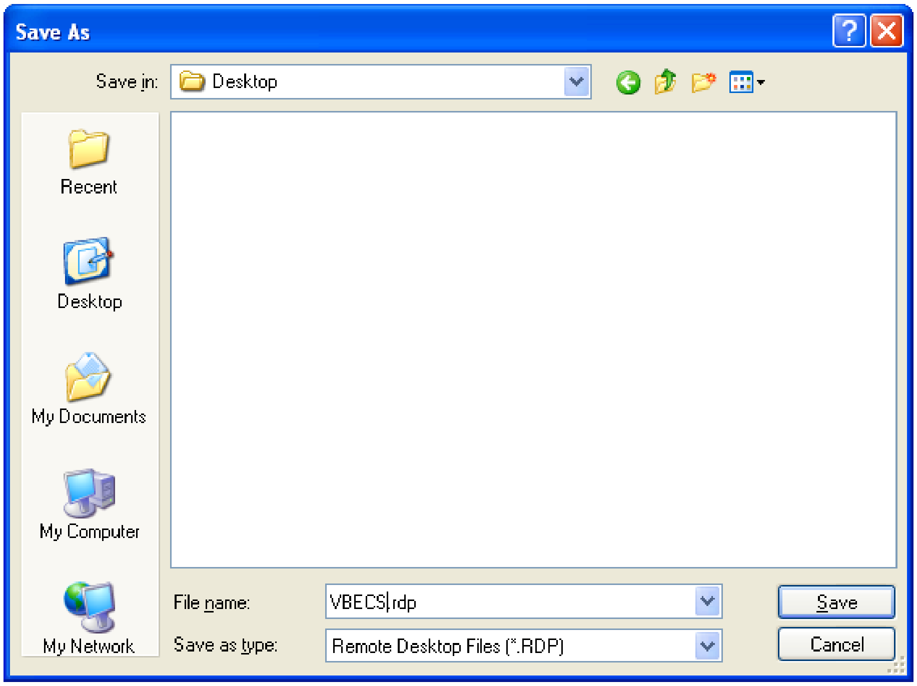
The remote computer name is not valid. Enter a valid remote computer name.

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

Create a Remote Desktop Connection Shortcut for VBECS

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

Figure 11: Example of Remote Desktop Connection Shortcut for VBECS



Save in: Desktop

File name: VBECS.rdp

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

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

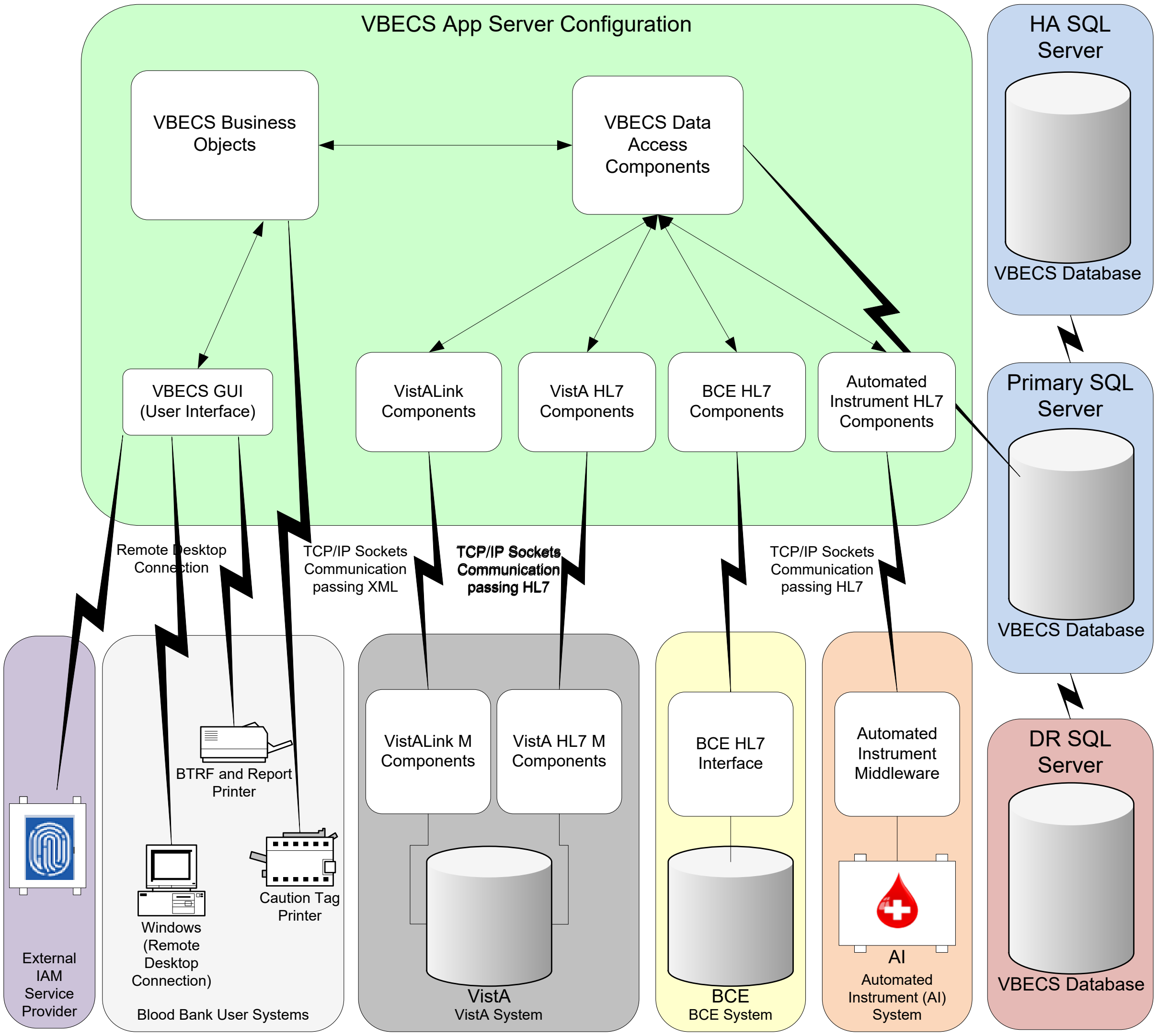
Server Hardware and System Configuration

The VBECS application requires hardware and system software to service the requirements of a user population of five users in a standard configuration and up to twenty-five users in an integrated Veterans Integrated Service Network (VISN) environment.

VBECS is installed in a virtualized environment using vSphere® as the virtualization platform. This section focuses on the configuration of the virtual machines. Table 15 and Table 16 contain the virtual machine specifications for the Application and SQL Servers respectively. 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 other HL7 interfaces 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. Up to 15 sites share a single SQL Server.
  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 SQL Server: This server fields all requests. Its data are replicated to the High Availability and Disaster Recovery servers.
    - High Availability (HA) SQL 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) SQL 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 Workstations**: Users continue to access the VBECS application using Remote Desktop Services.

Figure 12: System Schematic


VBECS App Server Configuration
VBECS Business Objects
VBECS Data Access Components
VBECS GUI (User Interface)
VistALink Components
VistA HL7 Components
BCE HL7 Components
Automated Instrument HL7 Components
HA SQL Server
VBECS Database
Primary SQL Server
VBECS Database
DR SQL Server
VBECS Database
Remote Desktop Connection
TCP/IP Sockets Communication passing XML
TCP/IP Sockets Communication passing HL7
TCP/IP Sockets Communication passing HL7
External IAM Service Provider
BTRF and Report Printer
Windows (Remote Desktop Connection)
Caution Tag Printer
Blood Bank User Systems
VistALink M Components
VistA HL7 M Components
VistA
VistA System
BCE HL7 Interface
BCE
BCE System
Automated Instrument Middleware
AI
Automated Instrument (AI) System

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, Z4MPlus or ZT410; Must print at 300 DPI and have Ethernet connectivity.

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.

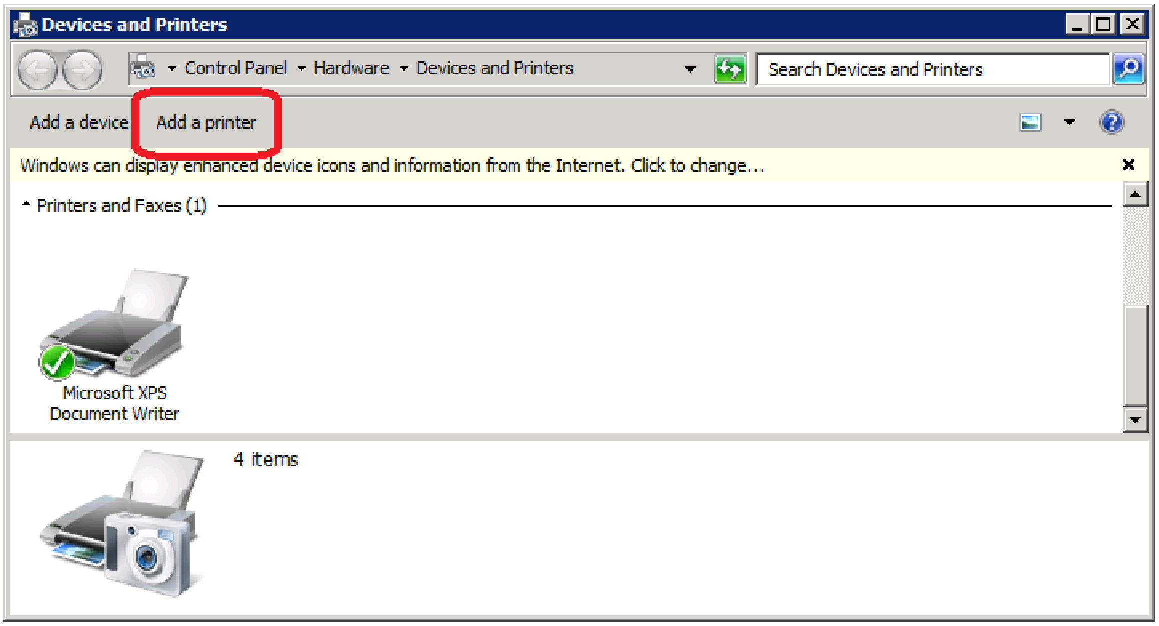
Installing a Printer (Server Administrators Only)

To install a printer, execute the following instructions:

1) Copy the printer driver to the **C:\temp** directory on the app server.
2) Log into the app server with administrative privileges.

3) Click **Start**, **Devices and Printers.** The Device and Printers window is displayed (Figure 13). Click the **Add a printer** button.

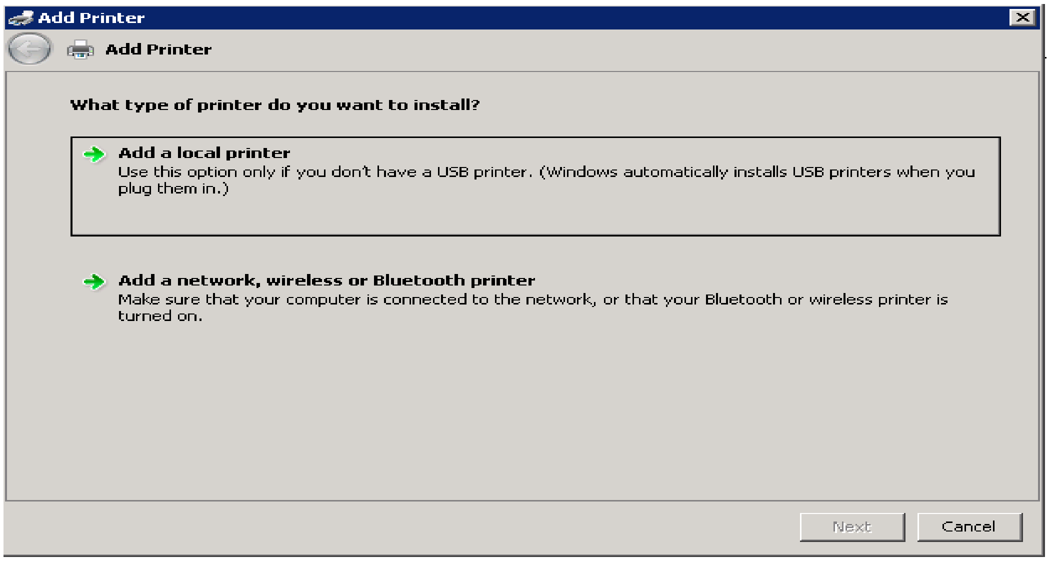
Figure 13: Example of Devices and Printers, Add a printer


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...

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

Figure 14: Example of Add Printer Wizard



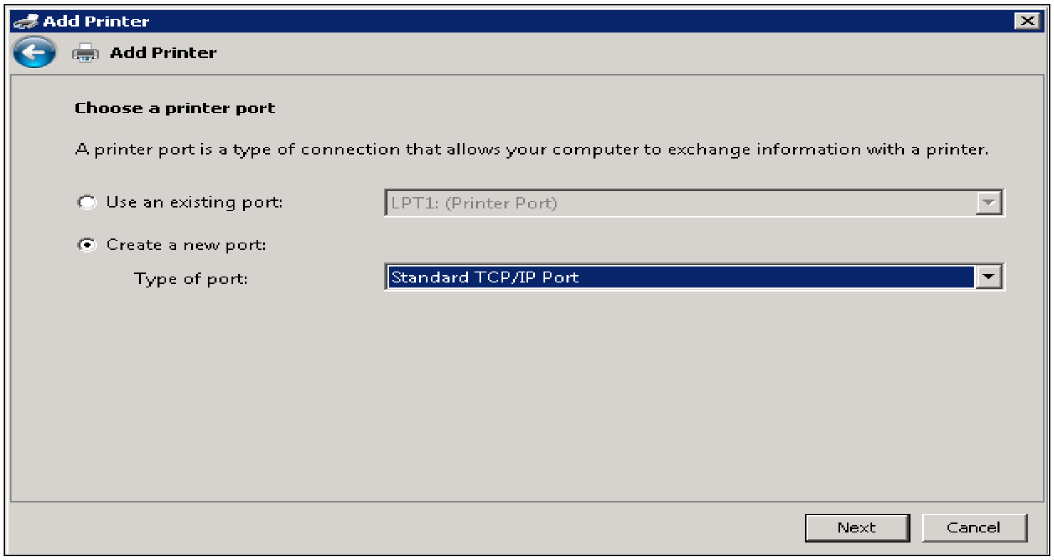
What type of printer do you want to install?

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.

5) 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.

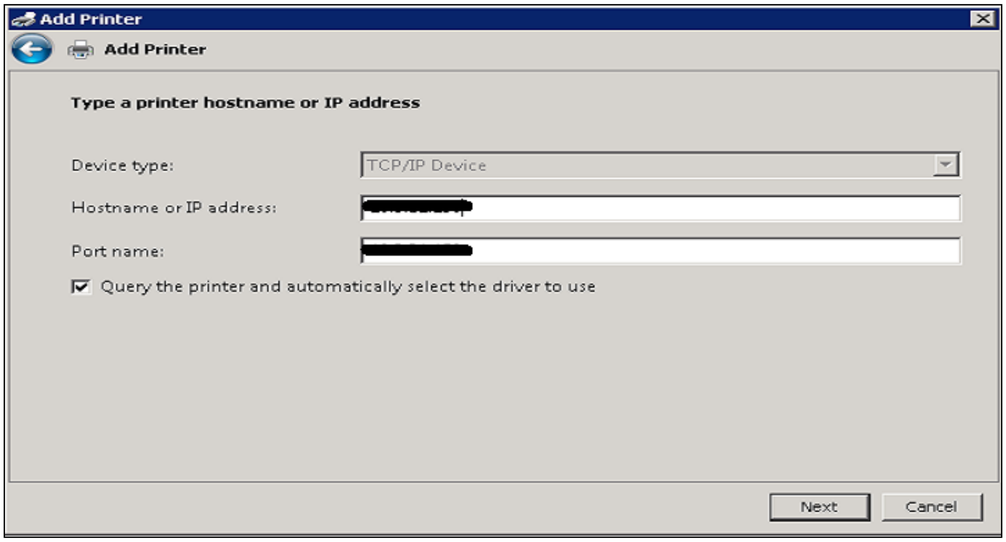
○ Use an existing port: LPT1: (Printer Port)

● Create a new port:

Type of port: Standard TCP/IP Port

6) 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

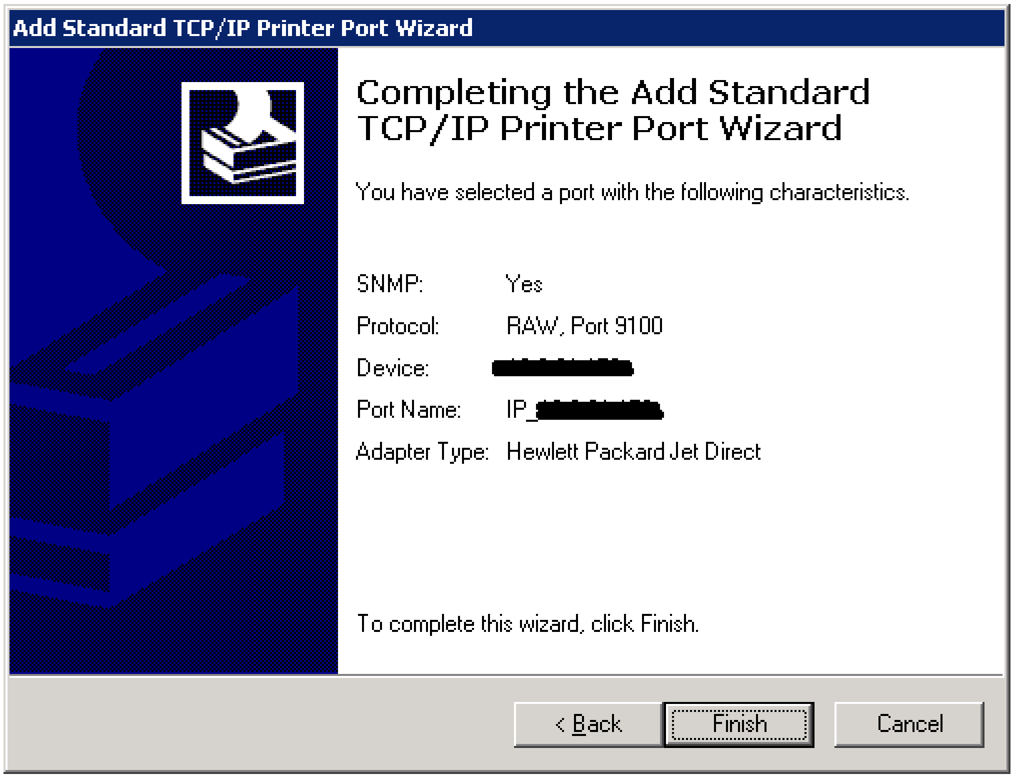
Hostname or IP address: [redacted]

Port name: [redacted]

☑ Query the printer and automatically select the driver to use

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

Figure 17: Example of Review Settings



Add Standard TCP/IP Printer Port Wizard

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: [redacted]

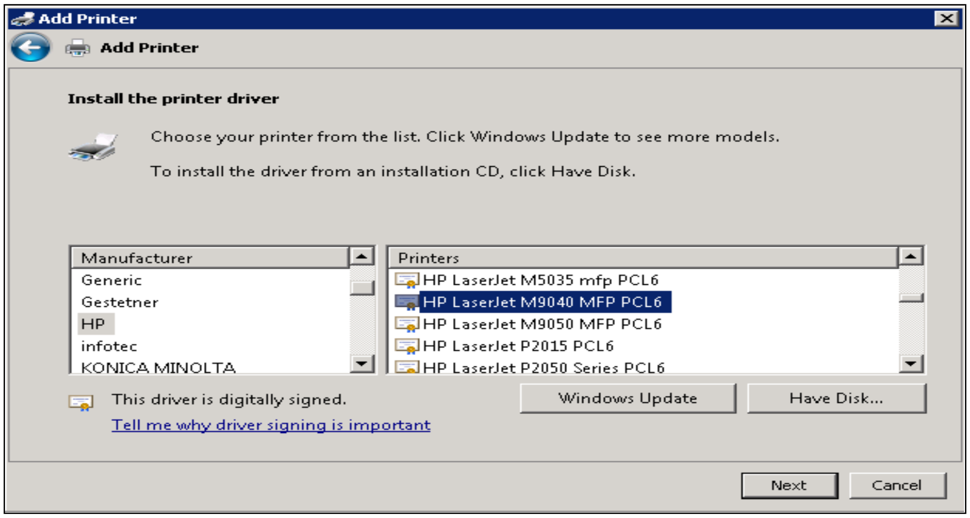
Port Name: IP_[redacted]

Adapter Type: Hewlett Packard Jet Direct

To complete this wizard, click Finish.

8) To select a driver, click **Have Disk** (Figure 18).

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

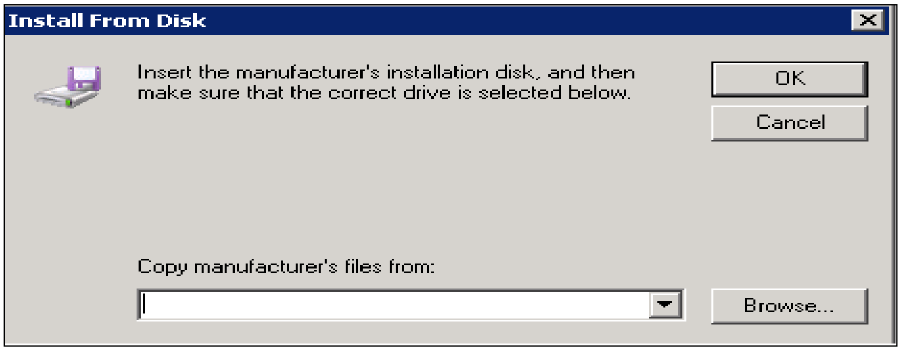
Printers
HP LaserJet M5035 mfp PCL6
HP LaserJet M9040 MFP PCL6
HP LaserJet M9050 MFP PCL6
HP LaserJet P2015 PCL6
HP LaserJet P2050 Series PCL6

This driver is digitally signed.

Tell me why driver signing is important

9) Click **Browse** (Figure 19). Navigate to the driver that you copied to **C:\temp\** in Step 1. Click **Open** (Figure 20).

Figure 19: Example of Install from Disk

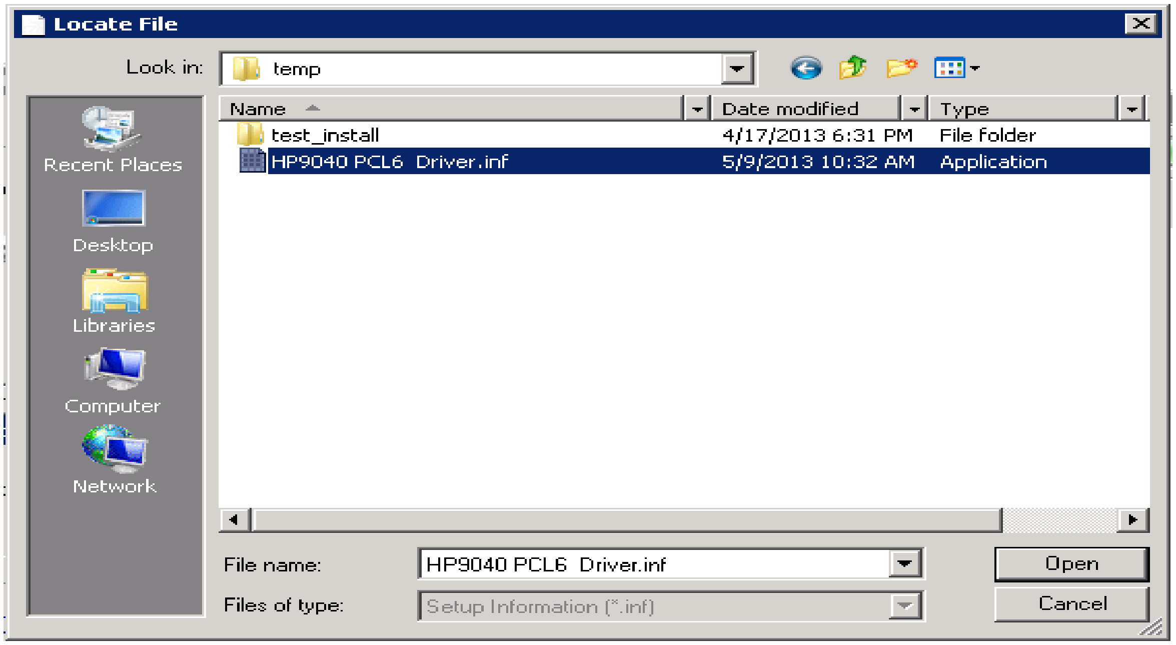


Install From Disk

Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:

Figure 20: Example of Select Driver



Locate File

Look in: temp

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

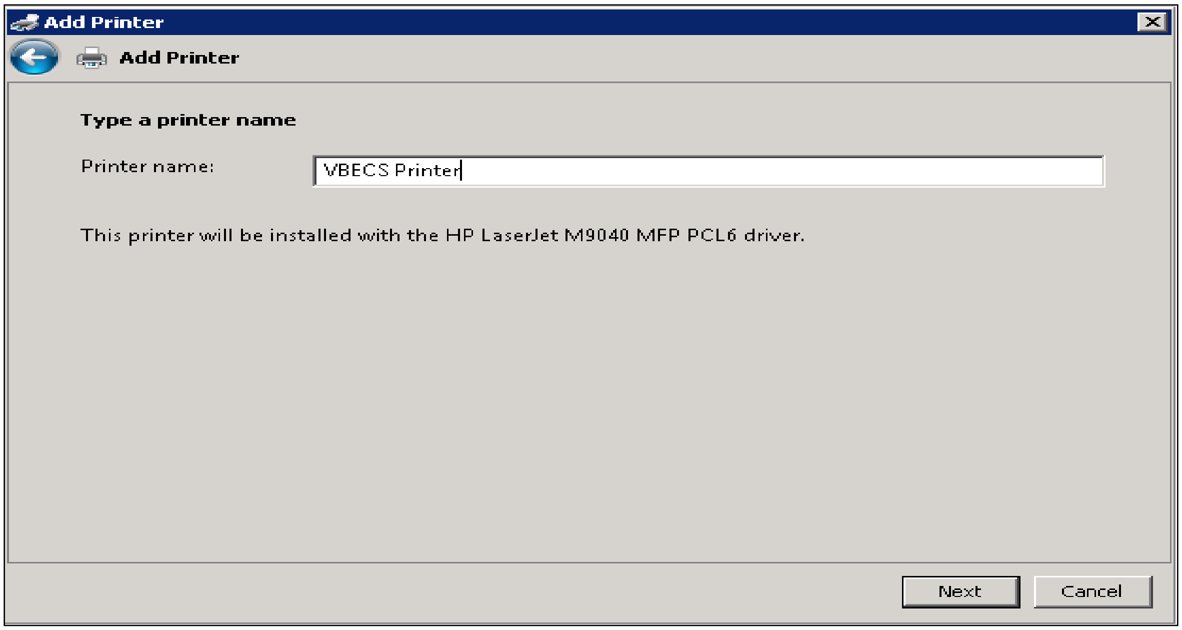
File name: HP9040 PCL6 Driver.inf

Files of type: Setup Information (*.inf)

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

11) 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 21)

Figure 21: Example of Add Printer Wizard



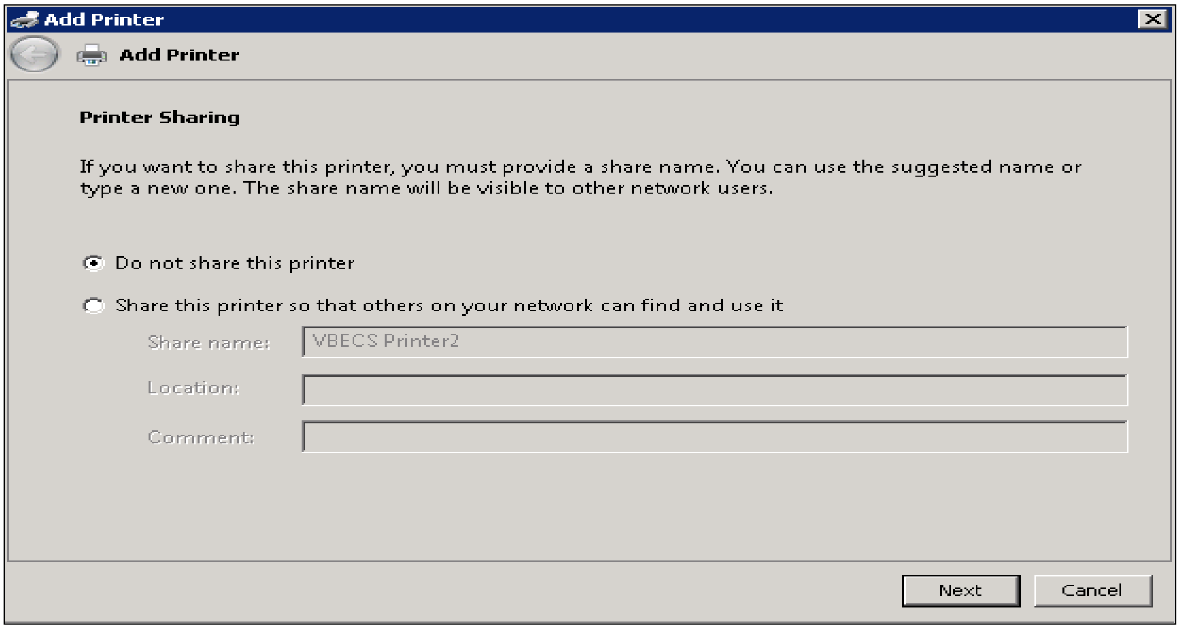
Type a printer name

Printer name: VBECS Printer

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

12) Click the **Do not share this printer** radio button. Click **Next** (Figure 22).

Figure 22: 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

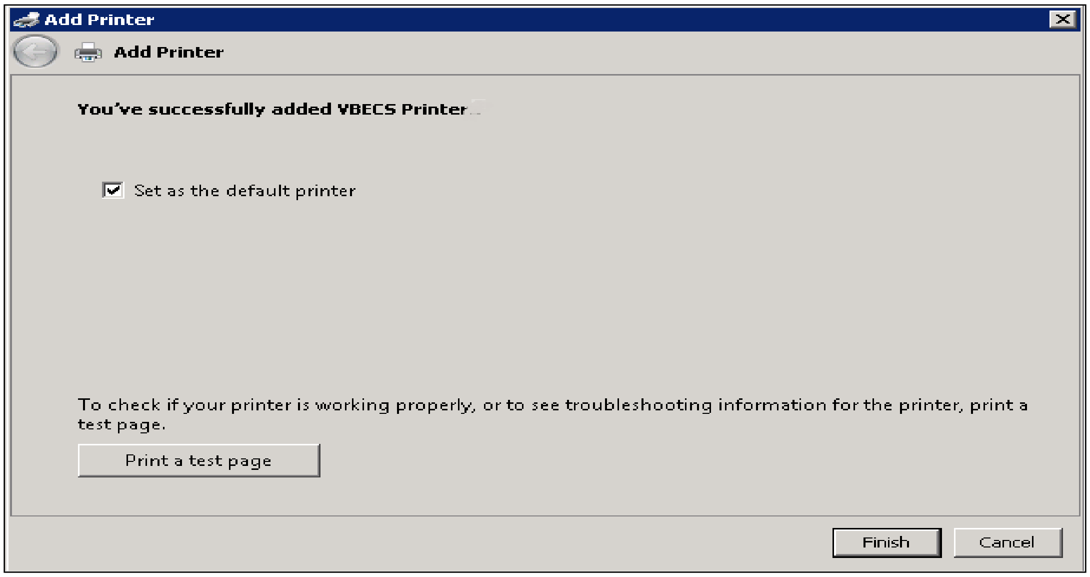
Share name: VBECS Printer2

Location:

Comment:

13) Click **Next** (Figure 23).

Figure 23: Example of Add Printer Wizard



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, Z4Mplus and ZT410)

Do not install the label printer on the VBECS Server. Connectivity is configured in VBECS Administrator (See the VBECS Administrator User Guide).

VBECS is configured to work only with Zebra printers: VBECS uses Zebra Programming 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

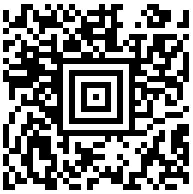
Prior to configuring the label printer, load the ribbon and label stock and ensure that the printer is on. If the printer does not display PRINTER READY, there is a problem that must be resolved before proceeding. Refer to the Zebra user guide or printer CD for more information.

Scanners

Scanners used with VBECS must be able to scan Codabar, ISBT 128, and PDF-417 barcodes. To configure a scanner. VBECS no longer supports entry of new Codabar units into the system.

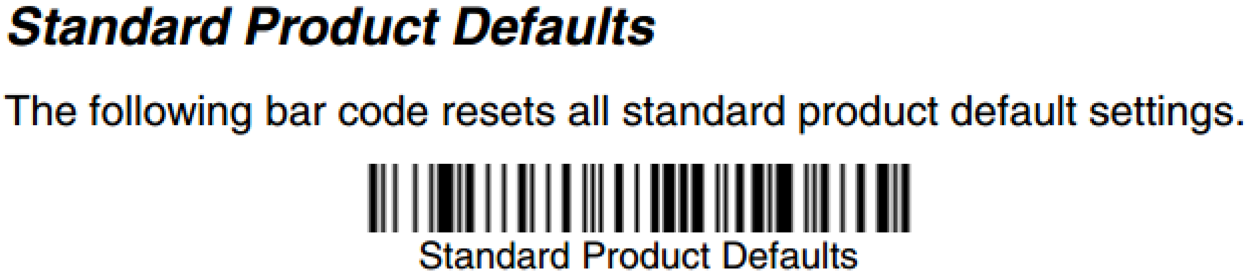
1) Connect the scanner to the workstation.
    a. To configure a **Hand-Held 4600** scanner, scan the barcode in Figure 24.

Figure 24: Configuration Barcode for a Hand-Held 4600



    b. The configuration barcodes below only apply to the **Honeywell Xenon 1900** series scanner. Do not try to configure any other scanners with these barcodes. To configure a **Honeywell Xenon 1900** scanner, scan the **Standard Product Defaults** barcode in Figure 25 followed by the **VBECS Default** barcode in Figure 26.

Figure 25: Xenon 1900: Restore Defaults

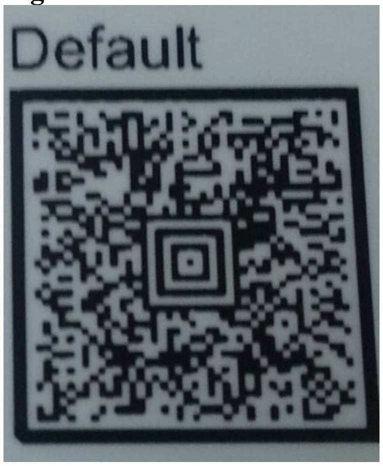


Standard Product Defaults

The following bar code resets all standard product default settings.

Standard Product Defaults

Figure 26: Xenon 1900: VBECS Settings



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

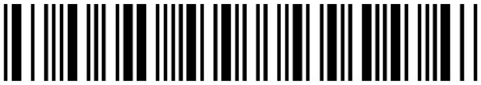


Figure 28: ISBT 128

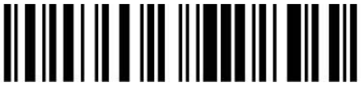
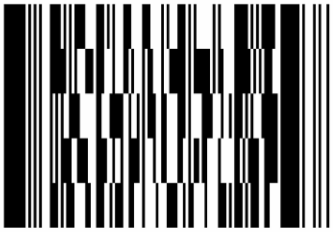


Figure 29: PDF 417



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
- Input Devices: U.S. 101-key keyboard, mouse
- Audio: Sound card and speakers
- Personal Identity Verification (PIV) card reader: required for PIV card access

Report Share

The VBECS system provides a share for users to access reports from their workstations (see Configure a Shortcut to the Report Share). While VBECS administrators have the ability to create and delete files and folders, users have read-only access to the share.

Implementation and Maintenance (Data Center 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	Wednesday, two weeks after 2nd Tuesday of the month	See Applying Windows Updates.
VBECS Reports folder cleanup	As needed	Users are able to export reports to the division subfolder located within D:\VBECSReports folder on the App Server. The D drive is 10 GB in size and logs are also stored there. Whenever the drive is over 90% full, old reports must be deleted. This activity may be performed by a blood bank supervisor or by a server administrator in coordination with blood bank personnel. For multidivisional sites, each division's subfolder should be maintained by its respective 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 REDACTED.

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).

Table 5: VBECS Level Jobs

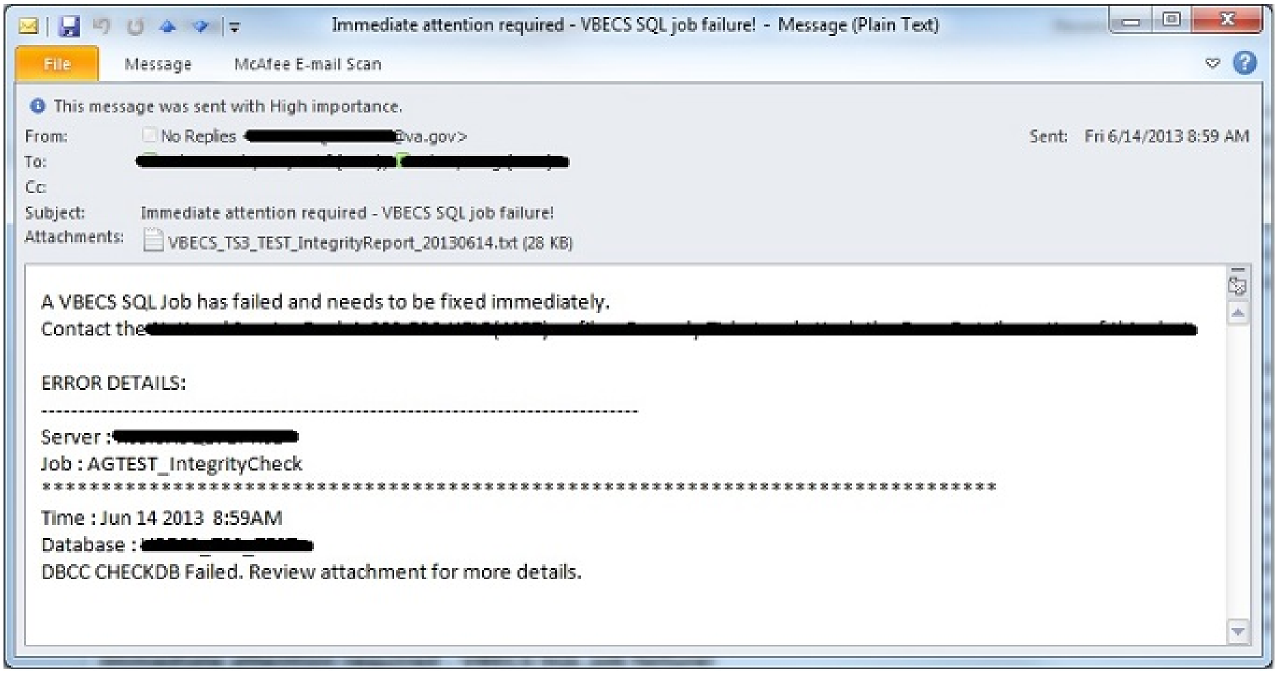
Databases Affected	Job Name	Start Time
(Test SQL Server) VBECS_*SSS*_TEST (SSS is equal to the Site Code)	AGVISN*XX*_VBECS_*SSS*_TEST_Background_Jobs	12:01am
(Production SQL Server) VBECS_*SSS*_PROD	AGVISN*XX*_VBECS_*SSS*_PROD_Background_Jobs	

SQL Maintenance Job Alerts

Email alert messages are sent only when a SQL maintenance job fails. System Level job alerts are sent to REDACTEDRefer to the *VistA Blood Establishment Computer Software (VBECS) Admin User Guide.*

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 the Service Desk Primary Contact. 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 30).

Figure 30: 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 [redacted]@va.gov>

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

To: [redacted]

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 [redacted]

ERROR DETAILS:
-------------------------------------------------------------------------------
Server : [redacted]
Job : AGTEST_IntegrityCheck
******************************************************************************************
Time : Jun 14 2013  8:59AM
Database : [redacted]
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

> *App server updates require downtime, which is detailed in Table 6 and Table 7. SQL server updates require no downtime.*

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 and Table 7).

Microsoft typically releases Windows updates on the second Tuesday of the month, commonly referred to as **Patch Tuesday (PT)**. The monthly updates are analyzed by the AITC Infrastructure Team and a patch offering is created in IBM's BigFix software. The BigFix software analyzes each server to determine which updates are needed.

All Windows updates are tested before being released to customer VBECS servers:

1) AITC staff installs Windows updates to VBECS development test servers.
2) VBECS maintenance team tests the updated pre-production servers and proves that the updates do no harm to VBECS.
3) After the VBECS maintenance team approves the updates, AITC staff creates change orders for applying the approved Windows Updates to the remaining VBECS servers.

BigFix Patch Windows

- **Patch Offer**: On-demand (pull) method. Patches are downloaded and installed manually by AITC staff.
- **PreProd - TUE 0000 Manual**: Patches are pushed out to servers and installed @00:00AM on Tuesday (PT + 7 days).
- **Prod - Second Saturday 0500 Manual**: Patches are pushed out to servers and installed @5:00AM on Saturday (PT + 11 days).

Table 6: Customer System Patch Schedule

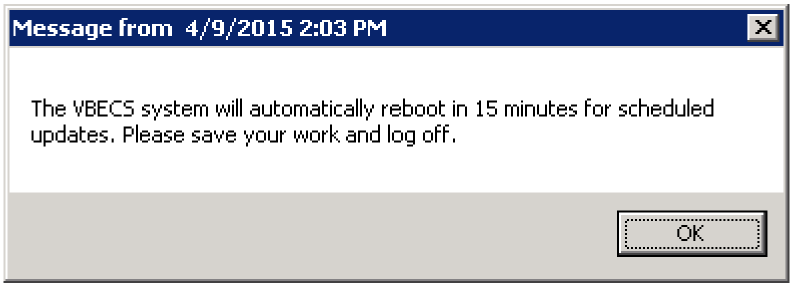
Patch Day	Environment	Affected Servers	VBECS Downtime	Server Reboot	BigFix Patch Window
Tuesday PT + 14 days	Customer	SQL Servers (Test)	NO	08:00 AM CST	Patch Offer
Wednesday PT + 15 days	Customer	App Servers	YES	10:00 AM local	Prod - Second Saturday 0500 Manual
	Customer	SQL Servers (Production)	NO	08:00 AM CST	Patch Offer
	Customer	Qurorum Server	NO	10:00 AM CST	Prod - Second Saturday 0500 Manual

Table 7: Development System Patch Schedule

Patch Day	Environment	Affected Servers	VBECS Downtime	Server Reboot	BigFix Patch Window
Monday PT + 6 days	Development	SQC 700s	NO	09:30 AM CST	Patch Offer
Tuesday PT + 7 days	Development	APP7AUS QOR600	YES	08:00 AM CST	PreProd - TUE 0000 Manual
Tuesday PT + 14 days	Development	APP750 APP751 SQC 750s	NO	10:00 AM CST	Prod - Second Saturday 0500 Manual
	Product Support	PRD200 PRD201	YES	10:00 AM CST	Prod - Second Saturday 0500 Manual

On the designated patch day, VBECS App servers will notify any user connected to the server before the server is restarted. At 9:45AM (local time), users will see a message similar to the message displayed in Figure 31. Unless the users log off, they will receive additional messages at 9:50, 9:55, 9:56, 9:57, 9:58 and 9:59AM local time.

Figure 31: 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.

How long will VBECS be down?

Windows updates are unpredictable and can take anywhere from 30 to 120 minutes to finish installing. During this time, the VBECS App server will not be available. Patching speed can be affected by increased patch size or quantity as well as datacenter load. As a result, patching times may vary month-to-month. We recommend trying to reconnect every 10-15 minutes.

If you are unable to reconnect to your VBECS app server by 11:30 AM local time, contact the Service Desk Primary Contact.

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

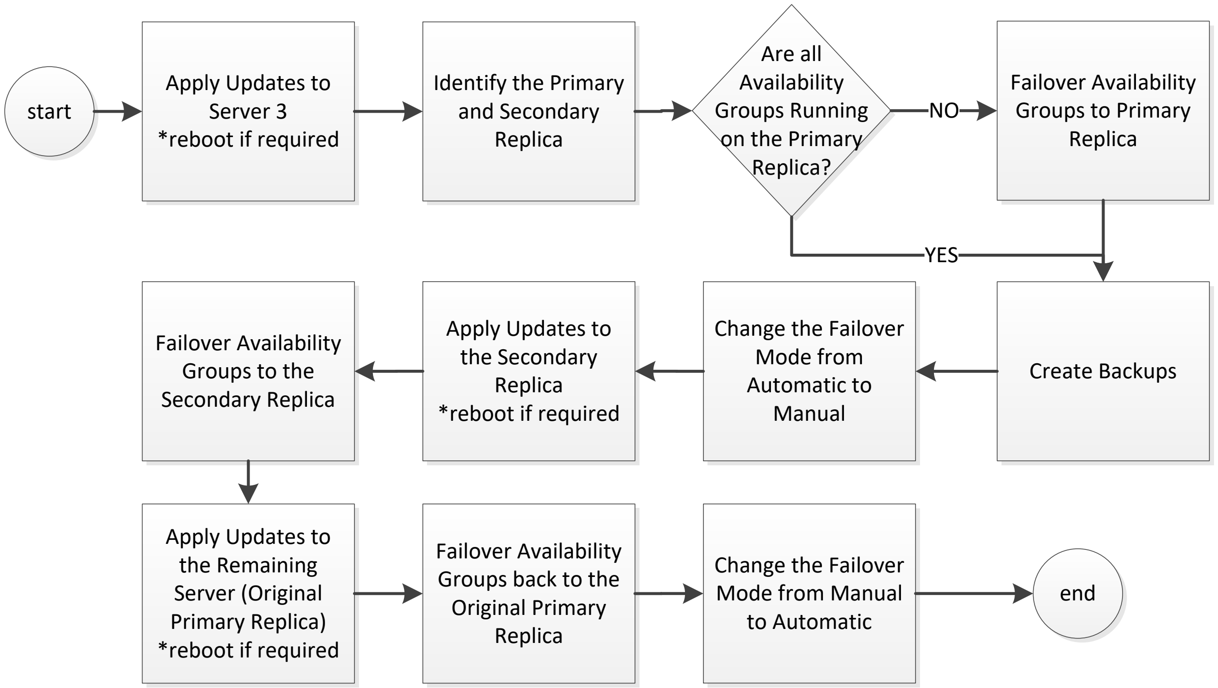
Replica is another name for a server within a SQL Server AlwaysOn configuration.

The names of the VBECS SQL servers can be found on the Data Center Worksheet.

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 33 for the proper execution order.

Figure 32: 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
Failover Availability Groups to Primary Replica
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

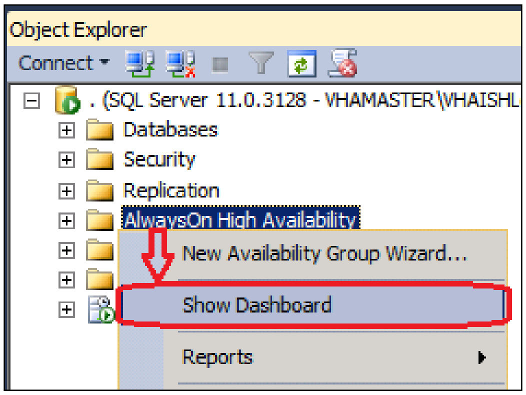
1) Open a remote desktop connection to Server 3 of the VBECS SQL Server system.
2) Apply the Windows/Software Updates using the supplied instructions for the updates (reboot Server 3 only if instructed).

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**.

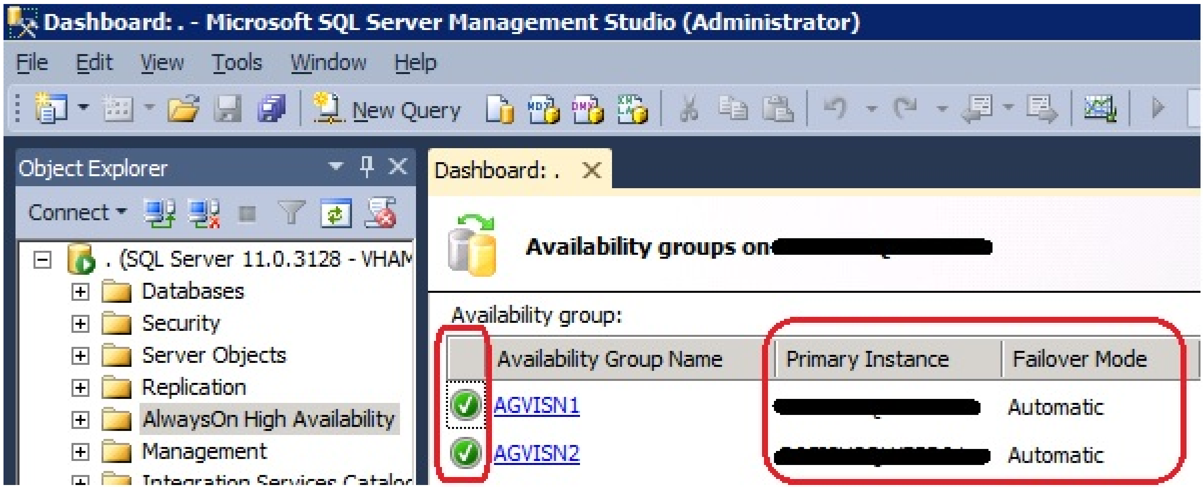
4) When prompted to connect to a server, enter the name of Server 1 in the **Server Name** field and click **Connect**. Note 1: VBECS Test system SQL Servers are named differently than production SQL servers. Note 2: If you have issues connecting, use the fully qualified domain name.
5) On the left side of the SQL Server Management Studio (SSMS) screen is the Object Explorer pane. Within the Object Explorer pane, right-click on the A**lwaysOn High Availability** folder and select **Show Dashboard** (Figure 35).

Figure 33: 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 36) 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 34: Example of the SQL Server Dashboard


Dashboard: . - Microsoft SQL Server Management Studio (Administrator)
File
Edit
View
Tools
Window
Help
New Query
Object Explorer
Connect ▾
. (SQL Server 11.0.3128 - VHAM
Databases
Security
Server Objects
Replication
AlwaysOn High Availability
Management
Integration Services Catalog
Dashboard: .

Availability groups on [redacted]

Availability group:

	Availability Group Name	Primary Instance	Failover Mode
✓	AGVISN1	[redacted]	Automatic
✓	AGVISN2	[redacted]	Automatic

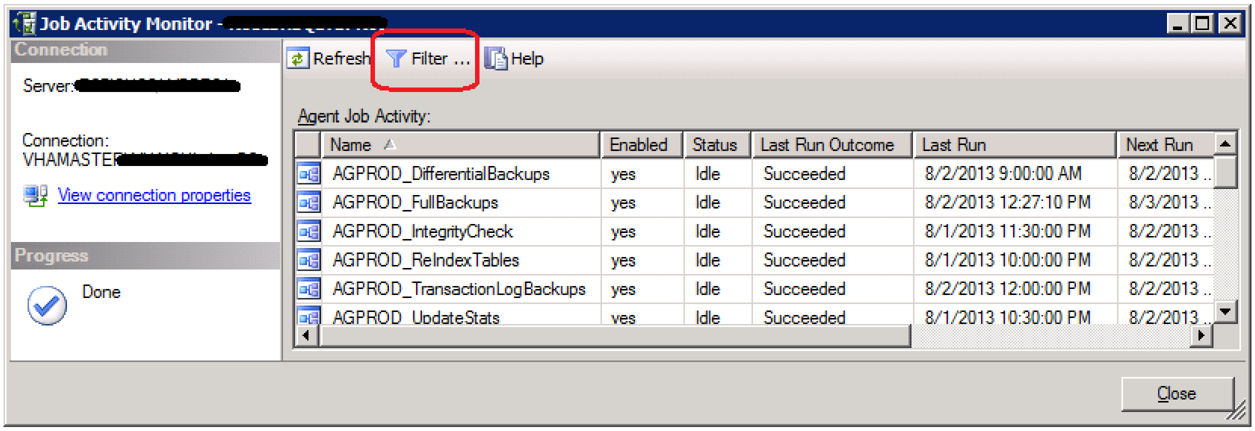
If any Availability Group status indicators are ⊗ or if there are a mix of ✓ and ○ indicators, VBECS is down and the problem must be resolved immediately.

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 37).

Figure 35: Example of Job Activity Monitor



Server: [redacted]

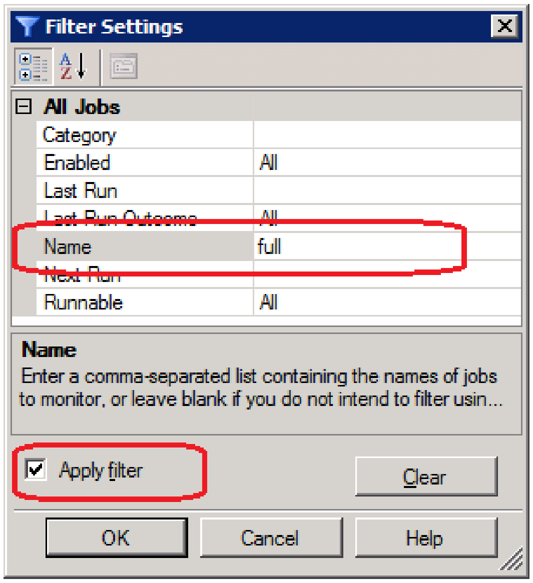
Connection:
VHAMASTER[redacted]

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 ..

12) In the Filter Settings window, enter **full** in the **Name** field, check the **Apply filter** box and click **OK** (Figure 38).

Figure 36: Filter Settings



Filter Settings

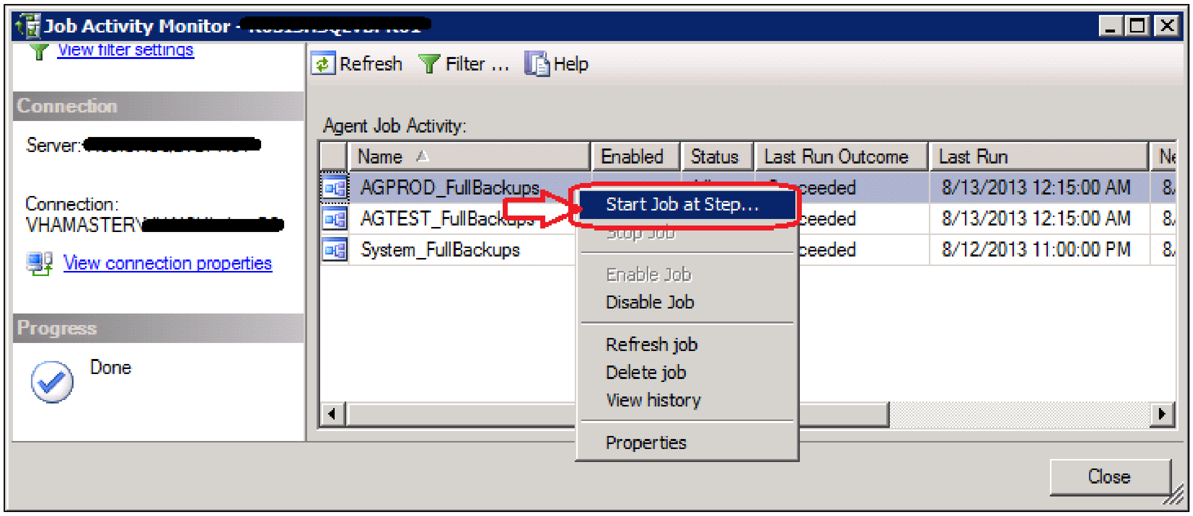
All Jobs	
Category	
Enabled	All
Last Run	
Last Run Outcome	All
Name	full
Next Run	
Runnable	All

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

13) Right-click the first job in the filtered list and select **Start Job at Step…** (Figure 39).

Figure 37: Example Starting a SQL Job



Job Activity Monitor - [redacted]

Server: [redacted]

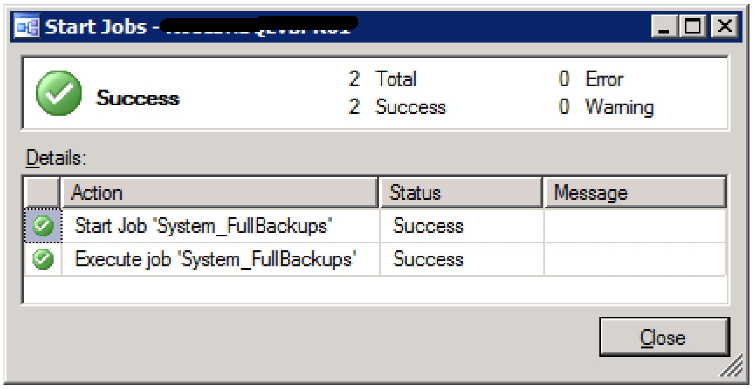
Connection:
VHAMASTER\[redacted]

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 40). Verify the status indicator is **Success** before clicking **Close**.

Figure 38: Example Job Completion Message



Start Jobs - [redacted]

✓ Success

2	Total	0	Error
2	Success	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.

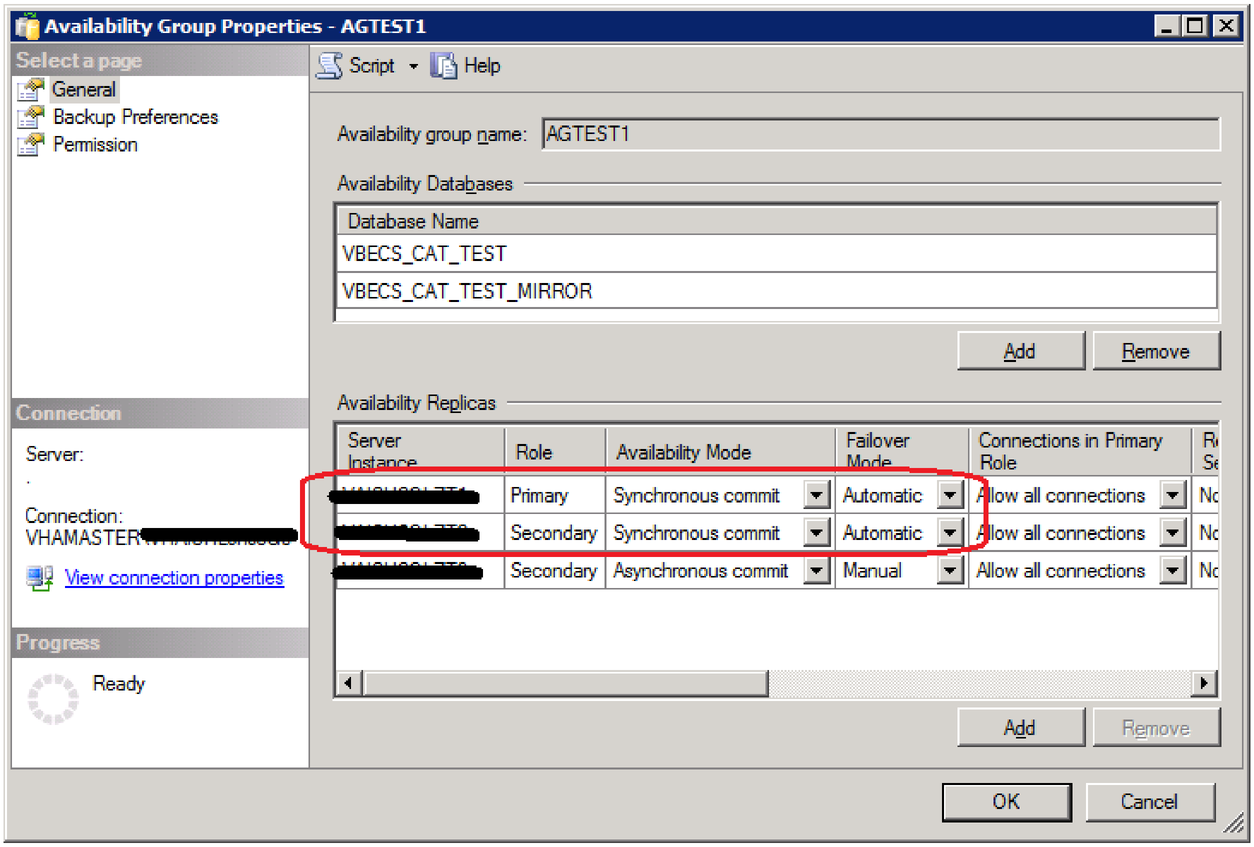
If any of the jobs fail to complete successfully, please notify the appropriate support personnel immediately by contacting the Service Desk Primary Contact.

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 41). 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 39: 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
[redacted]	Primary	Synchronous commit	Automatic	Allow all connections	Nc
[redacted]	Secondary	Synchronous commit	Automatic	Allow all connections	Nc
[redacted]	Secondary	Asynchronous commit	Manual	Allow all connections	Nc

Server:
.

Connection:
VHAMASTER[redacted]

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.

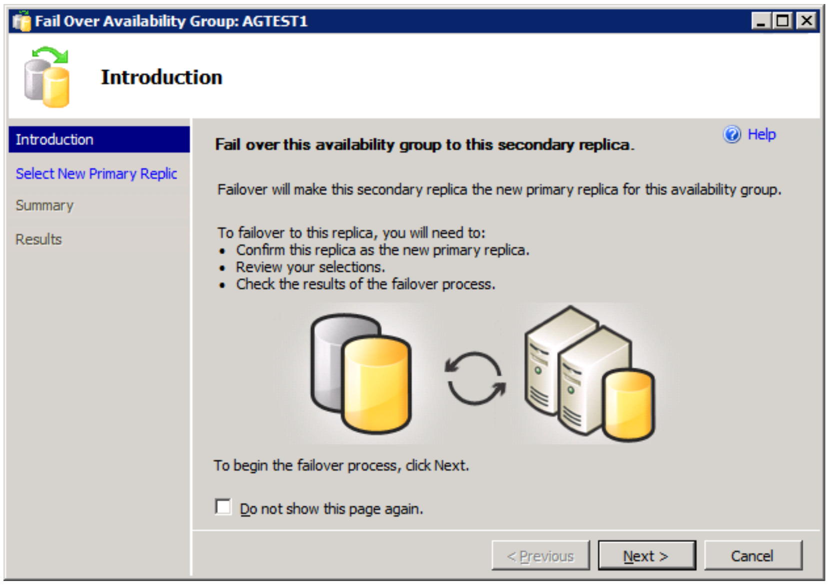
Apply Updates to the Secondary Replica

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 42).

Figure 40: 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:

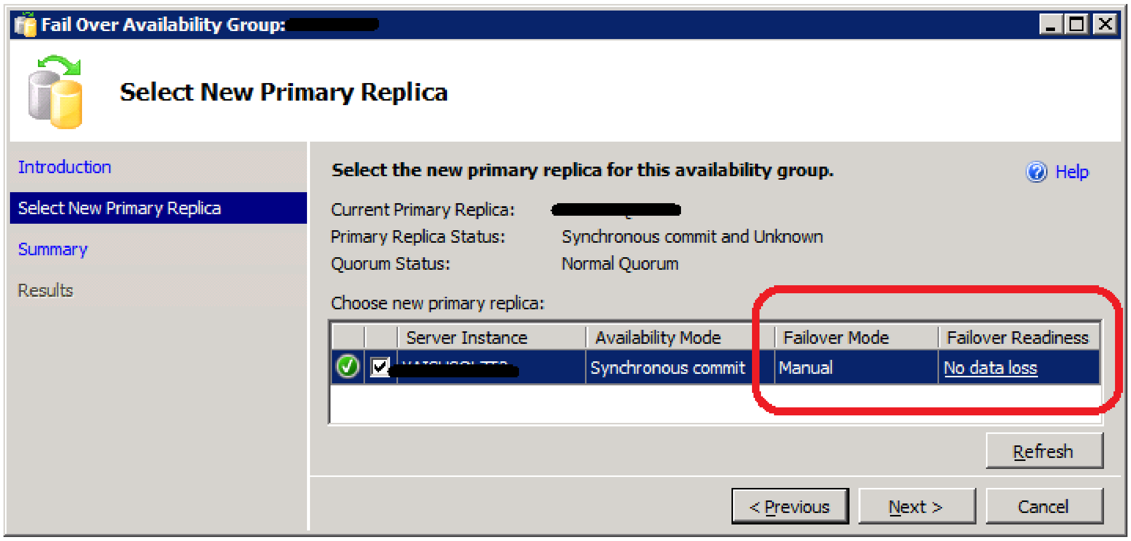
- Confirm this replica as the new primary replica.
- Review your selections.
- Check the results of the failover process.

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 43). 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 41: Example of Selecting the New Primary Replica



Fail Over Availability Group: [redacted]

Select New Primary Replica

Select the new primary replica for this availability group.

Current Primary Replica: [redacted]
Primary Replica Status: Synchronous commit and Unknown
Quorum Status: Normal Quorum

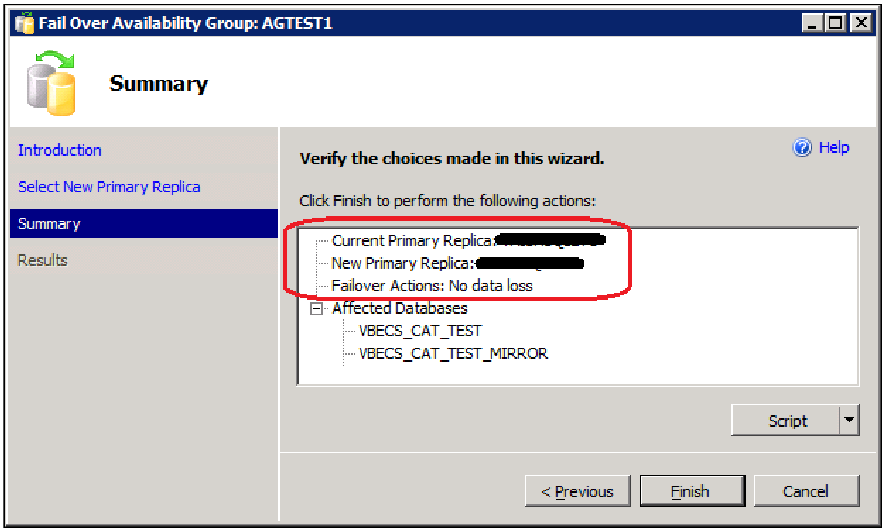
Choose new primary replica:

		Server Instance	Availability Mode	Failover Mode	Failover Readiness
✓	☑	[redacted]	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 by contacting the Service Desk Primary Contact.*

29) A Summary window is displayed (Figure 44). 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 42: Example of Availability Group Failover Wizard Summary



Verify the choices made in this wizard.

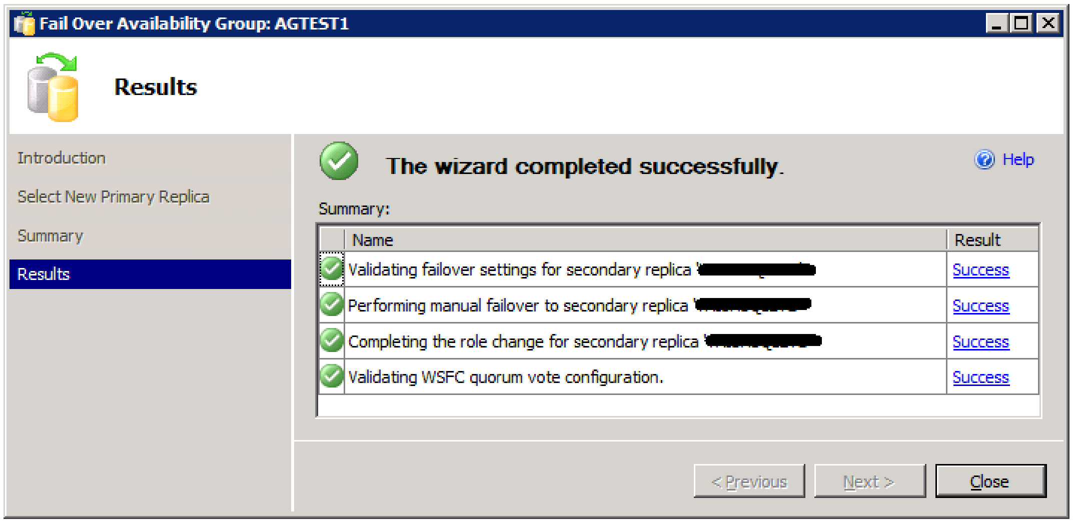
Click Finish to perform the following actions:

- Current Primary Replica: [redacted]
- New Primary Replica: [redacted]
- 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 45).

Figure 43: 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 [redacted]	Success
✓ Performing manual failover to secondary replica [redacted]	Success
✓ Completing the role change for secondary replica [redacted]	Success
✓ Validating WSFC quorum vote configuration.	Success

If any of the Results indicate Error, Warning or Failure, contact SQL Server support personnel by contacting the Service Desk Primary Contact. 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 42).
39) Verify the Failover Mode is **Manual** and Failover Readiness is **No data loss**. Click **Next** (Figure 43). 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 (contact the Service Desk Primary Contact).*

40) A Summary window is displayed (Figure 44). 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 45).

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

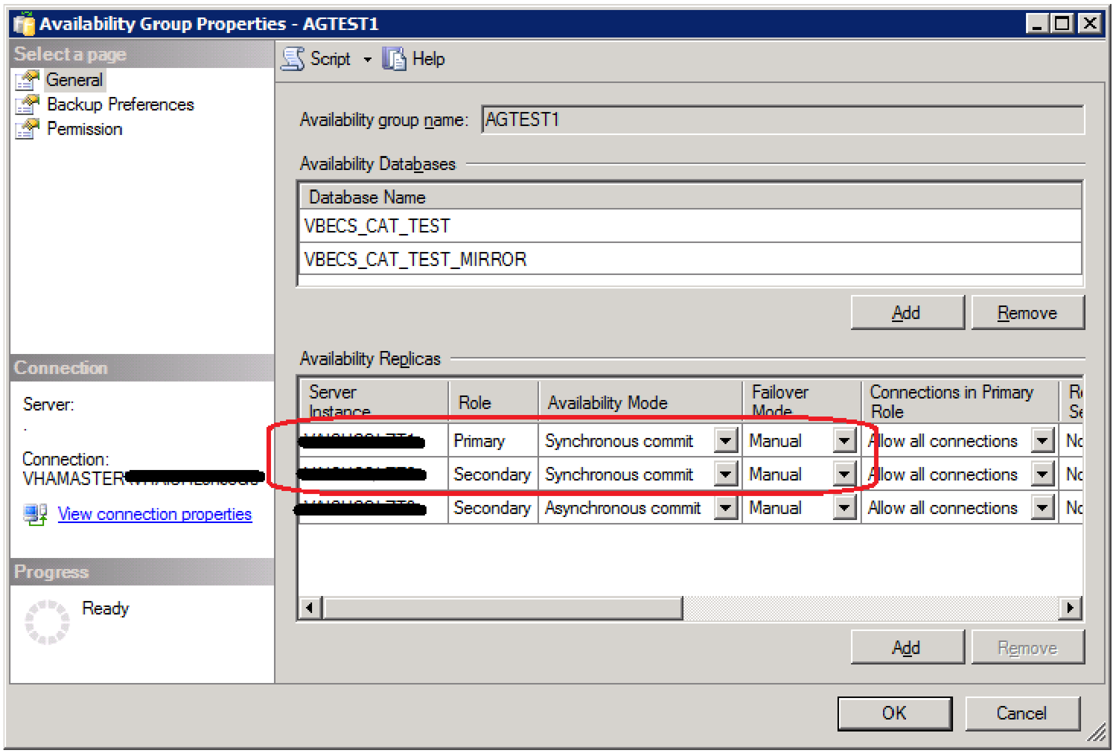
43) Repeat Steps 28 through 42 for each AG on the server.

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 46). Change both **Failover Mode** cells from **Manual** to **Automatic** and click **OK**.

Figure 44: Example of the Availability Group Properties



Availability Group Properties - AGTEST1

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
[redacted]	Primary	Synchronous commit	Manual	Allow all connections	No
[redacted]	Secondary	Synchronous commit	Manual	Allow all connections	No
[redacted]	Secondary	Asynchronous commit	Manual	Allow all connections	No

Connection

Server:
.

Connection:
VHAMASTER[redacted]

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.

This page intentionally left blank.

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

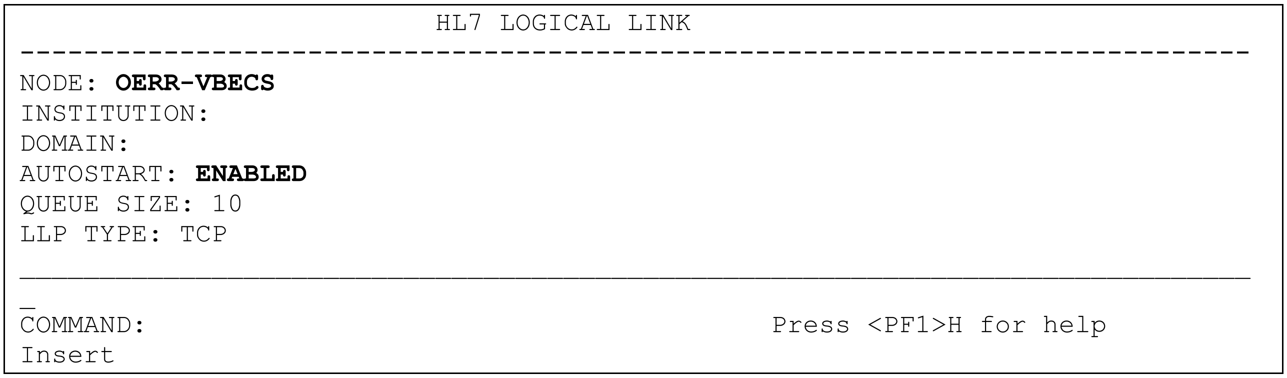
1) At the “Select HL7 Main Menu Option:” prompt, enter **Filer**.
2) Shut down the logical link.
3) At the “Select Filer and Link Management Options Option:” prompt, enter **Link Edit**.
4) At the “Select HL LOGICAL LINK NODE:” prompt, enter **OERR-VBECS** (Figure 47).

Figure 45: 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 48).
6) Move the cursor to the LLP TYPE field and press **Enter** (Figure 48).

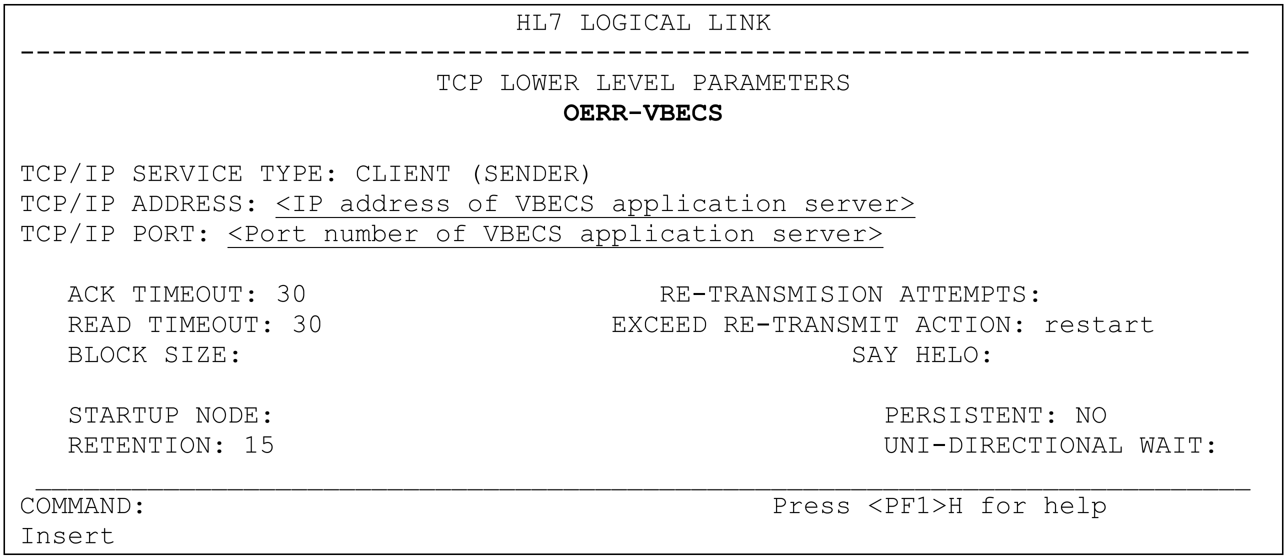
Figure 46: HL7 Logical Link



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

7) 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 (unique) port numbers. Unique port numbers are in the format 1mn93 for Test and 1mn94 for Prod, where "mn" is the site specific "magic number". Standard port numbers of 21993 for Test and 21994 for Prod can be used if unique ports have not been assigned.
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 47: TCP Lower Level Parameters: OERR-VBECS



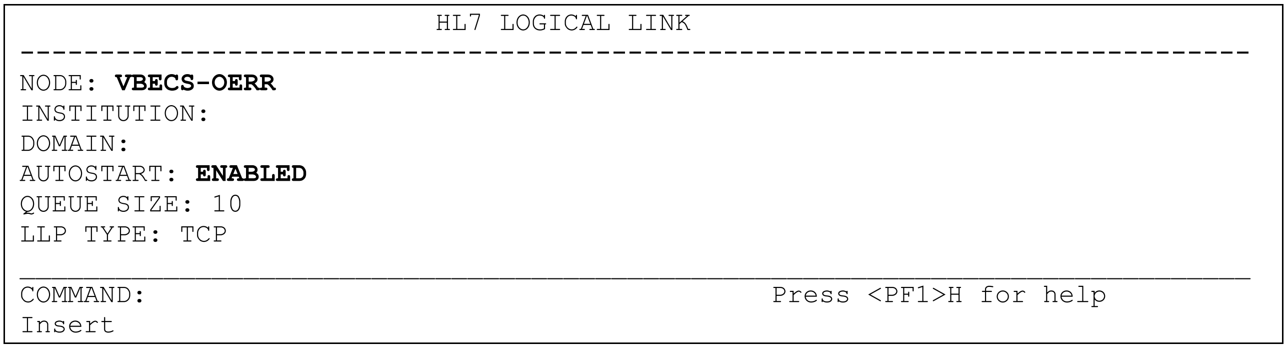
```
                                HL7 LOGICAL LINK
-----------------------------------------------------------------------------
                           TCP LOWER LEVEL PARAMETERS
                                   OERR-VBECS

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 47).
4) Enter **Enabled** in the AUTOSTART field (Figure 50).
5) Move the cursor to the LLP TYPE field and press **Enter** (Figure 50).

Figure 48: HL7 Logical Link

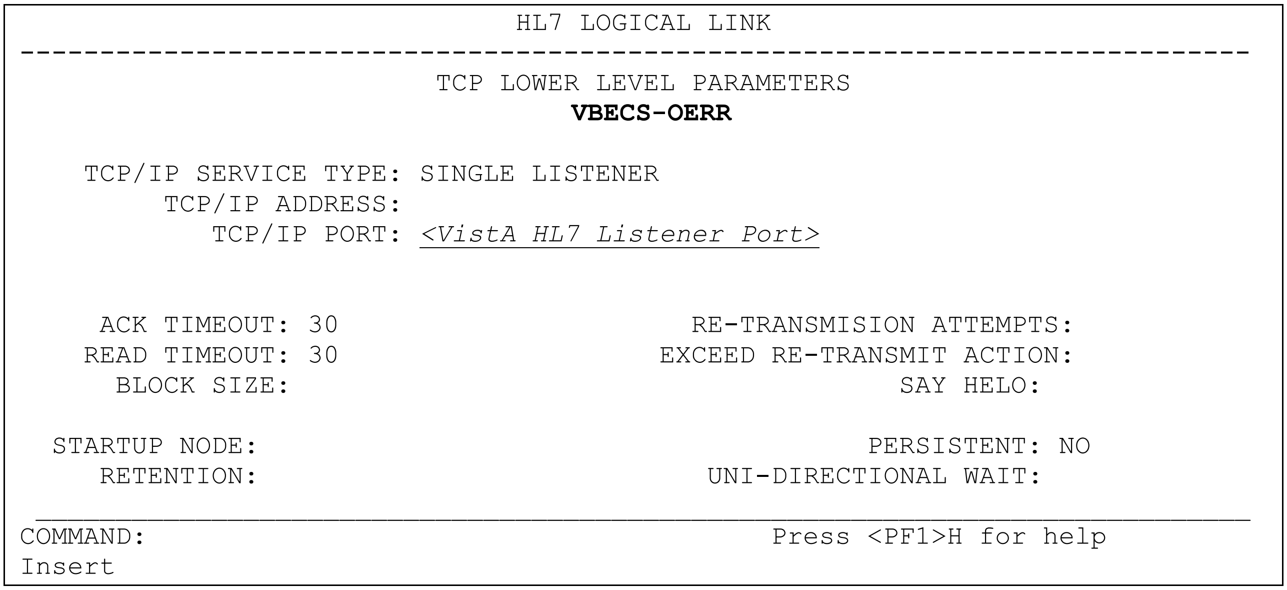


```
                          HL7 LOGICAL LINK
------------------------------------------------------------------------------
NODE: VBECS-OERR
INSTITUTION:
DOMAIN:
AUTOSTART: ENABLED
QUEUE SIZE: 10
LLP TYPE: TCP
______________________________________________________________________________
COMMAND:                                        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 49: 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

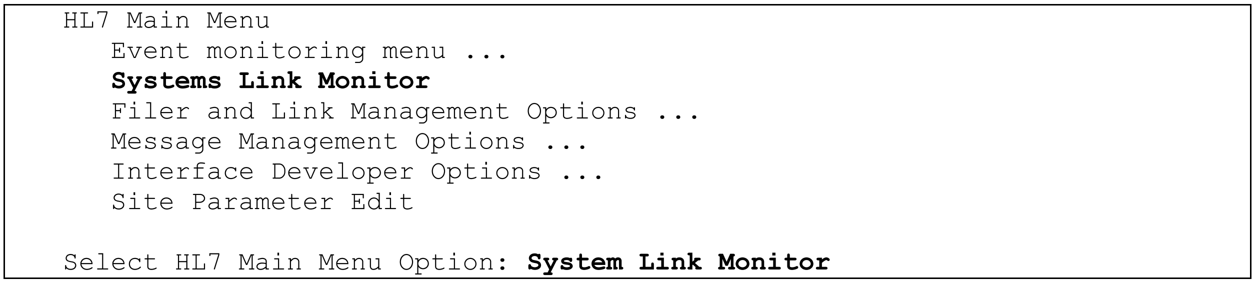
1) Before data can be transmitted over the VBECS logical links, edit the link definitions as described above.
2) To turn on the new VBECS logical links, select **START/STOP LINKS [HL START]**.
3) Start the "OERR-VBECS" logical link.
4) Start the "VBECS-OERR" logical link.
5) Start the "VBECSPTM" logical 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 52).

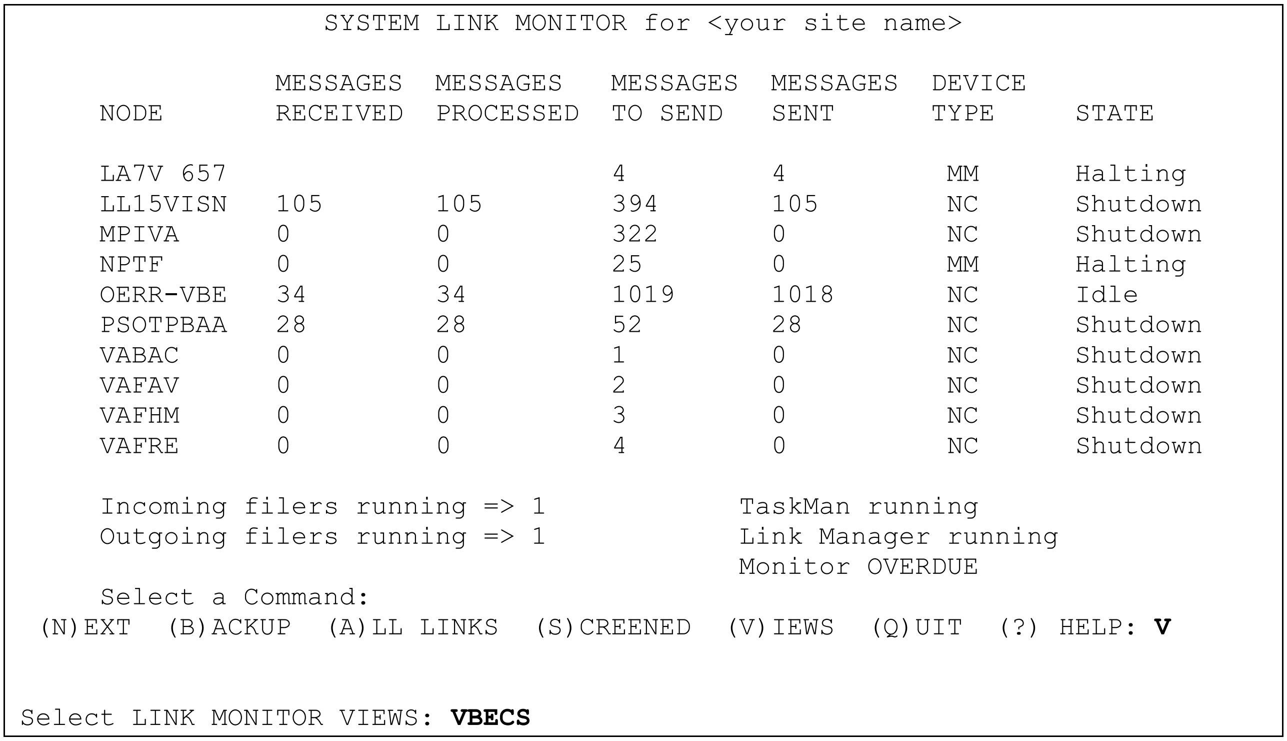
Figure 50: HL7 System Link Monitor Menu Navigation



```
   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 53).
4) At the “Select LINK MONITOR VIEWS:” prompt, enter **VBECS** (Figure 53).

Figure 51: 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 54 appears.

Figure 52: 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.

Figure 53: 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: <IP address>//    ← 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

Refer to the *VistA Blood Establishment Computer Software (VBECS) Admin User Guide.* VBECS Administrator does not allow VistALink access through e-token.

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.
- Billing Awareness is being developed concurrently and related requirements are anticipated based on initial contact with the Billing Awareness team.
- 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.

User Action	VBECS
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

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 8: Remote Procedure Calls

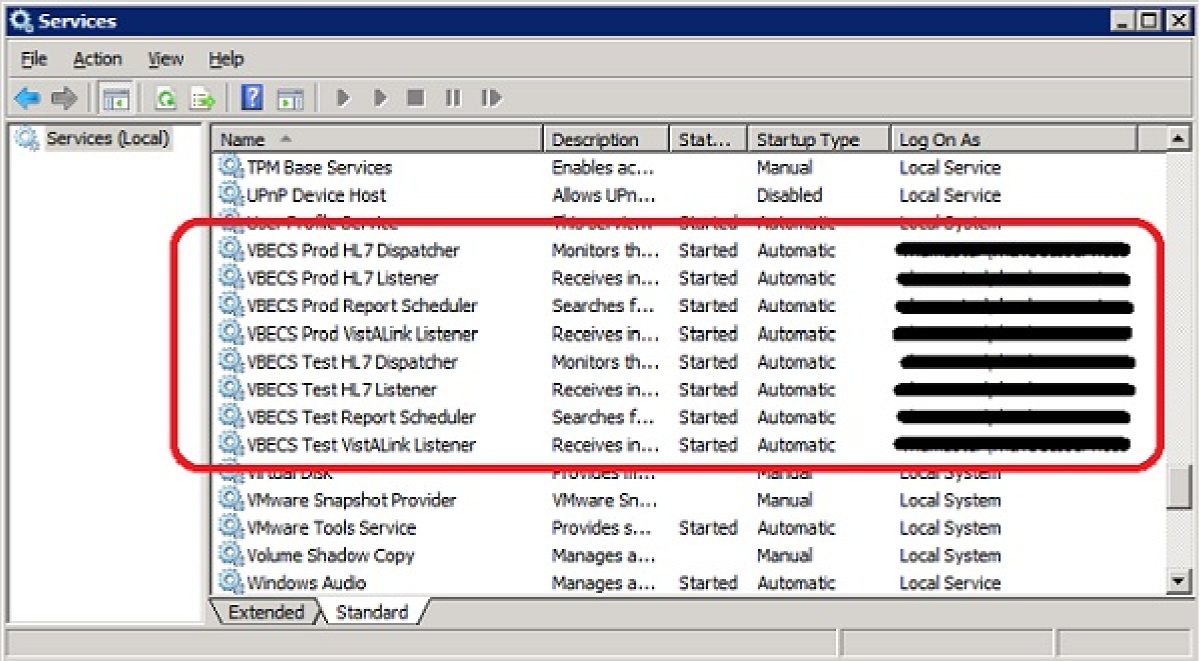
RPC Name	Database Integration Agreement (DBIA)	This RPC:
VBECS Order Entry	4619	Supports order entry of blood bank requests from the blood bank order entry dialog in CPRS
VBECS Patient Available Units	4620	Provides a list of assigned, crossmatched, autologous and directed blood units that are available 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	Updates completed workload-related data into the VBECS database after the VistA Laboratory Services package has completed workload-reporting transactions. Upon completion of the update, 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

RPC Name	Database Integration Agreement (DBIA)	This RPC:
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 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
TCPConnect	N/A	The purpose of this RPC is to establish a Broker TCP IP connection. This RPC initiates the initial connection between VBECS and the Broker. This is not yet using the token; this is an initial connection to the required Broker endpoint.
XUS SIGNON SETUP	N/A	The purpose of this RPC is to authenticate user with a Client Agent token during each application’s session. This is the IAM Sign on and Setup steps needed prior to validation.
XUS ESSO VALIDATE	N/A	The purpose of this RPC is to validate a user's token for each session. This is the IAM token validation that occurs inside VistA.
XUS GET TOKEN	N/A	The purpose of this RPC is to return a handle to a token that will sign-on a new process for subsequent RPC calls.

VBECS Windows Services

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 56 for a complete listing of VBECS services.

Figure 54: 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	[redacted]
VBECS Prod HL7 Listener	Receives in...	Started	Automatic	[redacted]
VBECS Prod Report Scheduler	Searches f...	Started	Automatic	[redacted]
VBECS Prod VistALink Listener	Receives in...	Started	Automatic	[redacted]
VBECS Test HL7 Dispatcher	Monitors th...	Started	Automatic	[redacted]
VBECS Test HL7 Listener	Receives in...	Started	Automatic	[redacted]
VBECS Test Report Scheduler	Searches f...	Started	Automatic	[redacted]
VBECS Test VistALink Listener	Receives in...	Started	Automatic	[redacted]
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 9: VBECS Windows Services

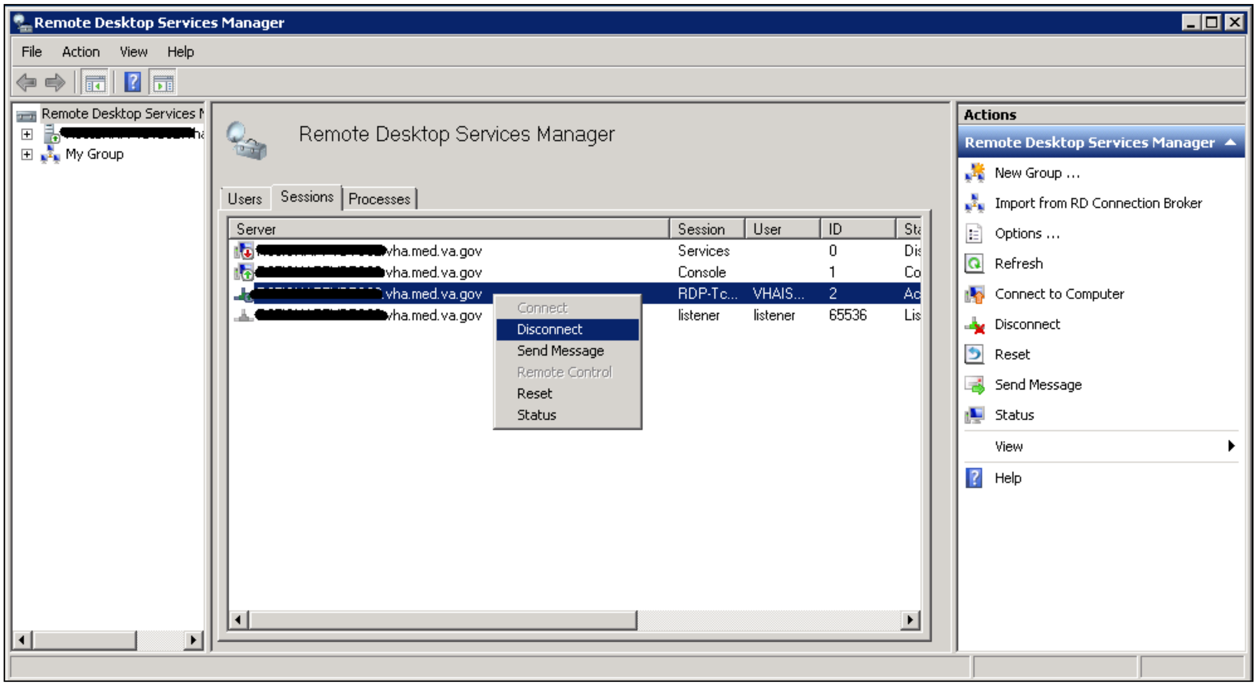
Windows Service Name	Description
VBECS Prod HL7 Dispatcher	The startup type is set to automatic. It polls the VBECS Production database for HL7 messages to be sent to CPRS in the VistA Production account.
VBECS Prod HL7 Listener	The startup type is set to automatic. This is the default HL7 listener service for all Production HL7 interfaces
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 in the VistA Test account.
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 VistA Test account applications.

Troubleshooting

Remote Desktop Session Issues

Occasionally remote desktop sessions require disconnection by a server 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 57).

Figure 55: Example of Remote Desktop Services Manager

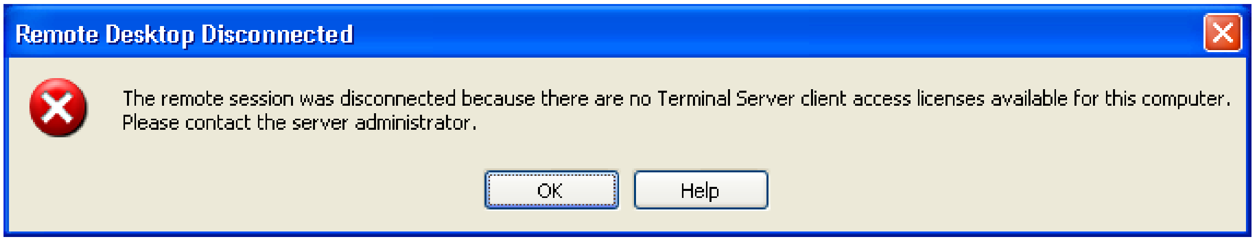


Server	Session	User	ID	Sta
[redacted]vha.med.va.gov	Services		0	Dis
[redacted]vha.med.va.gov	Console		1	Co
[redacted].vha.med.va.gov	RDP-Tc...	VHAIS...	2	Ac
[redacted]vha.med.va.gov	listener	listener	65536	Lis

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 58). 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 56: Example of Expired Remote Desktop License



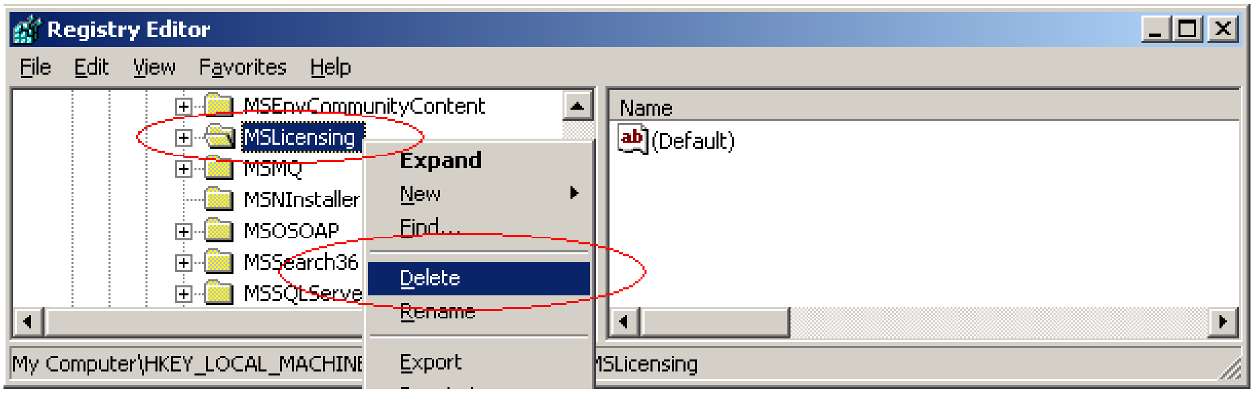
The remote session was disconnected because there are no Terminal Server client access licenses available for this computer. Please contact the server administrator.

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 58) 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 59).

Figure 57: Deleting the MSLicensing Registry Key

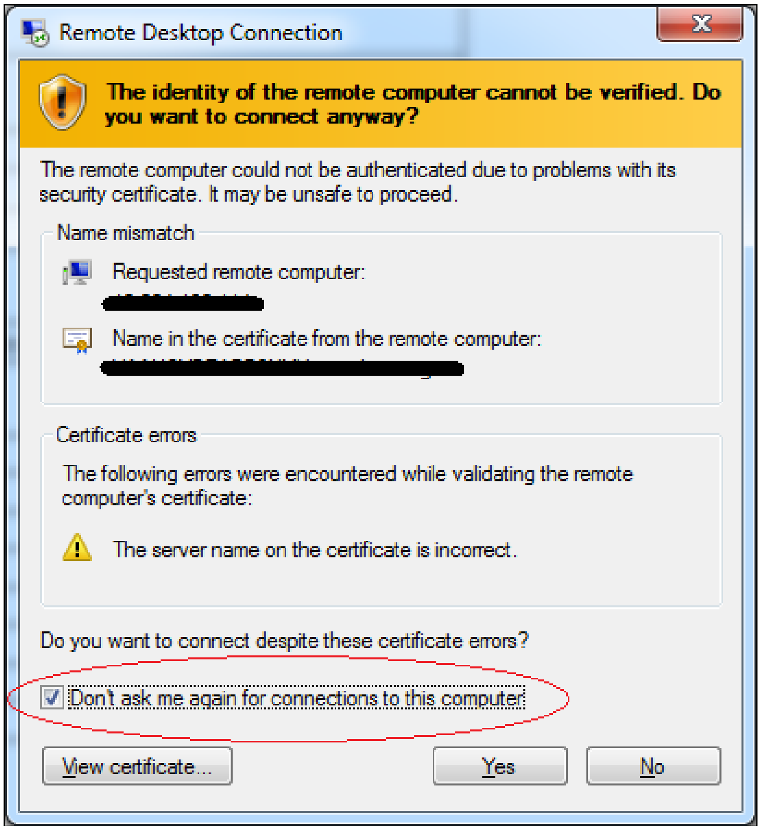


5) Make sure you are at the correct path and click **Yes** to confirm the deletion.
6) Close the Registry Editor.

Identity Verification Warning

Occasionally, a warning may appear when initiating an RDP session that states that the identity of the remote computer could not authenticated (Figure 60). This is due to an archived certificate and is not dangerous. Select **Don't ask me again**… and click **Yes**.

Figure 58: Example of Identity Warning



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Name mismatch

Requested remote computer:

[redacted]

Name in the certificate from the remote computer:

[redacted]

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The server name on the certificate is incorrect.

Do you want to connect despite these certificate errors?

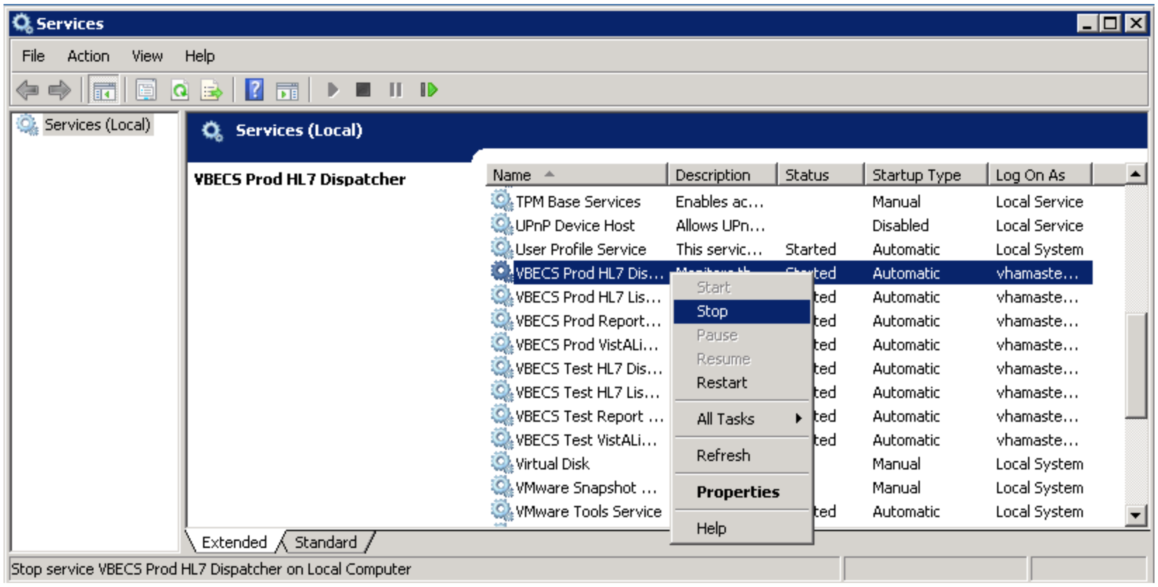
☑ Don't ask me again for connections to this computer

Stopping and Starting VBECS Services

Stopping VBECS Services

1) Click **Start, Administrative Tools, Services** (Figure 61).
2) Right-click on the service you would like to stop and click **Stop**.

Figure 59: Example of Stopping a VBECS Service



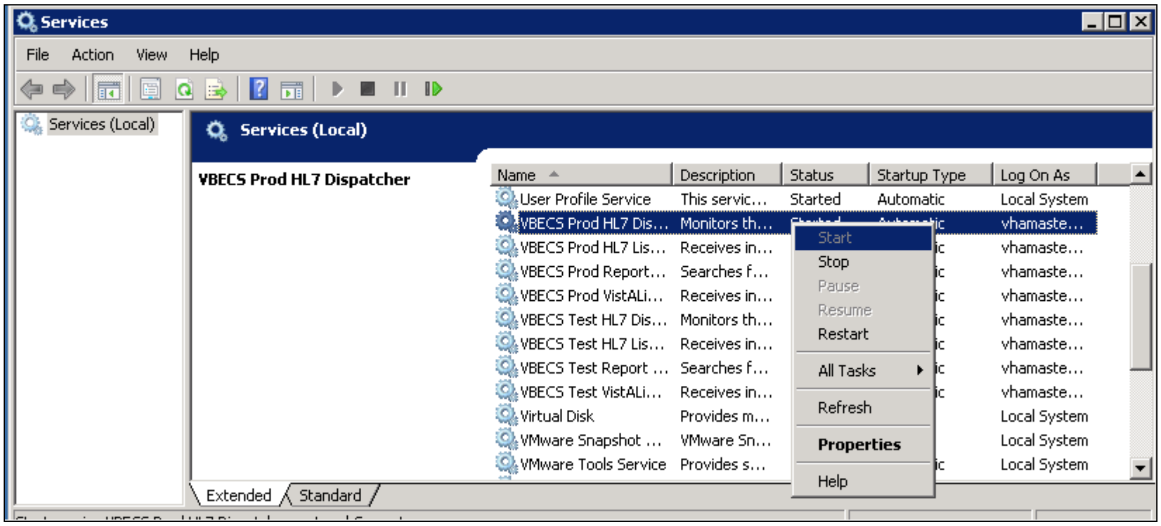
Name	Description	Status	Startup Type	Log On As
TPM Base Services	Enables ac…		Manual	Local Service
UPnP Device Host	Allows UPn…		Disabled	Local Service
User Profile Service	This servic…	Started	Automatic	Local System
VBECS Prod HL7 Dis…			Automatic	vhamaste…
VBECS Prod HL7 Lis…		ted	Automatic	vhamaste…
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 62).
2) Right-click on the service you would like to start and click **Start**

Figure 60: Example of Starting a VBECS Service



Name	Description	Status	Startup Type	Log On As
User Profile Service	This servic…	Started	Automatic	Local System
VBECS Prod HL7 Dis…	Monitors th…			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 Auditing

For a complete list of audited server events, please see: Appendix C: Auditing on VBECS Servers.

VBECS Exception Logging

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 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 Primary Contact 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 constraints, 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 10 describes the ERR codes (e.g., 203 like in the above example) descriptions.

Table 10: 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 11: VBECS HL7 Versions.
204	Unknown Key Identifier
205	Duplicate Key Identifier
206	Application Record Locked
207	Application Internal Error
208	Conflicting Processing Id

Table 11: 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
Automated Instrument	2.4

Table 12: 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 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 (Finding Application Log Entries from Email Alerts) and an email message containing the MSH segment of the rejected HL7 message.
VBECS Admin: Edit 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.

Source	Description of Problem	Possible Cause	Solution
		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 frequency (the recommended frequency is every 10 minutes) 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.
		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 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 (Finding Application Log Entries from Email Alerts) 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.

Source	Description of Problem	Possible Cause	Solution
		The HL7 message is missing patient 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.
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.
		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.

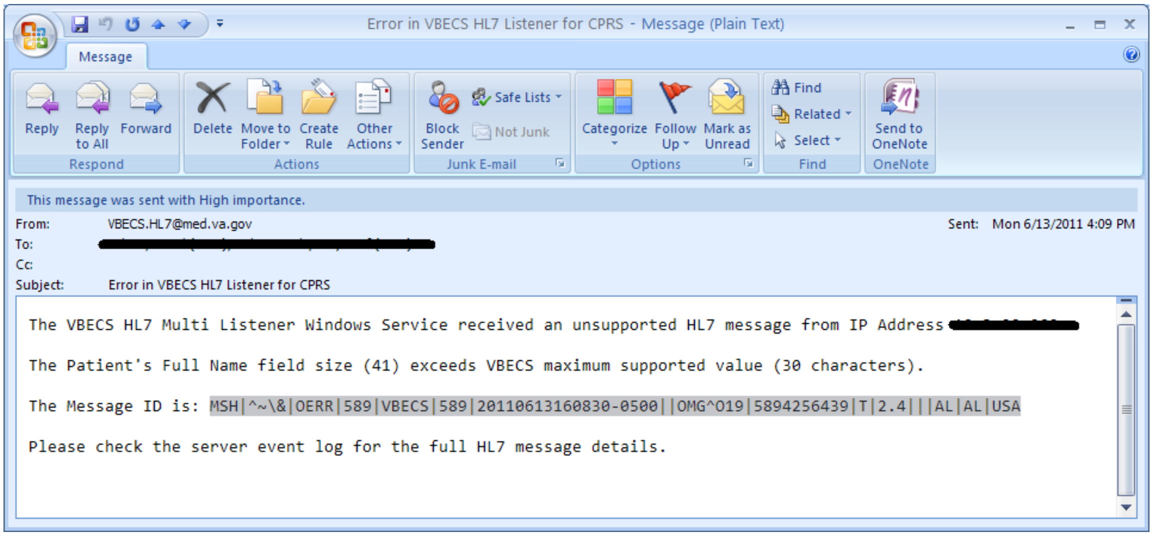
Source	Description of Problem	Possible Cause	Solution
CPRS: Blood Bank Order Dialog: Signing an Order	CPRS displays an "Error Saving Order" dialog screen with the text "The error, One or more orders to the VBECS system failed and are queued for later delivery."	An error occurred in the VBECS <Prod or 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.
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.

Source	Description of Problem	Possible Cause	Solution
Automated Instrument	Messages not being received from the instrument.	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.

Finding Application Log Entries from Email Alerts

When HL7 message patient last or first name components length(s) exceed(s) the VBECS maximum supported value of 40, an email will be received (Figure 63).

Figure 61: Example of Error in VBECS HL7 Listener for CPRS



This message was sent with High importance.

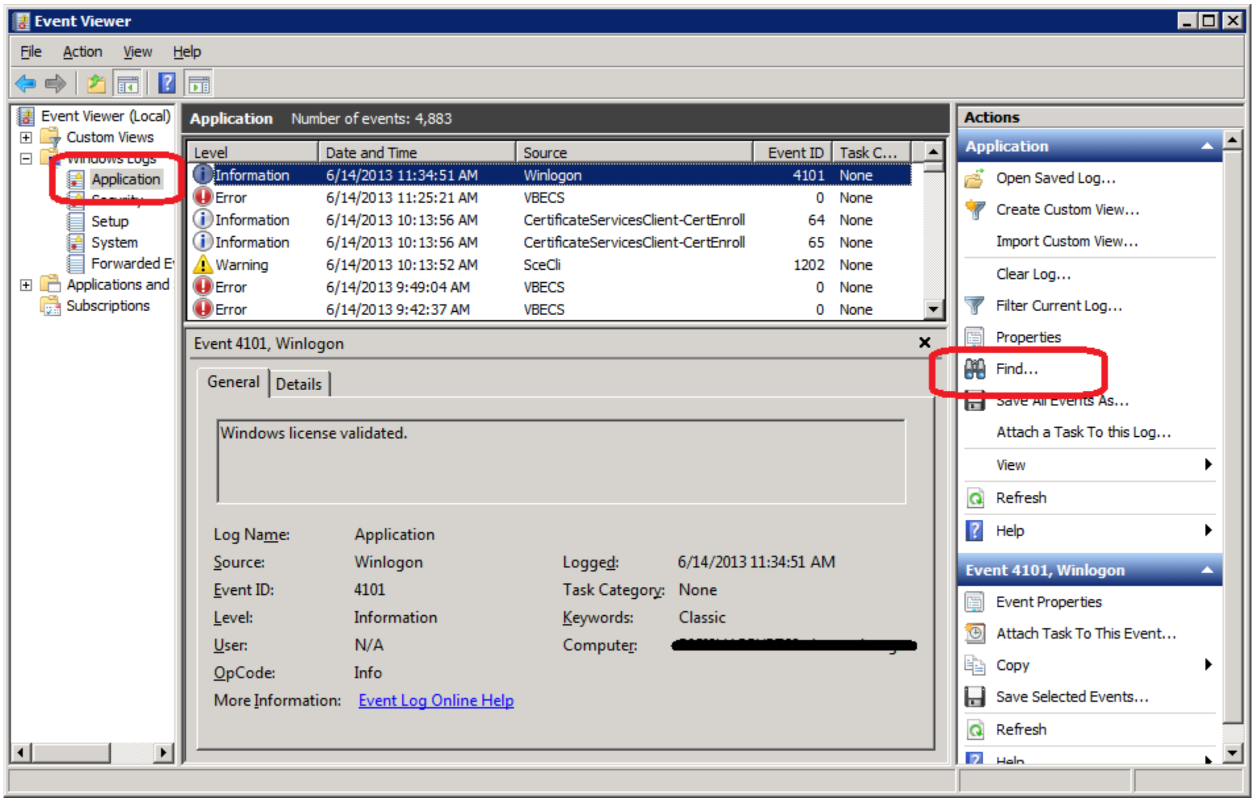
From: VBECS.HL7@med.va.gov
Sent: Mon 6/13/2011 4:09 PM
To: [redacted]
Cc:
Subject: Error in VBECS HL7 Listener for CPRS

```
The VBECS HL7 Multi Listener Windows Service received an unsupported HL7 message from IP Address [redacted]

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.
```

1) On the Application Server, click **Start, Administrative Tools, Event Viewer**.

2) 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 64).

Figure 62: 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

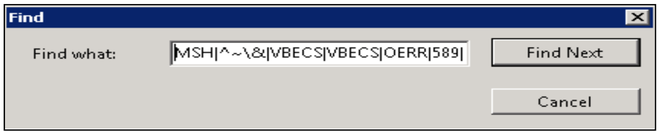
Event 4101, Winlogon

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: [redacted]
OpCode: Info
More Information: Event Log Online Help

3) Paste the **MessageID** highlighted in the email received (Figure 63) in the **Find What** text box. Click **Find Next** (Figure 65).

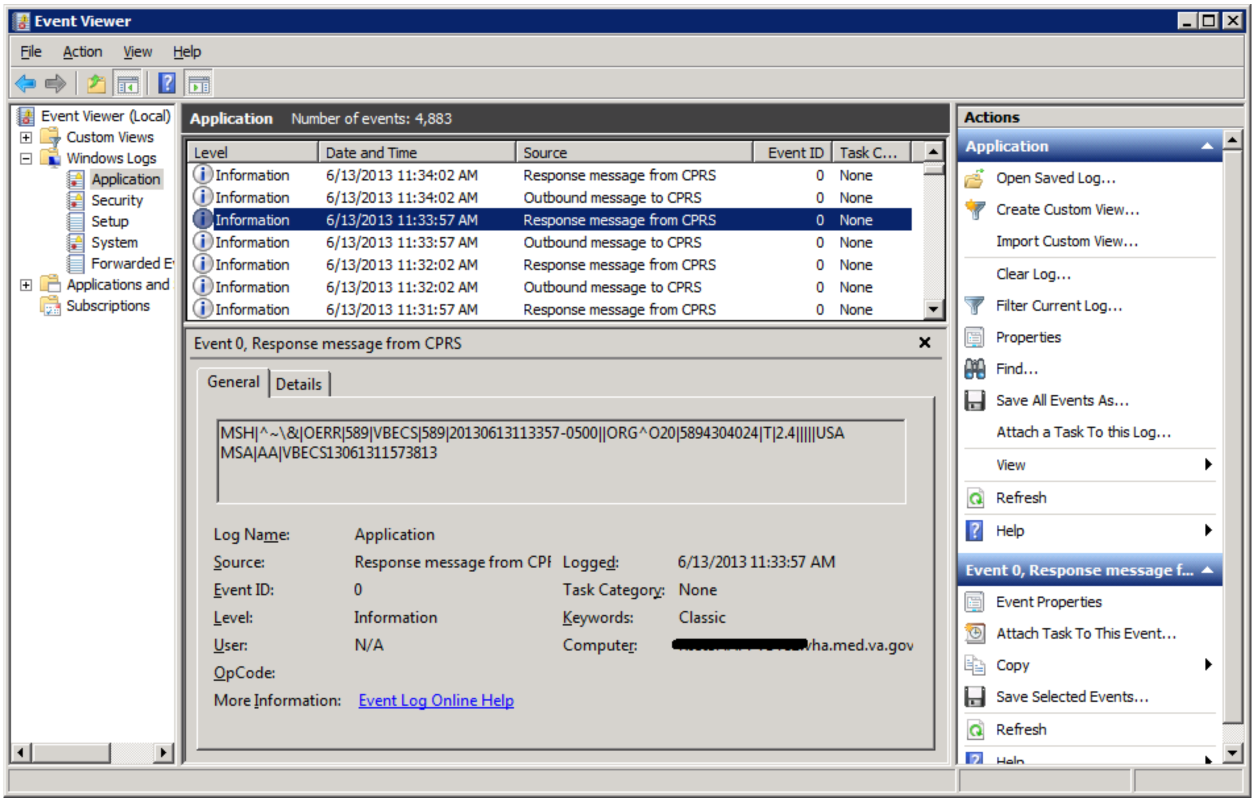
Figure 63: Example of Find in Local Application



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

4) When the event record has been found, the row will be highlighted (Figure 66).

Figure 64: 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

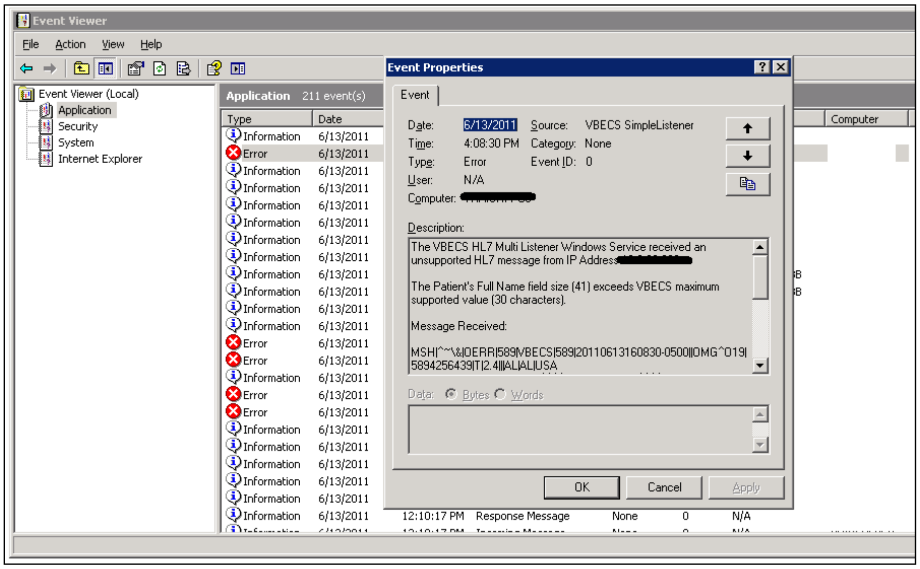
```
MSH|^~\&|OERR|589|VBECS|589|20130613113357-0500||ORG^O20|5894304024|T|2.4|||||USA
MSA|AA|VBECS13061311573813
```

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:	[redacted]ha.med.va.gov
OpCode:			
More Information:	Event Log Online Help		

5) Click **Cancel** to close the Find window (Figure 65).

6) Double-click on the highlighted row (Figure 67).

Figure 65: Example of Event Properties



Type	Date
Information	6/13/2011
Error	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Error	6/13/2011
Error	6/13/2011
Information	6/13/2011
Error	6/13/2011
Error	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011
Information	6/13/2011

12:10:17 PM Response Message None 0 N/A

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

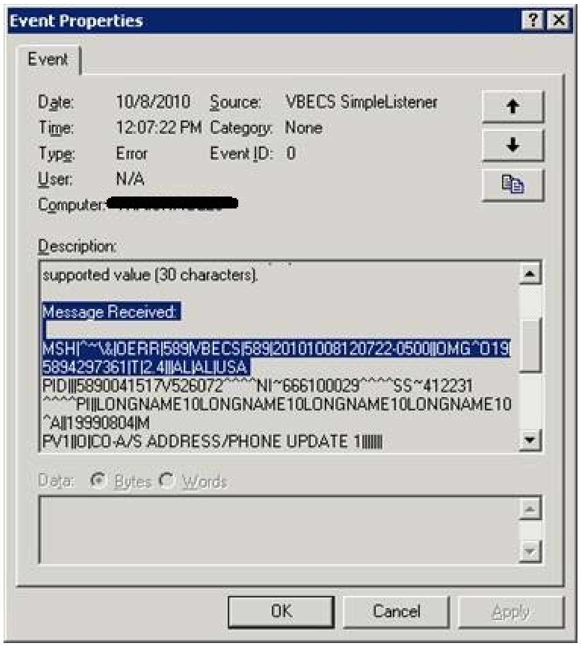
Description:

```
The VBECS HL7 Multi Listener Windows Service received an
unsupported HL7 message from IP Address[redacted]

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

7) 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 68).

Figure 66: 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: [redacted]

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

8) 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.

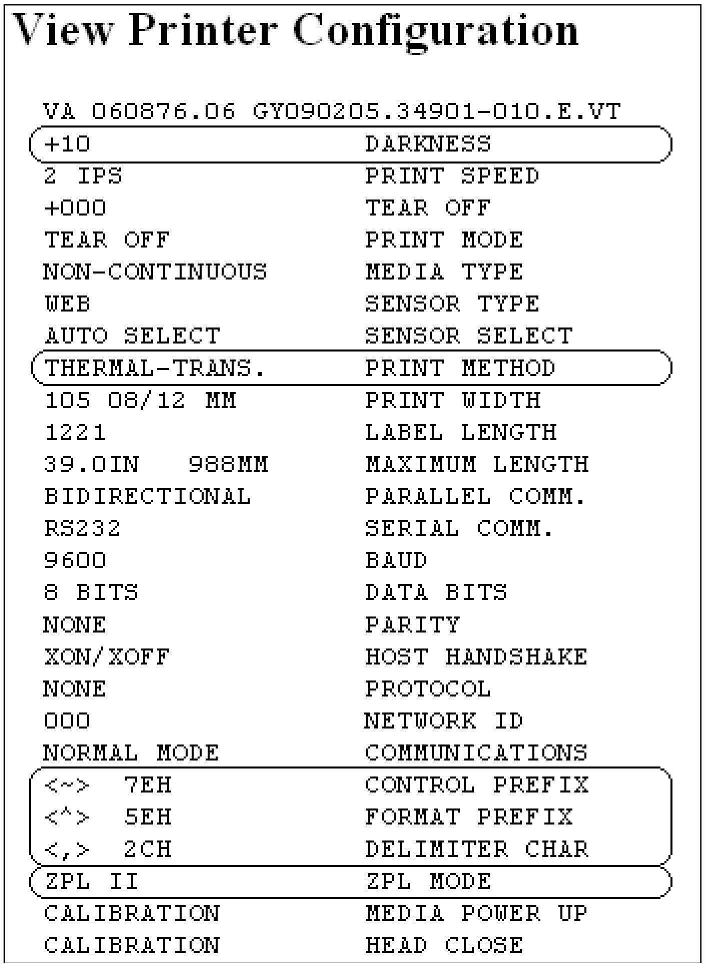
Zebra Printer Problems

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 69).

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

Figure 67: Example Zebra Printer Settings



View Printer Configuration

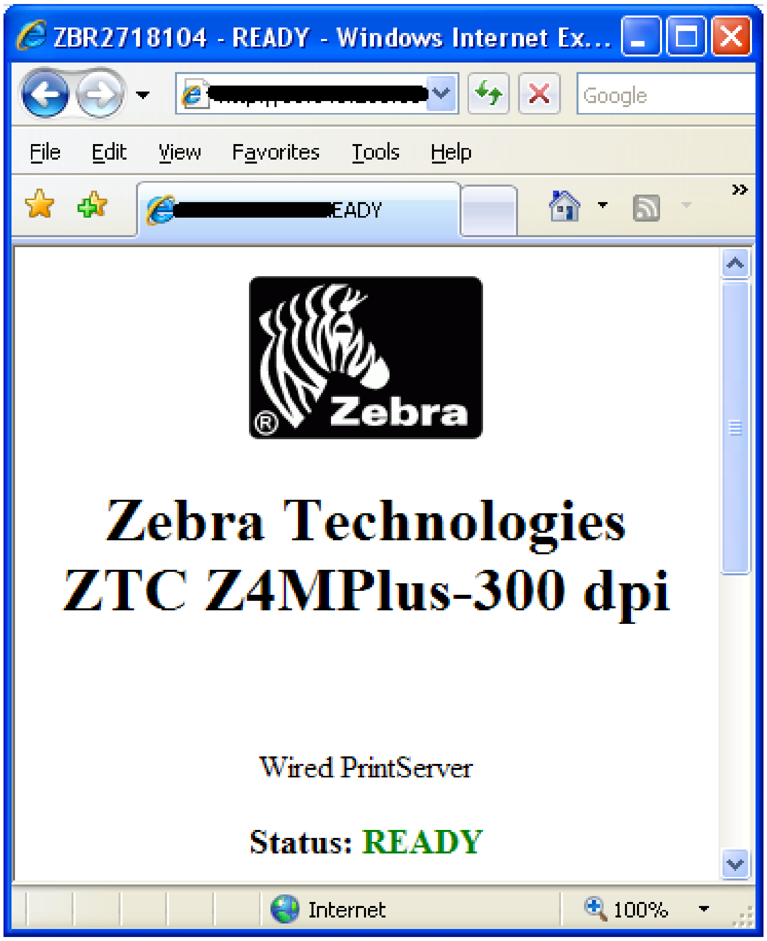
```
VA 060876.06 GY090205.34901-010.E.VT
+10                     DARKNESS
2 IPS                   PRINT SPEED
+000                    TEAR OFF
TEAR OFF                PRINT MODE
NON-CONTINUOUS          MEDIA TYPE
WEB                     SENSOR TYPE
AUTO SELECT             SENSOR SELECT
THERMAL-TRANS.          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 70).

Probable Cause: Network settings are not correct on the printer

Solution: Correct the printer's network settings. All printer manuals may be found on the VBECS SharePoint.

Figure 68: Example of Zebra Printer Web Console


ZBR2718104 - READY - Windows Internet Ex...
[redacted]
Google
File Edit View Favorites Tools Help
[redacted]EADY
Zebra
Internet
100%

Zebra Technologies
ZTC Z4MPlus-300 dpi

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.

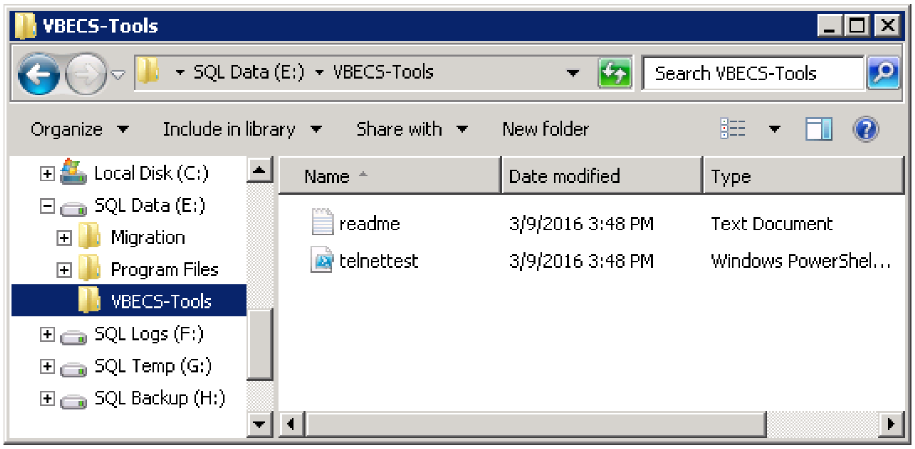
Solution: Verify that the PRINT METHOD, CONTROL PREFIX, FORMAT PREFIX, DELIMITER CHAR and ZPL MODE match the settings in Figure 69.

Problem: The printer is online and network settings have been verified (see previous), but the printer fails to print.

Probable Cause: The network is blocking the printer, most likely due to a firewall. Test with Telnet PowerShell script. You may find it on **D:\VBECS-Tools\** (App Server) (Figure 71). Read the accompanying **readme** file for instructions.

Solution: Open the firewall to the printer on port 9100.

Figure 69: Example of Telnet test setup



Name	Date modified	Type
readme	3/9/2016 3:48 PM	Text Document
telnettest	3/9/2016 3:48 PM	Windows PowerShel...

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 72 through Figure 79 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 70: 10 milliseconds

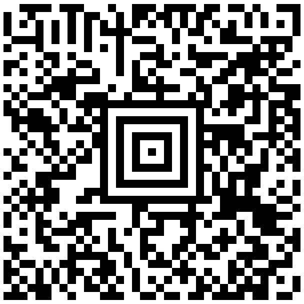


Figure 71: 20 milliseconds

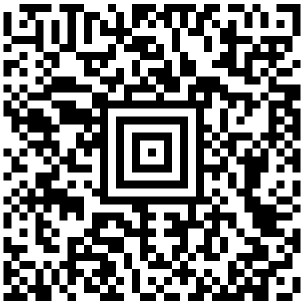


Figure 72: 30 milliseconds

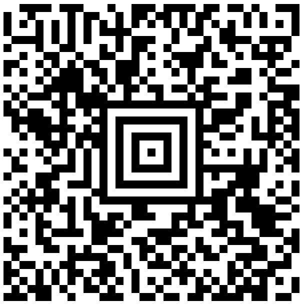


Figure 73: 40 milliseconds

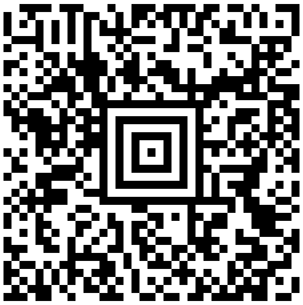


Figure 74: 50 milliseconds

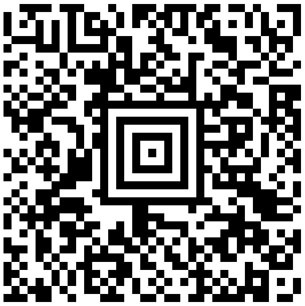


Figure 75: 60 milliseconds

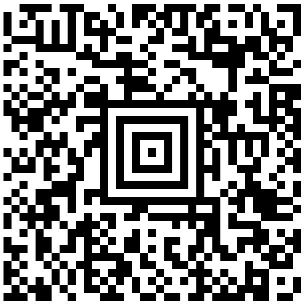


Figure 76: 70 milliseconds

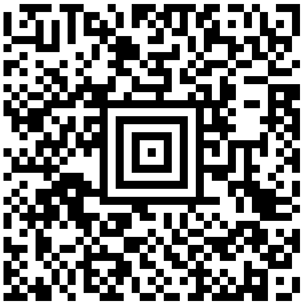
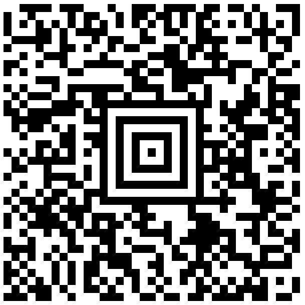


Figure 77: 80 milliseconds



This page intentionally left blank.

Archiving and Recovery (Data Center 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

See **Customer Support** section of *VBECS 2.3.1 Release Notes*.

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:

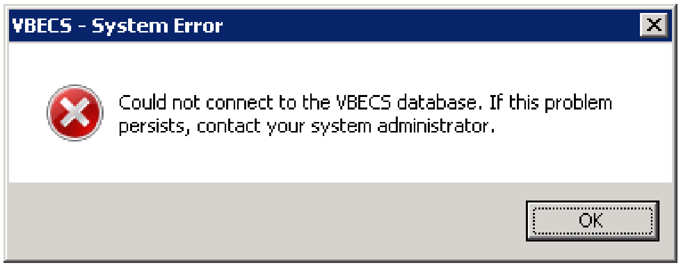
An application server can fail, or the VistA server can fail. When this connection is lost, no messages can be exchanged. When the connection between VBECS and VistA is lost due to a failure of VBECS, the messages are queued on the VistA side. Orders placed during this downtime will remain in the queue. 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 80:

Figure 78: 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 edit divisions portion of the VBECS Administrator application (refer to the *VistA Blood Establishment Computer Software (VBECS) Admin User Guide)*. 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. Contact the 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.

Access Request Process

To gain access to the VBECS server, reference the VBECS SharePoint site: (http://vaww.oed.portal.va.gov/projects/vbecs/default.aspx).

A NMEA must be used at all times to access a VBECS server with administrator access.

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.

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

Table 13: 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 14 explains the event sources that VBECS uses to write to the Application log in Event Viewer (Finding Application Log Entries from Email Alerts).

Table 14: 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	

This page intentionally left blank.

Configuring the App Server and Lab Workstations

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.

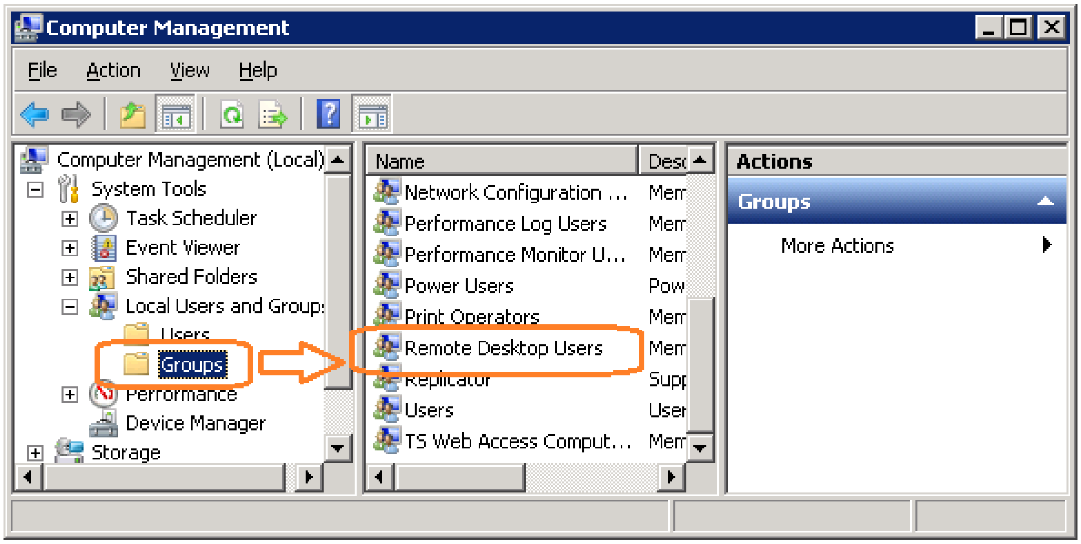
Server Tasks (Data Center Only)

Perform the following tasks on the App Server only.

Grant User Permissions

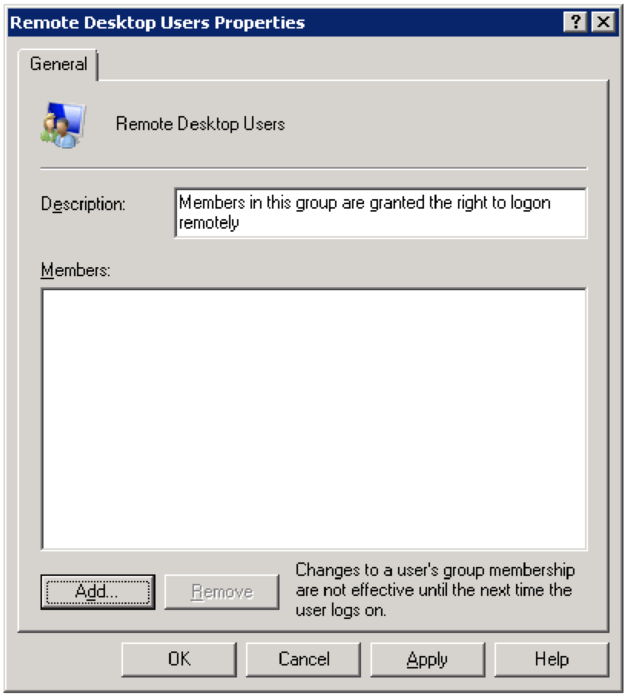
1) Open a remote desktop connection to the VBECS App Server and login with server administrator privileges.
2) Click **Start**, **Administrative Tools**, **Computer Management**. Expand **Local Users and Groups**. Select **Groups** and double-click **Remote Desktop Users** (Figure 81).

Figure 79: Computer Management



3) Click **Add** (Figure 82).

Figure 80: Remote Desktop Users Properties



Remote Desktop Users Properties

Remote Desktop Users

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

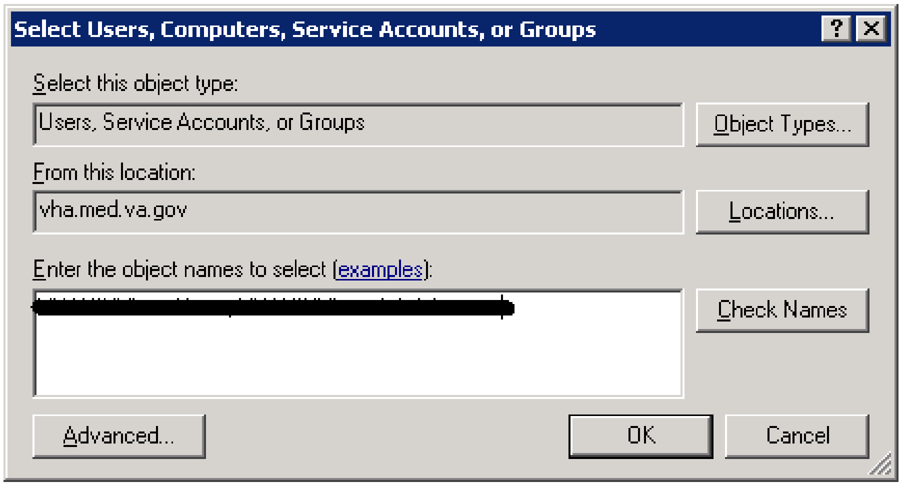
Members:

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 83). 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 81: Example of Select Users, Computers...



Select Users, Computers, Service Accounts, or Groups

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

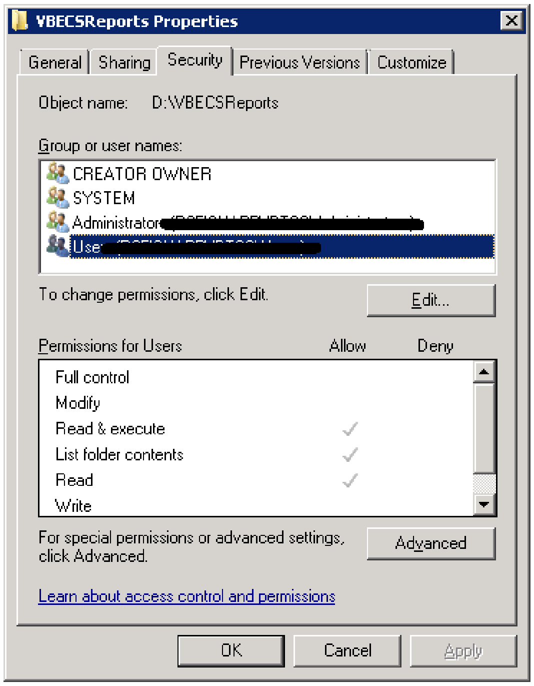
From this location: vha.med.va.gov

Enter the object names to select (examples): [redacted]

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 84).

Figure 82: Example of VBECSReports Properties



VBECSReports Properties

Object name: D:\VBECSReports

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrator [redacted]
- Use [redacted]

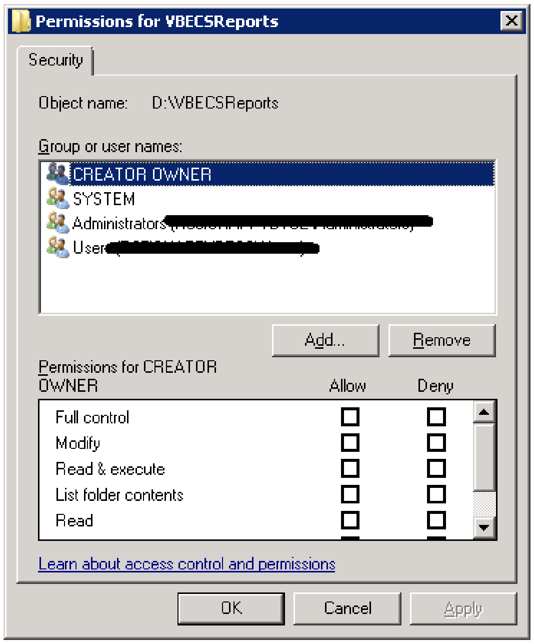
To change permissions, click Edit.

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 85).

Figure 83: 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 [redacted]
- User [redacted]

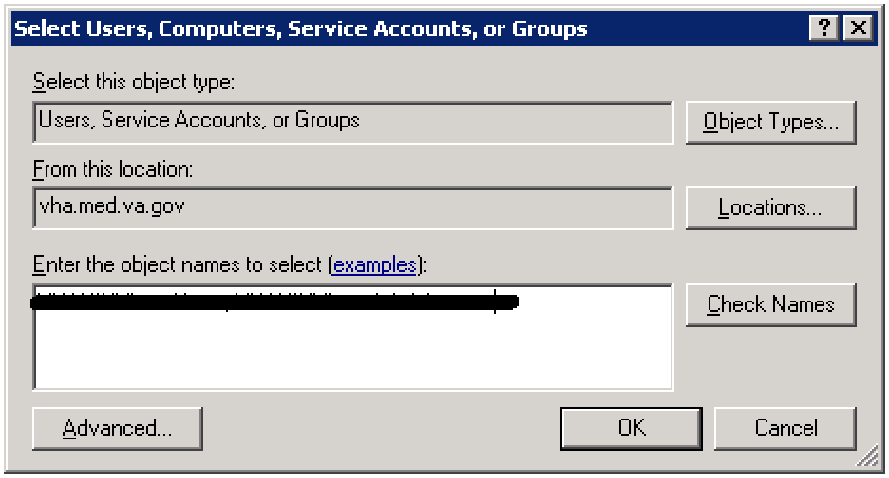
Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

5) Specify the VBECS Users and VBECS Administrators group (Figure 86). 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 84: Example of Select Users, Computers...



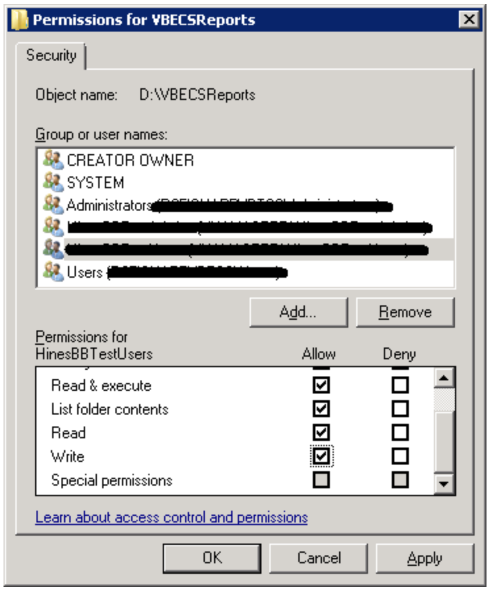
Select this object type: Users, Service Accounts, or Groups

From this location: vha.med.va.gov

Enter the object names to select (examples): [redacted]

6) In the **Permissions** window, assign **Write** access to both groups in addition to the rights granted by default. Click **OK** (Figure 87).

Figure 85: Example of Permissions


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

Object name: D:\VBECSReports

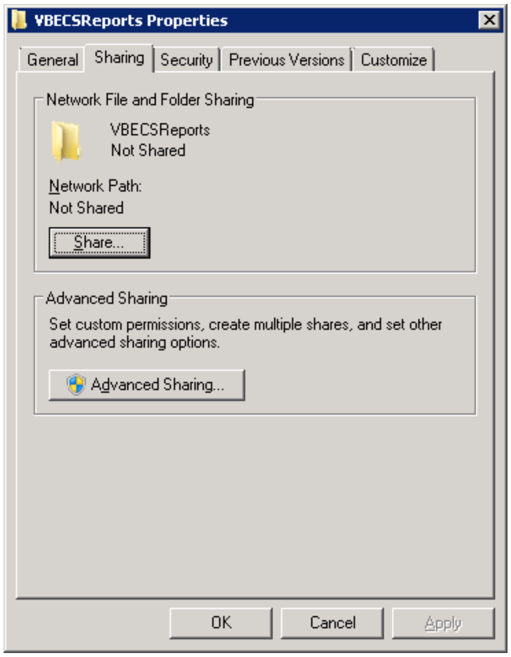
Group or user names:

CREATOR OWNER
SYSTEM
Administrators [redacted]
[redacted]
Users [redacted]

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

7) Select the **Sharing** tab and click **Advanced Sharing** (Figure 88).

Figure 86: VBECSReports Properties



Network File and Folder Sharing

VBECSReports
Not Shared

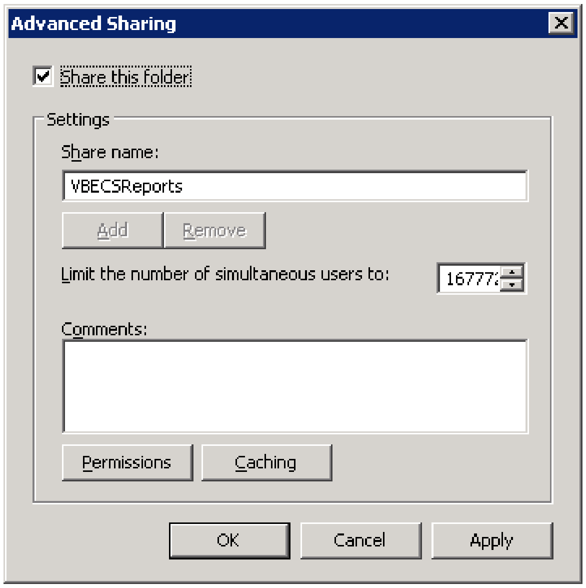
Network Path:
Not Shared

Advanced Sharing

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

8) Click **Share this folder** and then **Permissions** (Figure 89).

Figure 87: Advanced Sharing



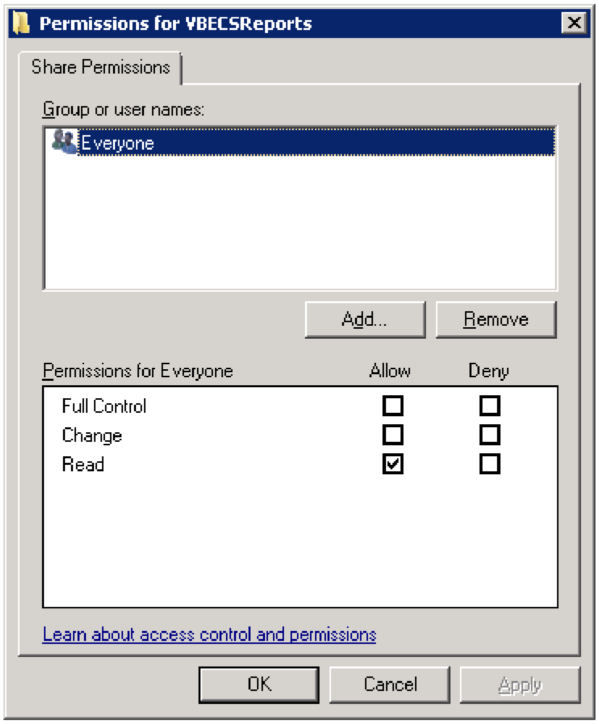
☑ Share this folder

Share name: VBECSReports

Limit the number of simultaneous users to: 16777

9) Click **Add** (Figure 90).

Figure 88: Permissions


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

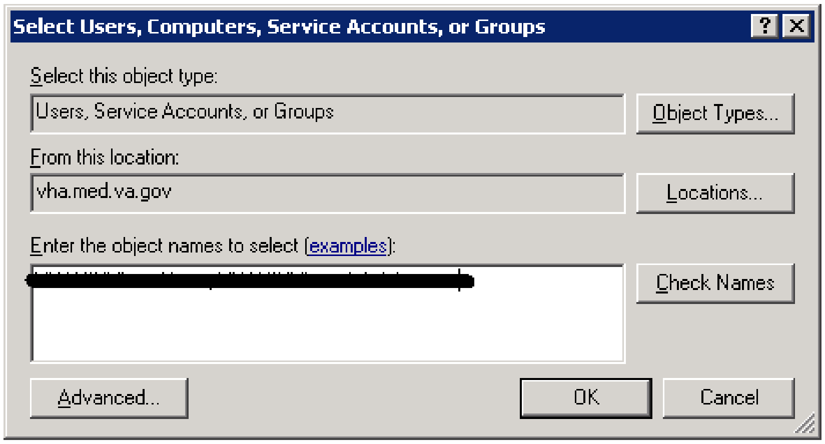
Group or user names:
Everyone

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

10) Specify the VBECS Users and VBECS Administrators group (Figure 91). Note that groups typically follow this naming convention (substitute the 3-letter site code for sss):
    - VBECS Users: *VHAsssVbecsUsers*
    - VBECS Administrators: *VHAsssVbecsAdministrators*

    Click **OK**.

Figure 89: Example of Select Users...



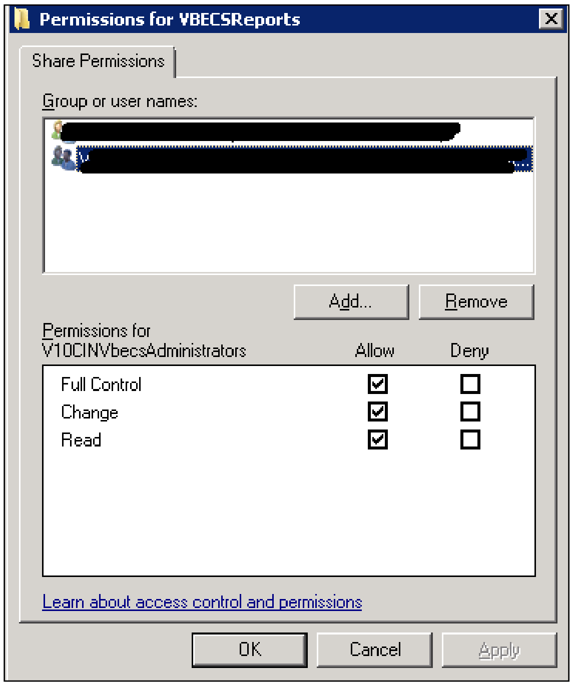
Select this object type:
Users, Service Accounts, or Groups

From this location:
vha.med.va.gov

Enter the object names to select (examples):
[redacted]

11) Select the VBECS Administrators group and select **Full Control**. Leave the default permissions for the VBECS Users group and click **OK** (Figure 92).

Figure 90: Permissions for VBECSReports



Permissions for VBECSReports

Share Permissions

Group or user names:

[redacted]

[redacted]

Add... Remove

Permissions for V10CINVbecsAdministrators	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Learn about access control and permissions

OK Cancel Apply

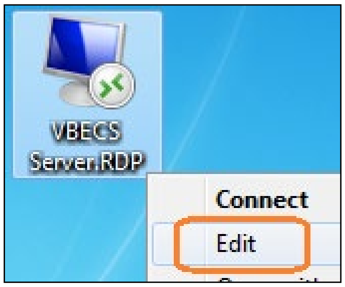
Workstation Tasks

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

Update the RDP Shortcut

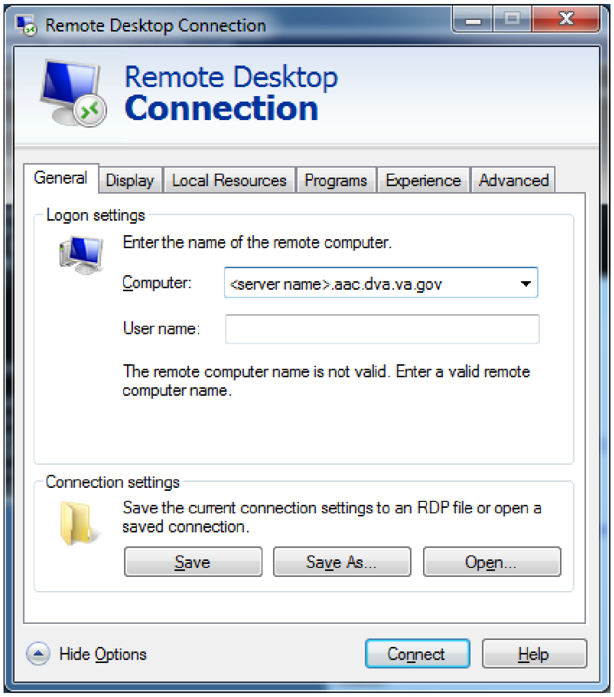
1) Log into the lab workstation with administrator privileges.
2) Right-click on the VBECs remote desktop shortcut and click **Edit** (Figure 93).

Figure 91: Edit shortcut



3) In the **Computer** field, the VBECS application server's fully qualified domain name. The name will always be your server name followed by **aac.dva.va.gov** (Figure 94). Click **Save**.

Figure 92: Remote Desktop Connection



Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: <server name>.aac.dva.va.gov

User name:

The remote computer name is not valid. Enter a valid remote computer name.

Connection settings

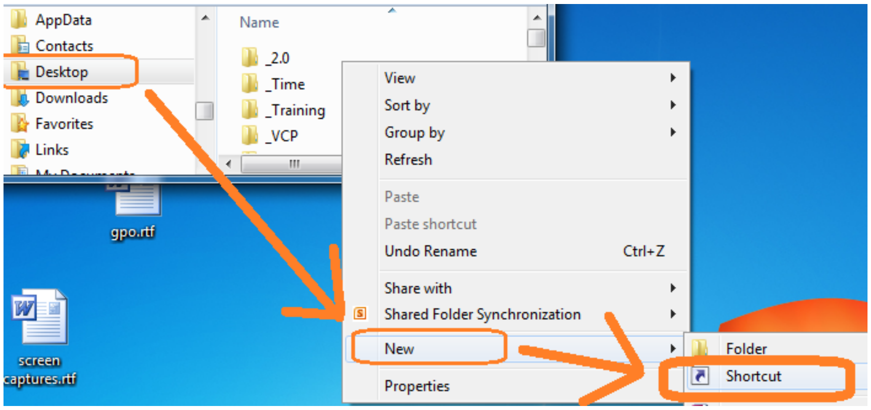
Save the current connection settings to an RDP file or open a saved connection.

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.

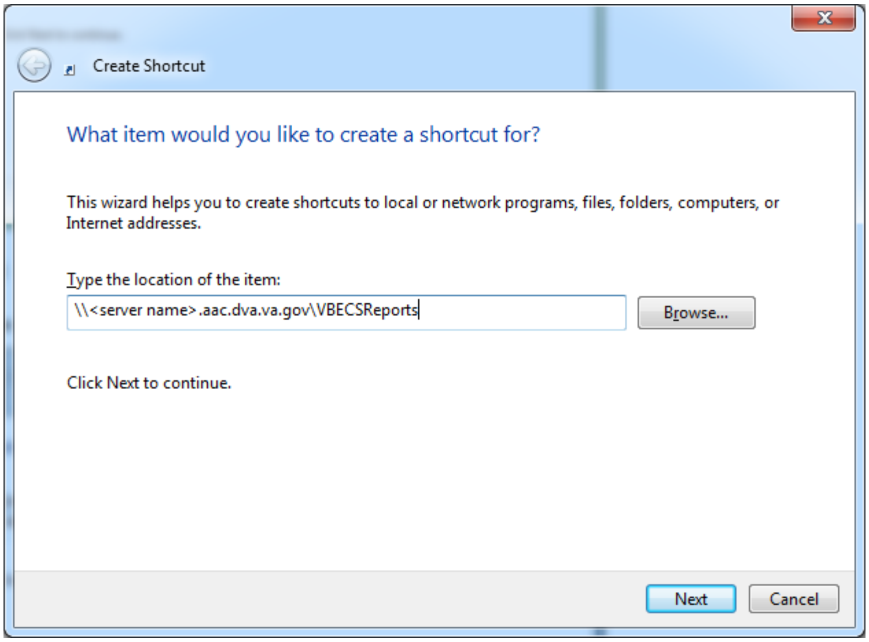
1) Log into the lab workstation with administrator privileges. Navigate to the user's desktop folder (C:\Users\Public\Public Desktop), right-click on the **Desktop** folder and select **New**, **Shortcut** (Figure 95). Note: If you cannot see the Public Desktop folder in the tree view type **C:\Users\Public\Public Desktop** in the address bar and hit enter.

Figure 93: Example of New Shortcut



2) Enter the share name (\\**<VBECS application server fully qualified domain name >\VBECSReports\Division Code**) and click **Next** (Figure 96). Division Code is the folder labeled with the site's station number. For all sites, reports are saved in subfolders named after the site's Division Code (Station Number).

Figure 94: Example of Report Share (if 518 is the Site's Station #)



What item would you like to create a shortcut for?

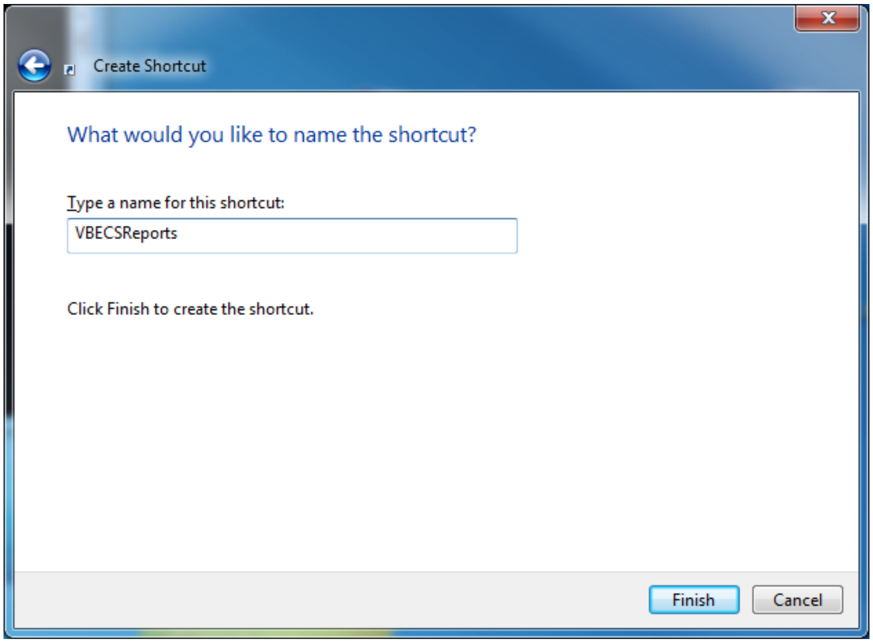
This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

Type the location of the item: \\<server name>.aac.dva.va.gov\VBECSReports

Click Next to continue.

3) Name the shortcut **VBECSReports**. Click **Finish** (Figure 97).

Figure 95: 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.
CPRS	Computerized Patient Record System.
DBIA	Database Integration Agreement.
DC	Data Center.
DR	Disaster Recovery.
DSS	Decision Support System.
DUZ	Designated User.
FQDN	Fully Qualified Domain Name.
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:

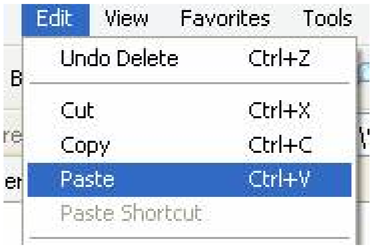
- Open a blank document (for example, in Microsoft Word) and save it as (click **File**, **Save As**) "mmddyy Technical-Security Validation Record," or another easily identified file name.

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 98**)**.

Figure 96: 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: Data Center Instructions (Data Center 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 15 and Table 16 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 15: 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 16: 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) **Shared storage**: 4 x 980GB drives*: E (Data), F (Logs), G (TempDB) and H (Backup)
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 17 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 17: 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.

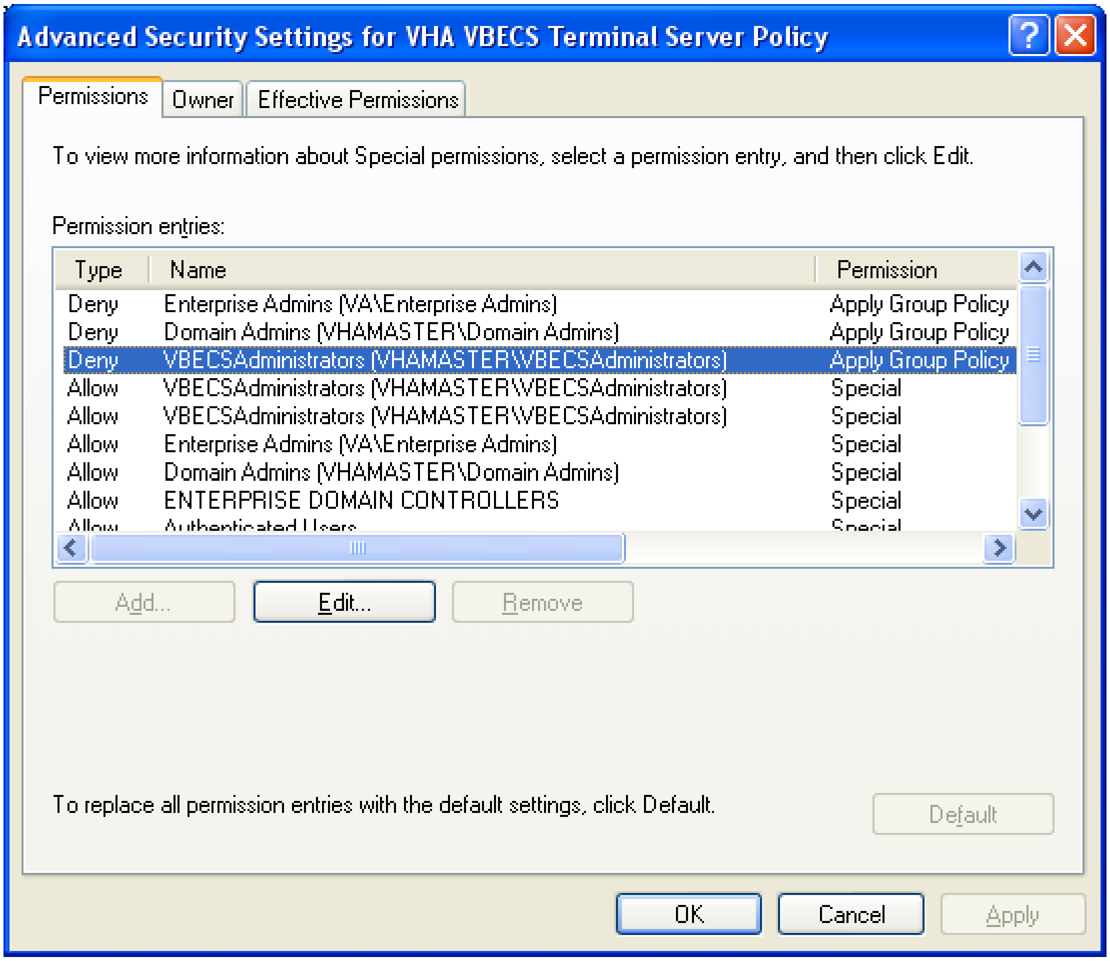
Group Policy

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 99.

Figure 97: Example of a Group Policy Not Applied to VBECSAdministrators Group



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 an 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: **<specify the VA's license server with the server's fully qualified domain name>**

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: VAITEngineeringCISIDM@va.gov.

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 Active Replica 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, DC 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 C: 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.

Index

Revision History

Date	Revision	Description	Author
3/5/19	1.0	Modified VistA Blood Establishment Computer Software (VBECS) 2.3.0 Technical Manual-Security Guide, Version 2.0 to create the VistA Blood Establishment Computer Software (VBECS) 2.3.1 Technical Manual-Security Guide, Version 1.0. Task 871370	BBM team

This is the last page of the *VistA Blood Establishment Computer Software (VBECS) 2.3.1 Technical Manual-Security Guide*.