VistA Blood Establishment Computer Software (VBECS) Version 1.6.0

Technical Manual-Security Guide

July 2012

Department of Veterans Affairs
Product Development

This page intentionally left blank.

Revision History

Date	Revision	Description	Author
		Modified VistA Blood Establishment Computer Software (VBECS) Technical Manual-Security Guide for VBECS 1.5.0.0, Version 5.0: Global: Replaced “VBECS 1.5.0.0” with “VBECS 1.6.0”. Global: Replaced “July 2010” with “September 2011”. Global: Replaced “5.0” with “1.0” in the document footer. Global: Updated figure and table numbers due to document revisions. Global: Removed all mention of our Service Monitor service since we removed it with this patch (CR 2732). Global: Removed all text associated with these services: VBECS Patient Merge HL7 Listener, VBECS Patient Update HL7 Listener and VBECS CPRS HL7 Listener. Title page: Changed “Office of Enterprise Development” to “Product Development” Introduction: Added a section “VBECS Version Numbers” explaining how the VBECS software versioning works. (TR 1298) Current Figure 9: Updated figure, and moved figure to Server Hardware and System Configuration section. Maintenance Operations section: Removed bullet list – KID bundles, LR_5.2_335 patch information and VistA data conversion is complete. Limitations and Restrictions sub-section: First bullet added VBECS to VISTALINK OCNTEXT. Released Technical Bulletins (one-time execution required) section: Added the following Technical Bulletins (DR 3847): • Updating the Printer Driver on Existing VBECS Servers (BB08-03) – revised Step 2 under Update the printer driver • VLAN Verification for MDIA Compliance (BB10-03) – Table 7 VLAN requirements: VBECSPatching row changed ports to read 20000 - 20004 • Securing Simple Network Management Protocol (SNMP) on VBECS Servers (BB10-05) VBECS Application Interface section (DR 3910): • Updated Table 10 Solution for the following: VBECS:-Order Alerts and Pending Orders, Patient Update Alerts and Patient Merge Alerts. • Added section Example of How to Find Patient Information Causing Error from the HL7 Message in the Event log Given the MSG Segment (ID). SQL maintenance Jobs (CR 2808): Updated Table 6: • Job Name - changed WeeklyIntegrityChecks to DailyIntegrityChecks. • Description - Revised description for Copy VBECS DB Backup Files to L Drive and L Drive Delete old Backup files • Added new job ExpireTestOrders for the VBECS_V1_PROD and VBECS_V1_TEST databases (CR 2368) • Revised Frequency and Time (local time) job runs for ResetServerLogFile job name. SQL Database Jobs Alerts section: • Revised section (CR 2808). • Added the designated recipients for the alerts is the email group specified in the Interface Failure Alert Recipient section of the CPRS Interface (CR 2732).	

Date	Revision	Description	Author
07-06-11	1.0	• Replaced Figure 29 Periodic System Maintenance section: Added warning box stating not to reboot server during the scheduled time interval for the VBECS SQL Maintenance jobs. (DR 4128) Table 5: Changed to show that Review Database Integrity Reports run daily. Configure Interfaces section: • Updated Figures 72, 73, 74, 75 and 76 to show the addition of the BCE COTS interface. • Added Configure BCE COTS Interface Parameters section. • Added note regarding the enable/disable of the BCE interface and the need to restart our service. (DR 4083) • Configure BCE COTS Interface Parameters section Step 8, added camera icon. External Interfaces: • Revised 2nd paragraph and deleted 4th paragraph • VistA Patient Merges- removed "The user must update the patient record manually to match the VistA record" from the paragraph. Troubleshooting section: • Added Remote Desktop Configuration. (DR 3841) • Revised Stopping and Starting VBECS Services by removing Test from heading and removing the paragraph. • Revised Step 5 (Stopping and Stopping VBECS Services) . • Revised Step 1 under Verify NIC Card Configuration. • Revised Step 21 and combined Steps 22 and 23 under Verify NIC Card Configuration. • Added new Steps 23 through 29 under Verify NIC Card Configuration and renumbered subsequent steps. • Removed Restarting VBECS Services section. • Removed VistA Query Timeout section. • Added VLAN ACL Network Connectivity Issues section and steps to add the VBECS FTP site to the Trusted Sites in Internet Explorer. Updated Figure VLAN Schematic . VBECS Build Version Numbers section: Removed, since this is documented in VBECS Version Numbers section. Replaced Figures 40, 41, 42, 60, 62, 63, 64,118 and 137. VBECS Windows Services: First Paragraph, replaced reference to Table 8 with Figure 118. VBECS Exception Workarounds: Revised paragraph. Glossary: Revised the definition for RPC. Table 13 VBECS Communication Requirements: Revised the IP address section for SMTP Support.	BBM Team
		Modified VistA Blood Establishment Computer Software (VBECS) 1.6.0 Technical Manual-Security Guide, Version 1.0: Global: Replaced "September 2011" with "October 2011". Global: Replaced "1.0" with "2.0" in the document footer. Figure 1: Updated. Implementation and Maintenance: - Table 5, 3rd row, Description cell, 1st sentence – Change "is sent" to "and an email alert is sent" - Changed "SQL Database Job Alerts" to" SQL Maintenance Job Alerts" and revised the section - Revised Windows Updates section (DR 4290) - Backup Exec Alerts section, Configure Backup Exec Alerts	

Date	Revision	Description	Author
10-27-11	2.0	subsection – Change bullets to steps Maintenance Operations: Configure Interfaces section: - Global revised steps to configure the Interface Failure Alert Recipient group parameter and added a note (DR 4245) Released Technical Bulletin (One time Execution Required): - Replaced previously released VLAN Verification for MDIA Compliance (BB10-03) with VLAN Updates (BB11-05) External Interface: - Added Purging the HL7 Message Log section (DR 4137) Reconfiguring the VBECS HL7 Multi Listener and VistALink Services: - Updated VBECS HL7 Multi Listener Service configuration example - Updated VBECS VistALink Service configuration example Glossary: Changed the definition for VDL. Appendix C: Reworded. Appendix I: Added this as a new appendix and moved the VBECS Communications Requirements table from Appendix E to Appendix I deleting the duplicated rows that existed between the 2 tables.	BBM Team
		Modified VistA Blood Establishment Computer Software (VBECS) 1.6.0 Technical Manual-Security Guide, Version 2.0: Global: Replaced “October 2011” with “March 2012”. Global: Replaced “2.0” with “3.0” in the document footer. Global: Replaced “MOM” with “SCOM” (SCOM is an equivalent replacement for MOM) (DR 4333). Global: Added “Example of” to figure captions where applicable. Global: Updated to accommodate Windows 7. Globally changed “server 1” to “cluster node 1” and “server node” to “cluster node”. VBECS Version Numbers: Updated to match Figure 1. Related Manuals and Reference Materials – added the following: • VistA CPRS- Order Update - CPRS OERR 2.4 • VistA PIMS Patient ADT Update - VAFC ADT 2.3 • VistA MPI/PD PatientMerge - MPI TRIGGER 2.4 • BCE COTS Patient Blood Product Transfusion Verification 2.5 Table 2- Revised description for Zebra printer. Table 3- Revised description for Processor, Memory and Operating System. Table 4- Revised description for .NET Framework and McAfee VirusScan. Table 5- Added Virus updates to the Action column of Windows updates. Table 6- Revised description of ExpireTestOrders and added rows for the following Job Name: - ShrinkLog - UpdateStats - TruncateDataFiles SQL Maintenance Jobs section: - Revised SQL Maintenance Job Alerts subsection - Revised VBECS Database Integrity Check Job Alerts subsection - Deleted figure (Example of Database Integrity Report with Errors) Backup Archiving Jobs section: Added. Windows Updates: Revised Step 5. Commonly Used System Rules: Revised 1st bullet.	

Date	Revision	Description	Author
		Deleted HP Array Diagnostic Utility section. Systems Shut Down and Restart Instructions section: Deleted extra figure (Example of Shut Down Window). Added warning box about ACL in the following sections: - Printers - Configure Interfaces - Zebra Printers Configure Interfaces section: - Added steps to open the interface for CPRS, PatientUpdate, PatientMerge and BCE COTS. - Deleted Internet message format RFC 2822 and added an example of email address. - Added warning box in Configuring BCE COTS interface section. Configure VistALink Parameters: Added new Steps 1 and 2 and revised Step 7. Configure CPRS HL7 Interface Parameters: Added new Steps 1, 2 and 6. Revised Steps 9 and 11. Configure Patient Update HL7 Interface Parameters: Added new Steps 1 and 2. Revised Steps 8 and 10. Configure Patient Merge HL7 Interface Parameters: Added new Steps 1 and 2. Revised Steps 8 and 10. Configure BCE COTS Interface Parameters: Added new Steps 1 and 2. Revised Steps 5, 9 and 11. Configure Users: Under Assumptions, added 2nd bullet and revised the 7th bullet. External Interfaces: Deleted the following subsections: - Introductory Summary (3 paragraphs). - Healthy Level Seven Interfaces - Client Server - Transport Layers and Lower Layer Protocols - TCP Client(Sender) - TCP Server(Listener) - Computerized Patient Record System - VistA Patient Updates - VistA Patient Merges VBECS Exception Workarounds: Revised1st paragraph. Released Technical Bulletins (one-time execution required): - Removed VLAN Updates (BB11-05) with VLAN Updates (BB11-06) section but kept Appendix H. - Updating the Printer Driver on Existing VBECS Servers (BB10-01): Revised. External Interfaces section: Revised. Troubleshooting section: - Changed name of “Remote Desktop Configuration” subsection to “Remote Desktop Licensing Issues” and revised. - Added “Deleting the Terminal Services Licensing Information on a VBECS Workstation” subsection. - Verify NIC Card Configuration: Revised Steps 1, 6, 7, 11, 16, 23 and 25. - VBECS Exception Logging: Revised Step 2. - Revised Table 9. - Cluster Connectivity Lost: Updated Solution Step 1. - Zebra Printer Problems: Added ACL warning box. - Scanner Problems: Revised section. Renamed “Example of How to Find Patient Information Causing Error from the HL7 Message in the Event Log Given the MSG Segment (ID)”	

Date	Revision	Description	Author
03-01-12	3.0	section as “Finding Application Log Entries from Email Alerts”. Renamed “VLAN ACL Network Connectivity Issues” section as “VBECS FTP Download Issues”. Restore the Databases section: Updated VA Service Desk Alternate Contacts. Notify VBECS Central Administrator section: Removed. Systems Center Operations Manger: Added note. Glossary: Added ACL and SCOM. Appendix C: Added Web site link. Deleted Appendix F: Database Conversion Updates and updated the document to reflect the change. Appendix H: - Added 137, 139 and 445 to Terminal Services license server’s ports. - Added IP address 10.3.9.181 to Servers (VBECS Development Support…… and FTP). - SMTP: Deleted the following IP addresses (10.3.27.92, 10.208.13.3, 10.252.93.8, 10.252.94.8, 10.252.95.8).	BBM Team
05-01-12	4.0	Modified VistA Blood Establishment Computer Software (VBECS) 1.6.0 Technical Manual-Security Guide, Version 3.0: Global: Replaced “March 2012” with “May 2012”. Global: Replaced “3.0” with “4.0” in the document footer. Global: Changed “10.3.21.76” to “10.3.9.181”. Updated Figure 160. Appendix H: Updated Table 13: VLAN Requirements per Technical Bulletin BB12-03.	BBM Team
07-20-12	5.0	Modified VistA Blood Establishment Computer Software (VBECS) 1.6.0 Technical Manual-Security Guide, Version 4.0: Global: Replaced “May 2012” with “July 2012”. Global: Replaced “4.0” with “5.0” in the document footer. Global: Updated all IP addresses with new VM based servers. Server Configuration: Deleted the caution box that mentioned filing a Remedy ticket for LAN speed. Label Printer: Added a caution box warning users not to install Zebra printer on server. Windows Updates: Deleted the detailed step-by-step instructions. Troubleshooting: Added a section that describes the hardware section of the VBECS SharePoint site. Added a description for the new scanner fix involving local keyboard settings. Table 9: Updated the Description of Problem, Probable Cause and Solution in the last row of the table to better describe the issue. Appendix F: Updates services list.	BBM Team

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Introduction

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

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

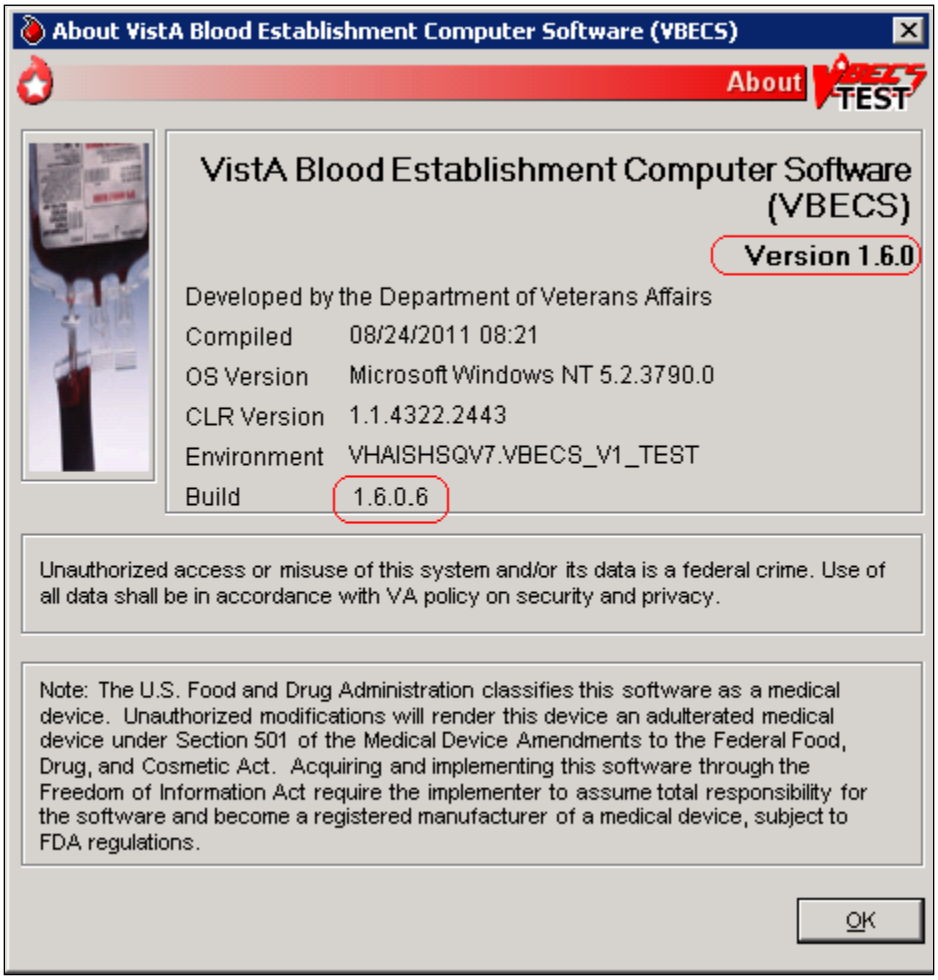
Do not change the system! The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and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

Changes to the system configuration must be documented with screen captures and kept with the installation record.

VBECS Version Numbers

In earlier VBECS patch releases, the user documentation referred to the VBECS version in a 4-digit format (e.g., 1.6.0.6 – where 1.6.0 represents the patch version and 6 is the patch build number). The build number is used by VBECS Product Support for diagnostic and troubleshooting purposes.
The VBECS version will be represented with only the first 3 digits (e.g., 1.6.0) and will appear that way in all user documentation to simplify readability. The full 4-digit version can still be found under the **Help**, **About VBECS** window in VBECS (Figure 1) and will appear in patch installation guides where build specific files are referenced.

Figure 1: Example of Help, About VBECS



Related Manuals and Reference Materials

- *Health Level Seven Implementation Support Guide for HL7 Standard Version 2.3.1*, Message & Interface Services (M&IS), VHA OI - Health Systems Design & Development Web site (©1999).
- *VistA CPRS- Order Update - CPRS OERR 2.4.*
- *VistA PIMS Patient ADT Update - VAFC ADT 2.3.*
- *VistA MPI/PD PatientMerge - MPI TRIGGER 2.4.*
- *BCE COTS Patient Blood Product Transfusion Verification 2.5.*
- *Kernel Systems Manual Version 8.0*, Chapter 1: Sign-On Security/User Interface, pp. 13–20.
- "Locking Down Windows Server 2003 Terminal Server Sessions," Microsoft Web site (October 29, 2003).
- *National Software Package Distribution*, SOP 196-5.
- *Release of Patches*, SOP 196-8.
- *VBECS Application Interfacing Support Software Installation and User Configuration Guide.*
- *VistA Blood Establishment Computer Software (VBECS) Installation Guide.*
- *VistA Blood Establishment Computer Software (VBECS) User Guide.*

- *VistALink Version 1.0 Developer-System Manager Manual*, Chapter 6: Security Management, pp. 34–35.
- *Windows Server 2003 Security Guide 2.1*, Microsoft Corporation (May 8, 2006).

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.

Appendices

The appendices contain truth tables and other materials for reference.

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

This page intentionally left blank.

Remote Desktop Configuration

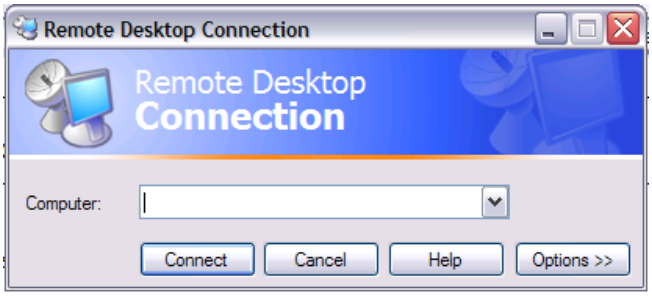
Configure the screen resolution, sound, and connection speed, and create a Remote Desktop Connection shortcut on each VBECS workstation.

Screen Resolution

To set the screen resolution:

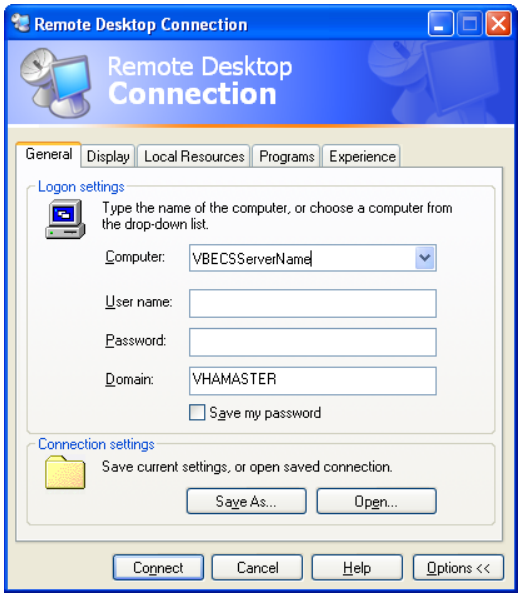
1) Double-click  (the **Remote Desktop Connection** icon).
2) Click **Options** (Figure 2).

Figure 2: Example of Remote Desktop Connection Options



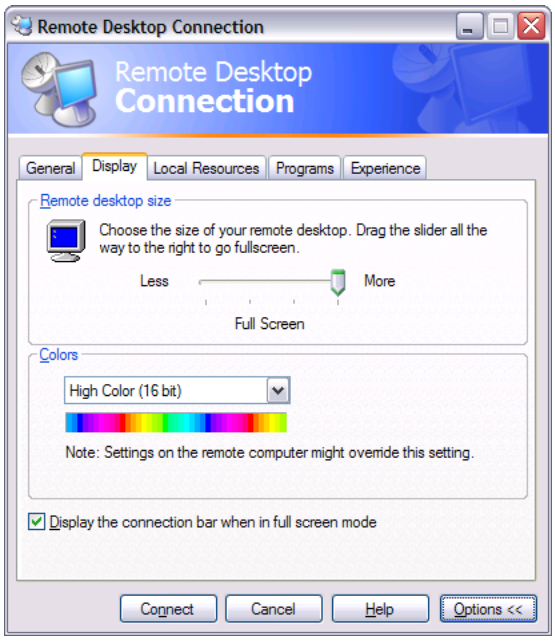
3) Click the **General** tab (Figure 3).
4) Enter the VBECS server cluster name or cluster IP address in the Computer field. Enter **your Domain** (e.g. VHAMASTER) in the Domain field. Do not enter a user name or password.

Figure 3: Example of General Tab: Computer and Domain



5) Click the **Display** tab (Figure 4).
6) Click, hold, and slide the pointer to a screen resolution of Full Screen.

Figure 4: Example of Display Tab



7) Click on the **General** tab.

Sound

To enable sound:

1) Click the **Local Resources** tab (Figure 5).
2) Select **Bring to this computer** from the Remote computer sound drop-down list.

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

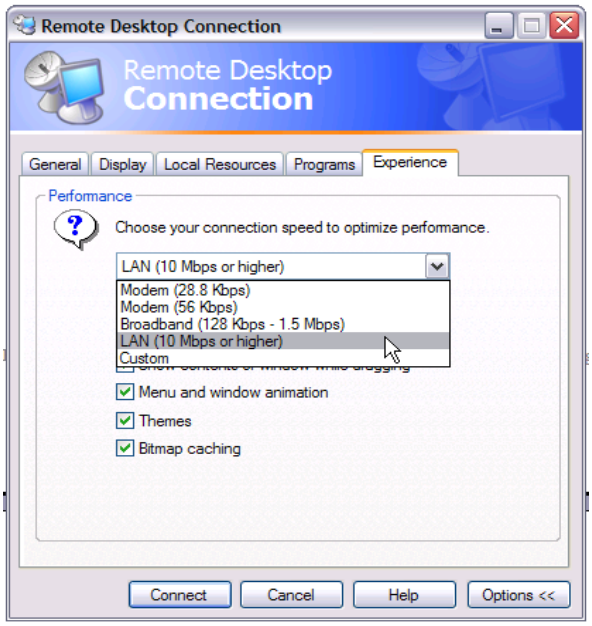
Figure 5: Example of Remote Computer Sound

Connection Speed

To set the connection speed:

1) Click the **Experience** tab (Figure 6).
2) Select **LAN (10 Mbps or higher)** from the **Choose your connection speed to optimize performance** drop-down list.

Figure 6: Example of Connection Speed

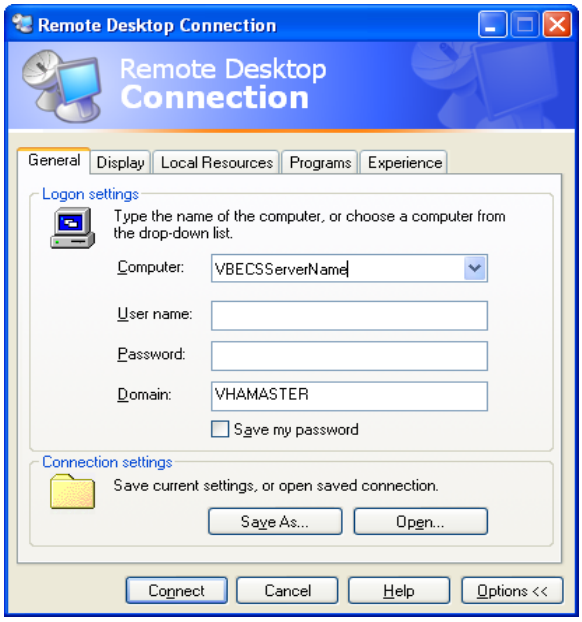


Save Settings

To save the settings:

1) Click the **General** tab (Figure 7).
2) Click **Save As**.

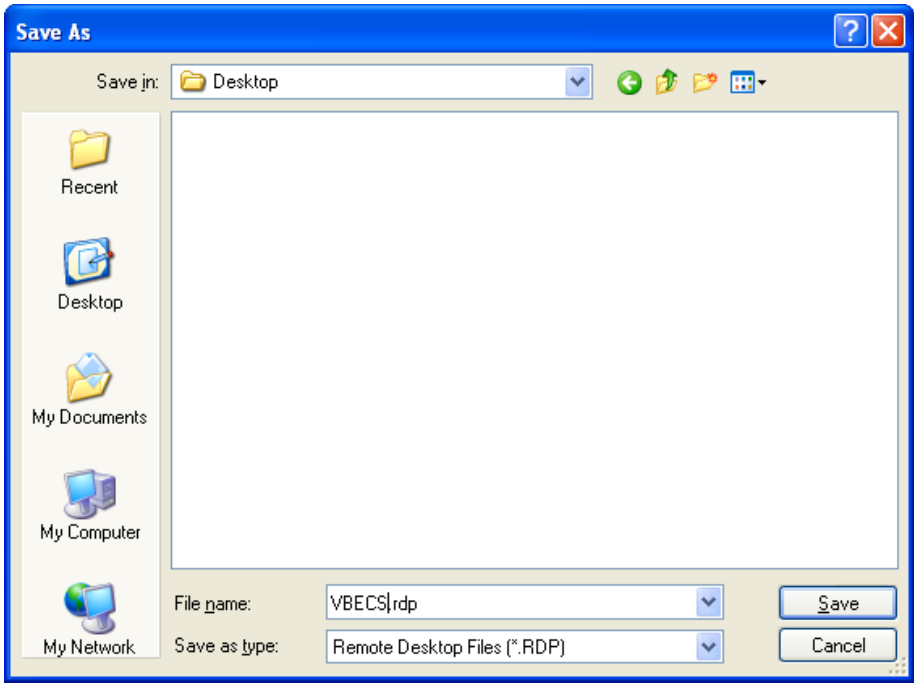
Figure 7: Example of General Tab: Save As



Create a Remote Desktop Connection Shortcut for VBECS

1) To create a Remote Desktop Connection shortcut for VBECS (Figure 8), save the file as VBECS.rdp in the **All Users, Desktop** folder.

Figure 8: Example of Remote Desktop Connection Shortcut for VBECS



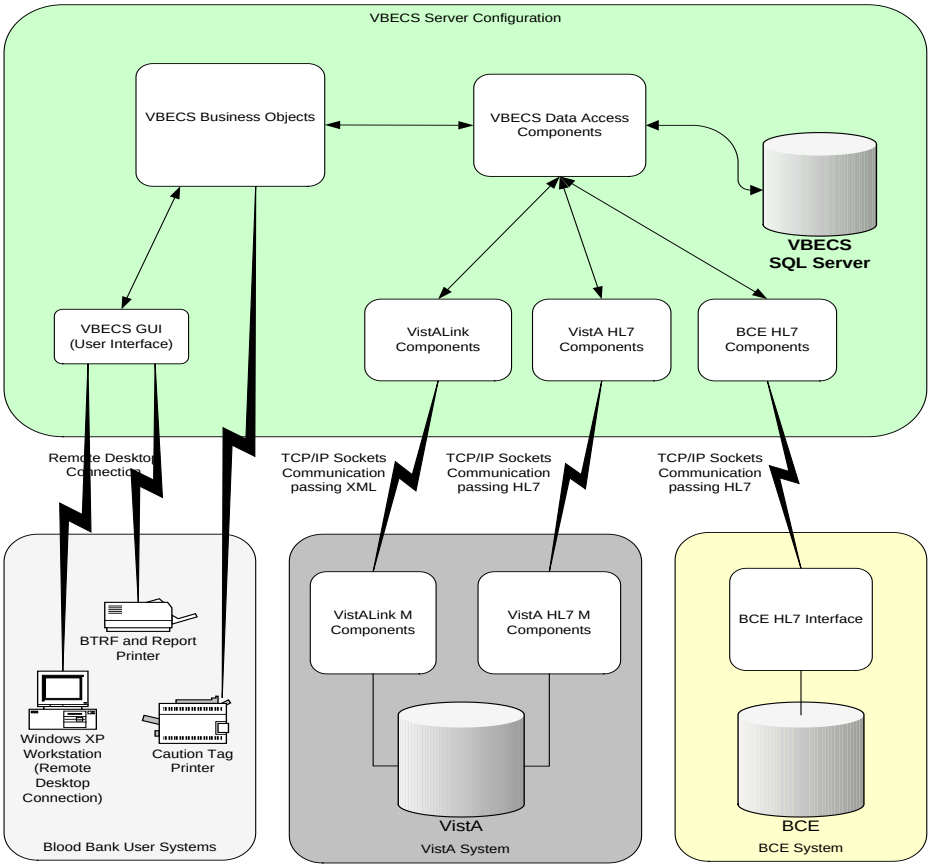
2) Double-click the shortcut to launch the remote desktop connection to VBECS.
3) The Windows start-up sound confirms that the sound functions.

Server Hardware and System Configuration

The VBECS application requires that hardware and system software serve five users in a standard configuration and up to 25 users in an integrated Veterans Integrated Service Network (VISN) environment.

The System Schematic diagram (Figure 9) describes the major system components: a Windows 2003 Server system (the execution environment for the VBECS application), Windows XP and Windows 7 workstations, with which the user will access the VBECS application using Windows Terminal Services [Remote Desktop Protocol (RDP)]. The VBECS server will also communicate with and exchange information with VistA applications through messages formatted using Extensible Markup Language (XML) and Health Level Seven (HL7) over Transmission Control Protocol/Internet Protocol (TCP/IP) networking.

Figure 9: System Schematic



Server and Shared Array Disks

Server Disk Configuration

Each VBECS server has two disks in a RAID 1 (mirroring) configuration (Figure 10). This means that if one disk fails, the server will continue to run normally.

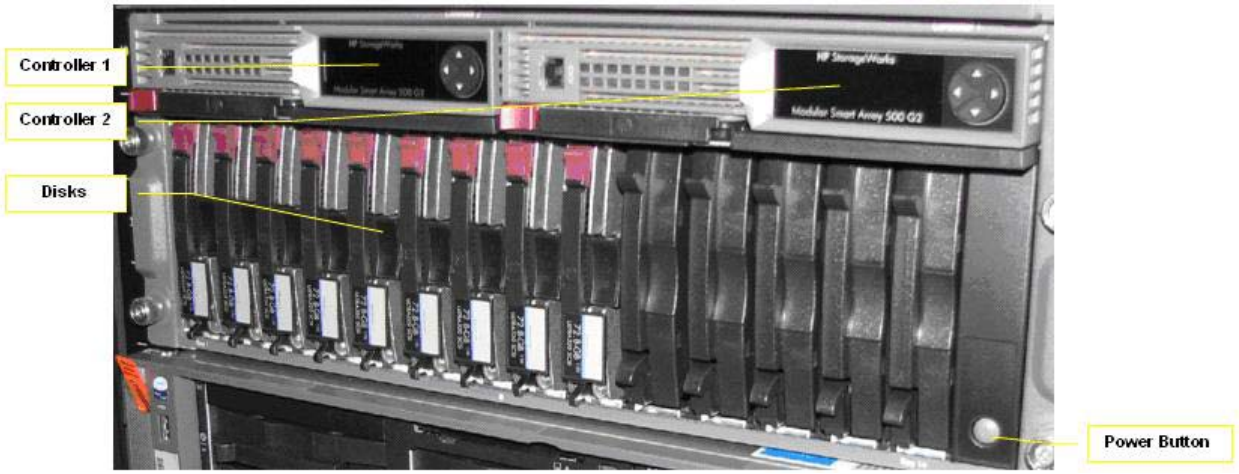
Figure 10: Server Disks

Shared Array Configuration

The shared disk array consists of nine disks (Figure 11).

- The first four disks are used to store VBECS specific data. These disks are configured as RAID 5.
- The fifth disk is a hot spare. It can be used if one of the other disks fails. Note that the LED on it will be off.
- Disks 6 and 7 are for log storage and backups. These disks are configured as RAID 1.
- Disks 8 and 9 are for cluster support. These disks are configured as RAID 1.

Figure 11: Shared Array



Replacing a Disk

All disks in the system, both server and array, are hot swappable. This means that if a disk should fail, it can be replaced without powering down the system or disrupting users. Simply remove the failing disk and replace it with a new one. It will take a couple of minutes to rebuild. For more information on monitoring and viewing disk health, please see the HP Array Configuration Utility section.

Printers

Printer IP address must be added to the Access Control List (ACL).

Laser Printer

A laser printer capable of printing 8.5" x 11" sheets may be used. Printer naming and drivers must be consistent across both servers.

Installing a Printer

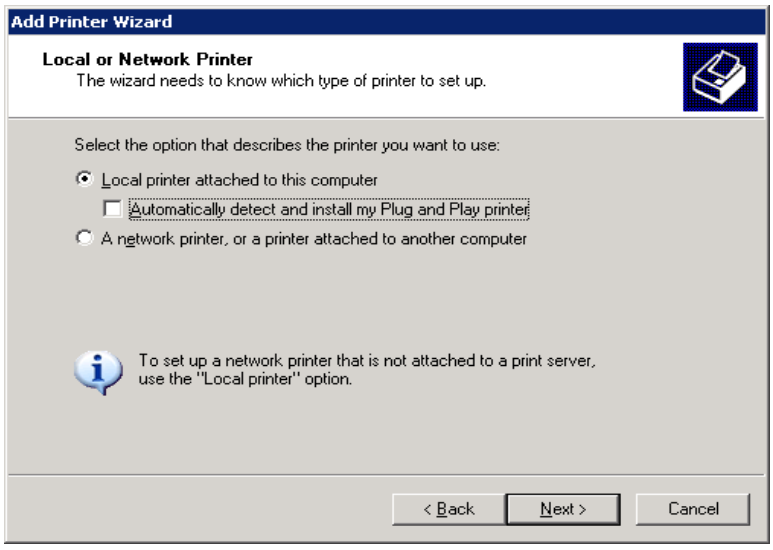
To install or reinstall a printer, execute the following instructions on each cluster node:

1) Log into the first server with your Windows ID.
2) Click **Start**, **Control Panel**, **Printers and Faxes**, **Add Printer.**
3) In the Add Printer Wizard screen, click **Next** (Figure 12).

Figure 12: Example of Add Printer Wizard

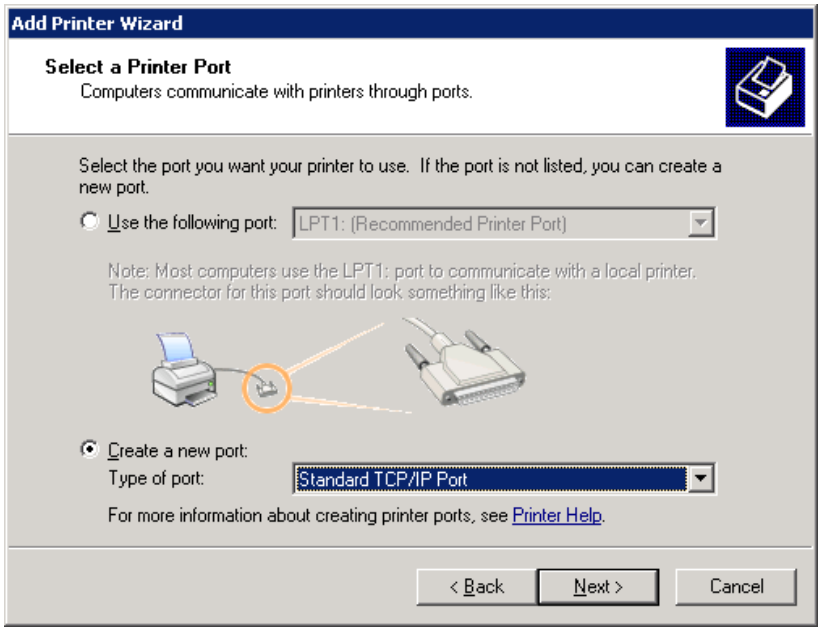
4) Make sure the **Local printer attached to this computer** radio button is selected.
5) Uncheck the **Automatically detect and install my Plug and Play printer** check box.
6) Click **Next** (Figure 13).

Figure 13: Example of Add Printer Wizard



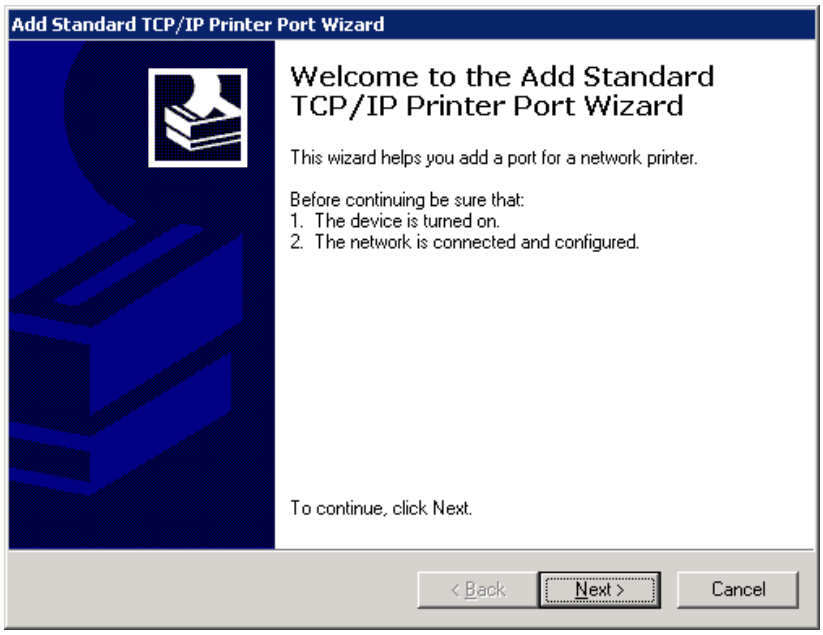
7) Select the **Create a new port** radio button.
8) Select **Standard TCP/IP Port** from the drop-down menu. Click **Next** (Figure 14).

Figure 14: Example of Add Printer Wizard



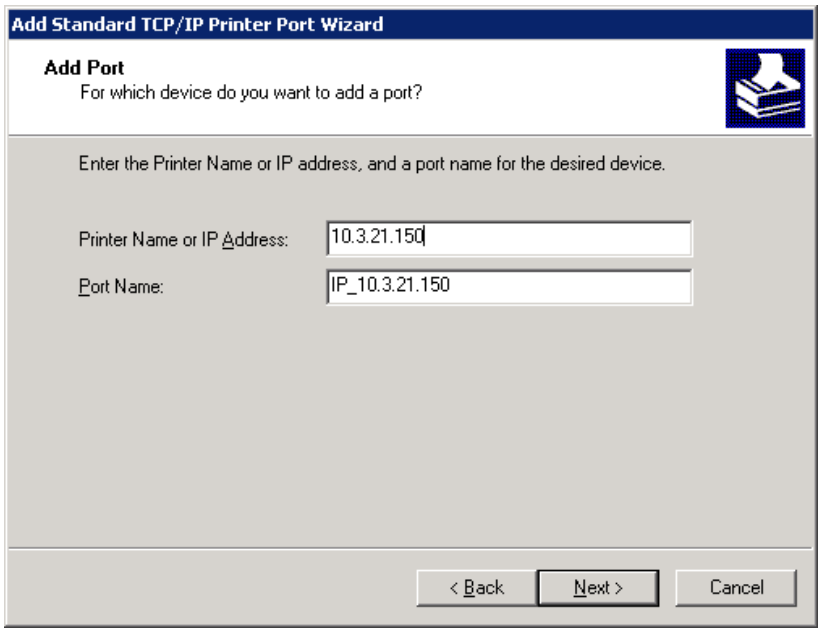
9) In the Add Standard TCP/IP Printer Port Wizard screen, click **Next** (Figure 15).

Figure 15: Example of Add Standard TCP/IP Printer Port Wizard



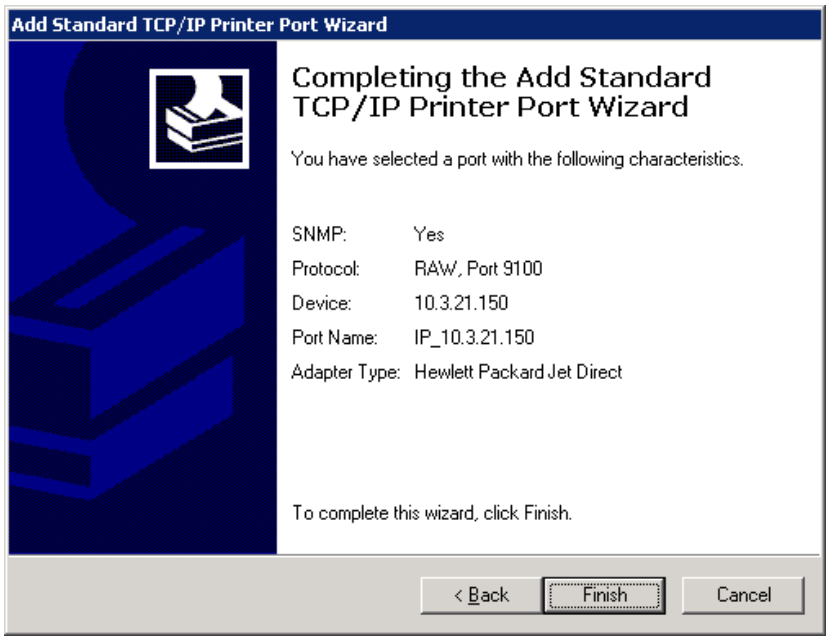
10) Enter the IP address of the printer in the "Printer Name or IP Address" field (the Port Name field will populate automatically). Click **Next** (Figure 16).

Figure 16: Example of TCP/IP Settings



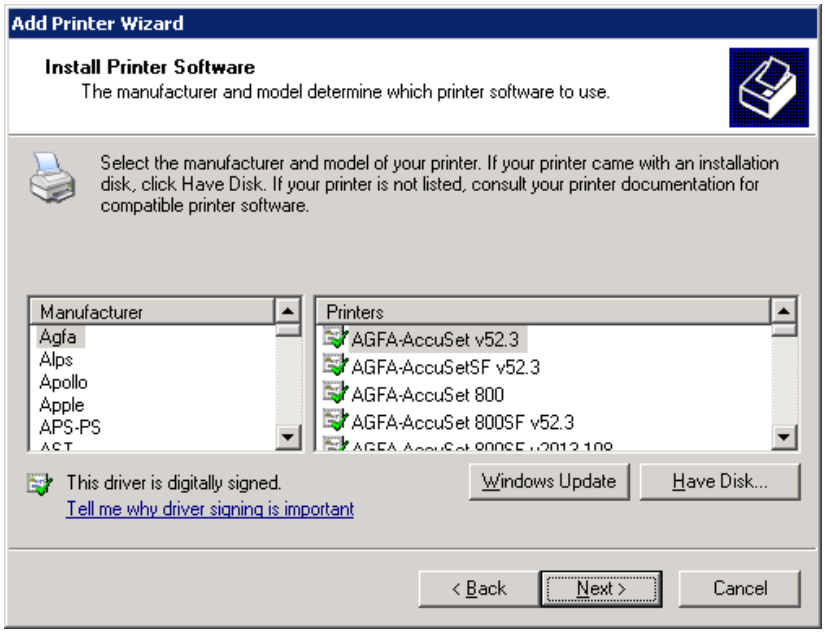
11) Click **Finish** (Figure 17).

Figure 17: Example of Review Settings



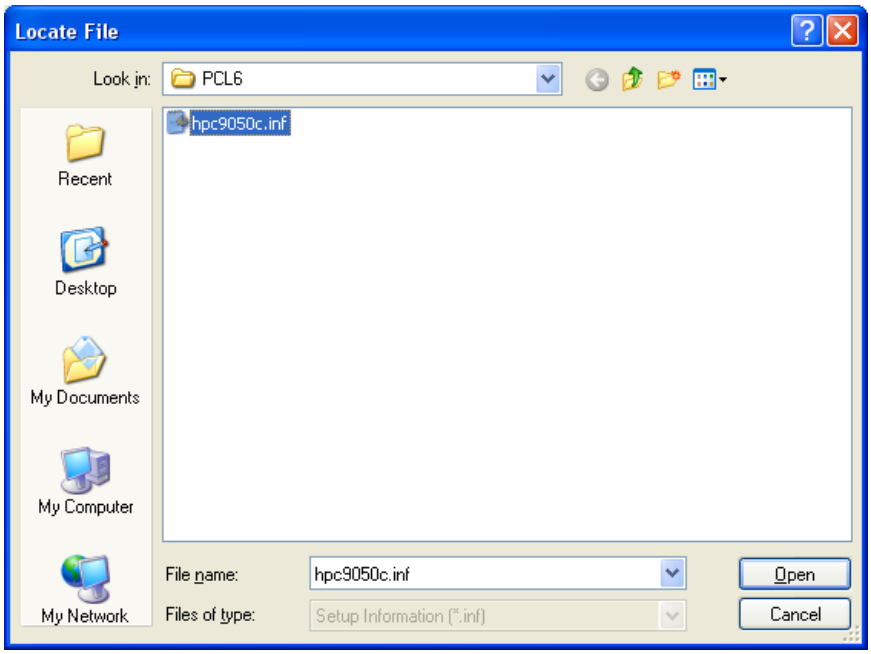
12) To select a driver, click **Have Disk** (Figure 18). Note: If your site has chosen to use a printer other than the HP LaserJet 9040, you must point to your own driver at this point, continue at Step 16.

Figure 18: Example of Add Printer Wizard



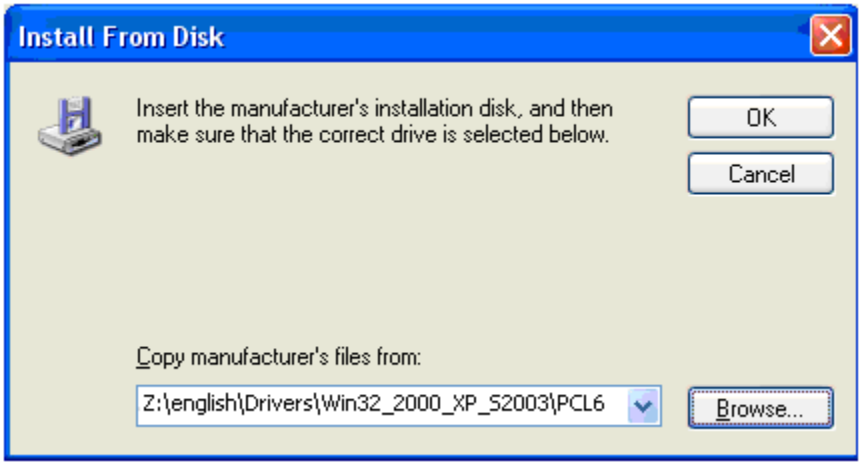
13) Enter **\\10.3.9.165\\PCL6**. Select **hpc9050c.inf**. Click **Open** (Figure 19).

Figure 19: Example of Navigate to the Driver



14) Click **OK** (Figure 20)**.**

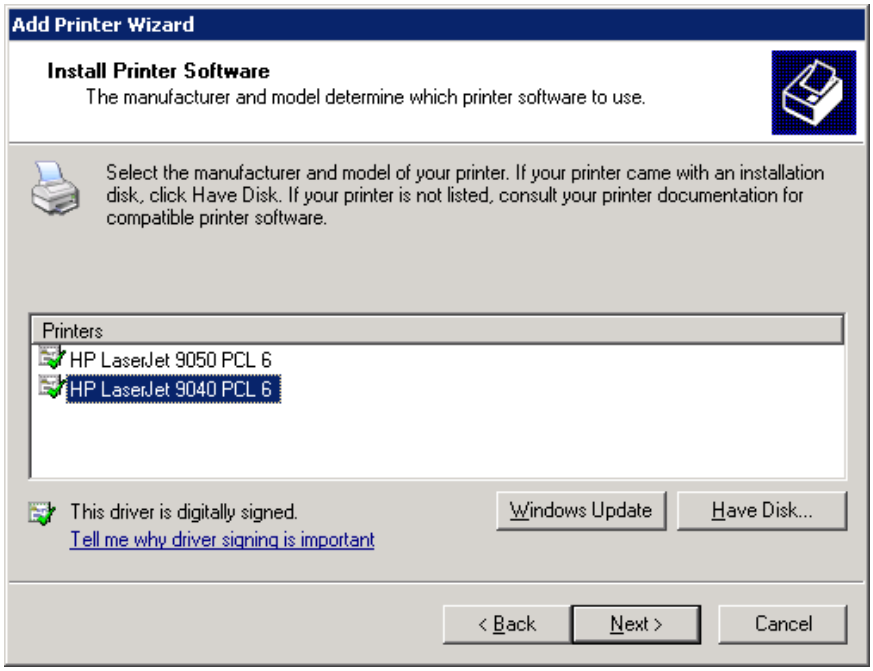
Figure 20: Example of Install From Disk



15) Select **HP LaserJet 9040 PCL 6**. Click **Next** (Figure 21).

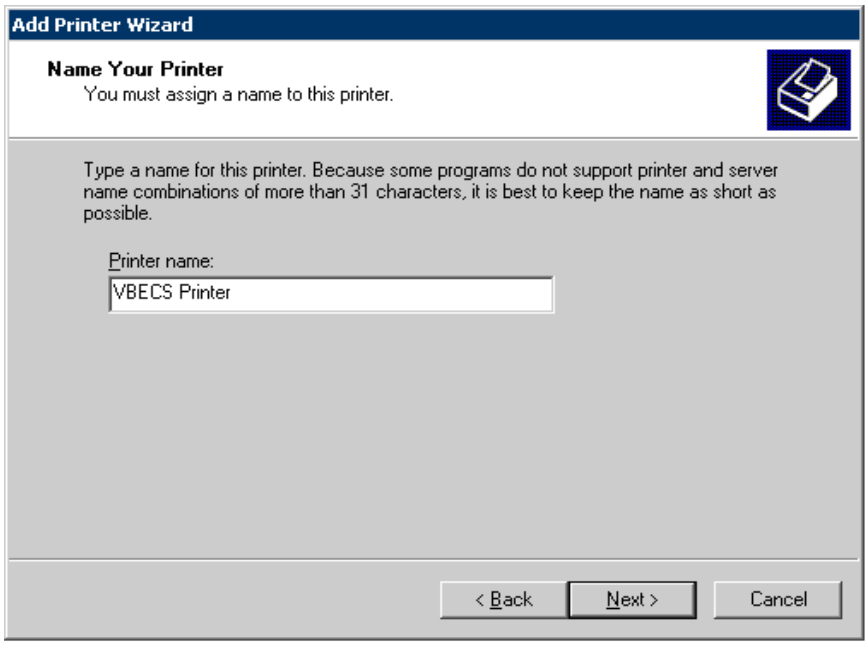
Make sure that the HP LaserJet 9040 PCL 6 driver is selected.

Figure 21: Example of Add Printer Driver Wizard



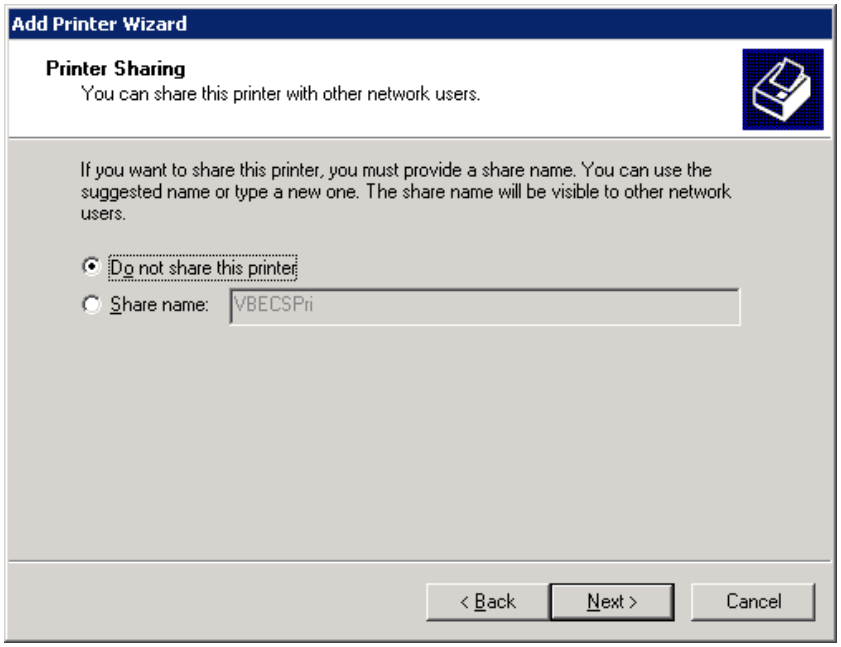
16) For a single-division site, enter **VBECS Printer** as the printer name. For a multi-divisional site, enter **VBECS Printer** and the site name (e.g., VBECS Printer Hines). Click **Next** (Figure 22).

Figure 22: Example of Add Printer Wizard



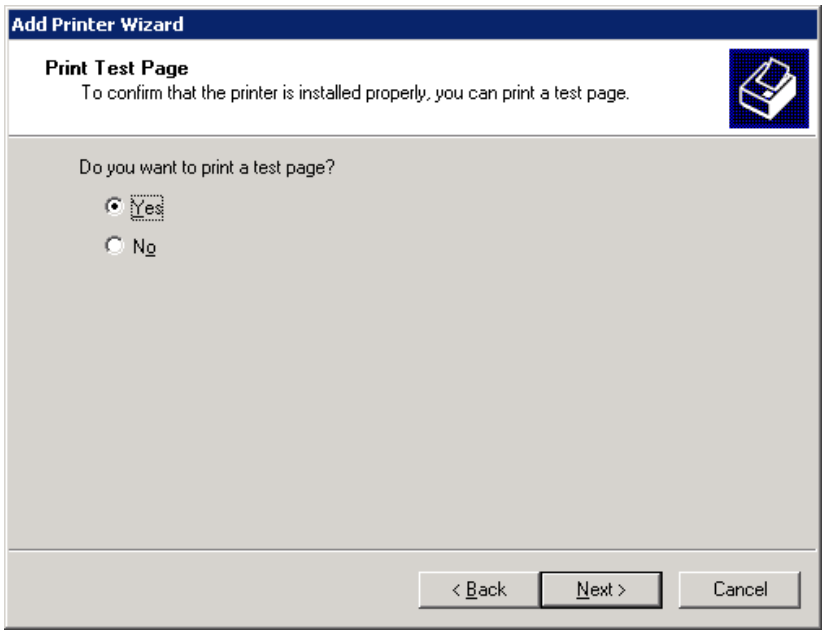
17) Click the **Do not share this printer** radio button. Click **Next** (Figure 23).

Figure 23: Example of Add Printer Wizard



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

Figure 24: Example of Add Printer Wizard



19) Repeat these instructions on the other cluster node.

Label Printer

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

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

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

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

Set the IP Address on the Printer

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

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

Test the Printer

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

Adjust Label Darkness

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

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

Adjust Label Offsets

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

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

Scanners

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

1) Connect the scanner to the workstation.
2) To configure a Hand Held 4600 barcode scanner, scan the barcode in Figure 25. Repeat for all scanners.

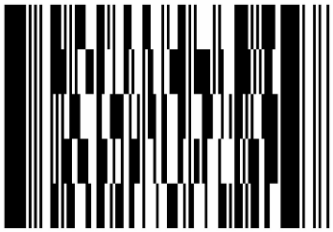
Figure 25: Configure a Barcode Scanner

3) To test the scanner, open Notepad. Print and scan the barcodes in Figure 26, Figure 27, and Figure 28. The Codabar and ISBT barcodes must scan as "~123456789"; the PDF 417 must scan as "~Testing."
4) Save and print the Notepad file for validation records.

Figure 26: Codabar

Figure 27: ISBT 128

Figure 28: PDF 417



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.*

Table 1: Server Configuration

Hardware	Clustered Database Server (two identical systems)
Processor	Multiple processors (2–4 processors) Pentium 4 Xeon 2.0 GHz processors (or greater) with 512kb level 1 cache
Memory	2-gigabyte (or greater) main storage (RAM)
Storage	Shared Storage Controller Unit. Disk configuration: 8 hot swappable SCSI hard drives (minimum 10,000 RPM). The system drives require 18 gigabytes (or greater) storage capacity. The application data drives require 36 gigabytes; log volume and historical data drives require 72 gigabytes (or greater) storage capacity. A ninth disk has been included that serves as a hot spare. If a live disk should fail, it can be replaced with this one.
Operating System	Microsoft Windows 2003 Server Enterprise with Microsoft Clustering Services providing failover data-device sharing
Network Controller	Multiple 10/100 network cards configured to provide fallback in event of failure.
Power Supply	Primary and secondary (redundant) power supply to server chassis and an uninterruptible power source (UPS)
Backup	Internal tape backup with software
Integrated Lights Out (iLO)	A hardware device attached to the servers that allows for remote management

This configuration is designed to promote 24/7 availability and use of the application. A clustered database server configuration will provide near immediate failover if one node of the server fails. Multiple processors will provide for more efficient processing of database access requests and operating system processes.

Dual power supply and UPS will ensure that the machine will not lose operating power. The disk storage configuration will allow the server disks to be shadowed; if a main disk fails, the shadow disk will automatically continue system operation until the primary disk is replaced. Hot swappable disk drives can be replaced without shutting down the server. Internal tape backup on the application data disk will allow an image of the application data to be restored to another machine if the server is damaged.

Required Hardware

Table 2: Required Hardware

Hardware	Description
Zebra Printer	Zebra printer capable of producing 300 DPI barcode labels (network capable)
Barcode Scanner	Symbol Model LS4006i barcode scanner for each workstation
Report Printer	Laser printer or comparable with sufficient speed to handle high-volume reports (network capable)

Workstation Configuration

Table 3: Workstation Configuration

Hardware	Description
Processor	Suitable for Windows XP or Windows 7
Memory	Suitable for Windows XP or Windows 7
Monitor	17" monitor or greater
Video	Video card capable of displaying minimum of 16-bit color at 1024 x 768 resolution
Disk Storage	9 gigabytes (minimum)
Operating System	Microsoft Windows XP/ 7 Professional with Microsoft Terminal Services Client
Network Controller	10/100 network card
Input Devices	U.S. 101-key keyboard, mouse
Audio	Sound card and speakers (may be internal)

Off-the-Shelf Software Requirements


Do not upgrade, change, or add software to the VBECS server as this may compromise the integrity of VBECS.

Table 4: Off-the-Shelf Software Requirements

Software	Description
.NET Framework	Version 1.1, Version 4.0
SQL Server	SQL Server 2000 Enterprise Edition
Crystal Reports	Crystal Reports .NET
Backup software	VERITAS Backup Exec Version 10.0
McAfee VirusScan	Version 8.5

Implementation and Maintenance

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 runs nightly from 12:00 AM to 3:15 AM. 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. Follow all instructions in the *VistA Blood Establishment Computer Software (VBECS) Installation Guide* for configuration.

Table 5: Periodic System Maintenance

Action	Frequency	Description
Backup tape rotation	Daily	If using Backup Exec, backups automatically occur every morning per the time specified in the VBECS Installation Guide. Refer to local policy for data retention and offsite storage requirements.
System Center Operations Manager (SCOM) Alerts	Daily	SCOM emails alert messages to the VBECS Administrators mail group, which is defined in the Installation Guide, as problems occur on the clustered servers. Investigate all alerts to completion.
Review Database Integrity Reports	Daily	The Integrity jobs run daily, an email alert is sent to designated recipients when allocation and consistency errors are found or the Integrity job fails. See the SQL Maintenance Jobs section for more details.
Windows / Virus Updates	2nd Tuesday of the month	A VistA Informational patch is released when the updates have been tested and approved for installation.
Firmware Updates	As needed	A VistA Informational patch is released when the updates have been tested and approved for installation.
VBECS Updates	As needed	A VistA Informational patch is released when the updates have been tested and approved for installation.

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 6. The following is a list of the SQL Server databases needed by the VBECS application:

- msdb (contains information relating to the SQL Server jobs)
- master (required for SQL Server and all databases within to operate)
- VBECS_V1_PROD (VBECS production account database)
- VBECS_V1_PROD_MIRROR (VBECS production account audit database)
- VBECS_V1_TEST (VBECS test account database)
- VBECS_V1_TEST_MIRROR (VBECS test account audit database)

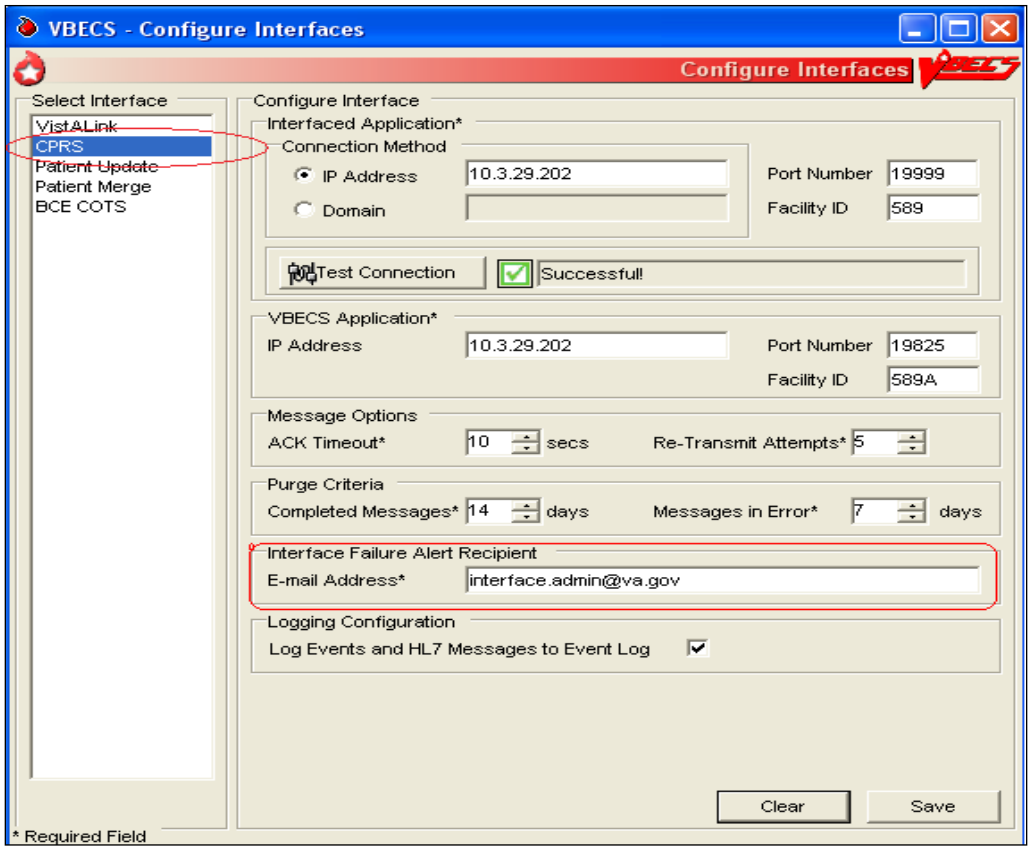
Table 6: VBECS SQL Maintenance Jobs

Database Affected	Job Name	Frequency and Time (local time) Job Runs	Description
All VBECS databases	ResetServerLogFile	Saturday, at 12:00:10 am	Truncates and starts a New log file for SQL Server without having to restart the server
All VBECS databases	DailyIntegrityCheck	Daily at 12:11:50 am	Checks the physical integrity of the database and generates a report for manual verification.
vbecs_v1_prod vbecs_v1_test	ExpireComponentOrders	Daily at 1:00:00 am	Expires component orders when the associated specimen expires or other specific criteria are met.
	ExpireTestOrders	Daily at 1:00:00 am	Expires test orders when the associated specimen expires or other specific criteria are met.
	MarkUnitsPresumedTransfused	Daily at 1:10:00 am	Marks units as presumed transfused if transfusion or bedside verification information was not returned to the blood bank within 48 hours.
All VBECS databases	ShrinkLog	Daily at 1:50:00 am	Removes free space at the end of the database log file.
All VBECS databases	DailyBackup	Daily at 2:00:00 am	Full database backup
All VBECS databases	UpdateStats	Daily at 2:20:00 am	Updates statistics on all user defined tables to improve performance.
	TruncateDataFiles	Daily at 2:30:00 am	Removes unused space from database files
All VBECS databases	CopyVBECSDBBackups to LDrive	Daily at 2:40:00 am	Copies the latest database backup and integrity log files to L:\Program Files\ Microsoft SQL Server\MSSQL\Backup\ <database> folder and renames the files to include the current date.
	L Drive Delete old Backup files	Daily at 2:50:00 am	Deletes database backup and integrity log files that are more than 7 days old.
All VBECS databases	ReIndexTables	Daily at 3:00:00 am	Re-Indexes the database tables to improve performance.

SQL Maintenance Job Alerts

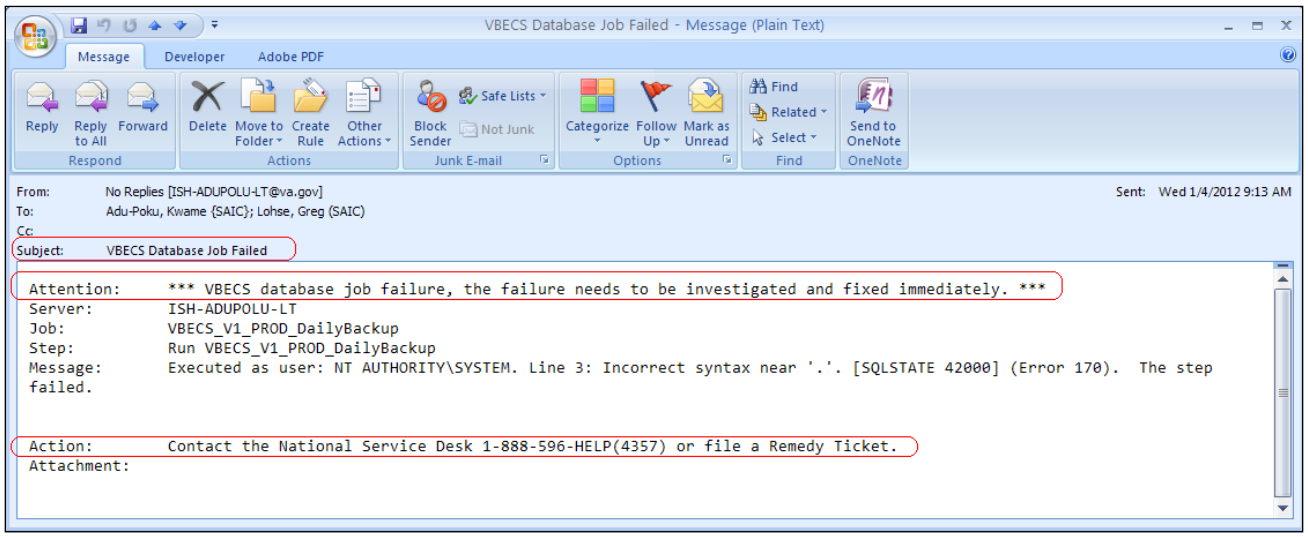
VBECS sends an email alert message only when a SQL maintenance job fails. The emails are sent via *smtp.va.gov* to the recipients as configured in the **Configure Interfaces** menu of the VBECS Administrator production software; the recipient email address is modifiable in the **Interface Failure Alert Recipient** section of the CPRS interface (Figure 29). The email recipients for all SQL jobs (VBECS test and production) use the value from the VBECS production database.

Figure 29: Example of Setting SQL Maintenance Job Alert Recipients



If you receive a SQL maintenance job failure email alert (Figure 30), the subject of the failure alert will be "**VBECS Database Job Failed**". Follow the instructions included with the email to resolve the underlying issue.

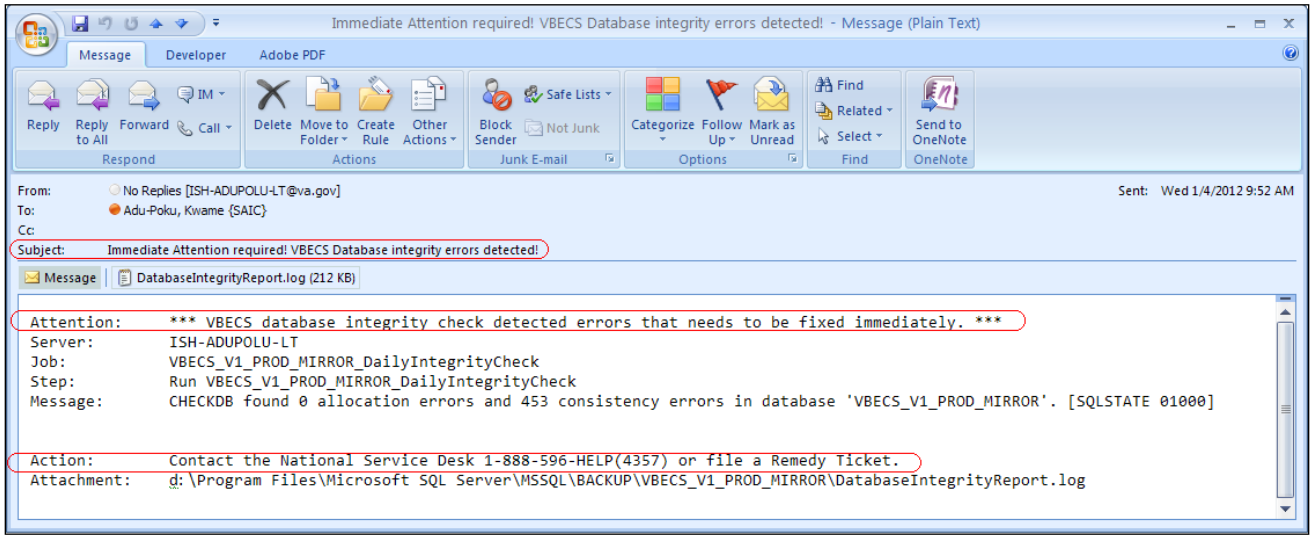
Figure 30: Example of a SQL Maintenance Job Failure Email



VBECS Database Integrity Check Job Alerts

Each database has its integrity verified daily to prevent data loss. If the integrity job detects consistency or allocation errors, an email alert will be sent with the subject: "**Immediate Attention required! VBECS Database integrity errors detected!**". The log file (named *DatabaseIntegrityReport.log*) will be attached to the email (Figure 31). Contact the National Service Desk or file a Remedy ticket.

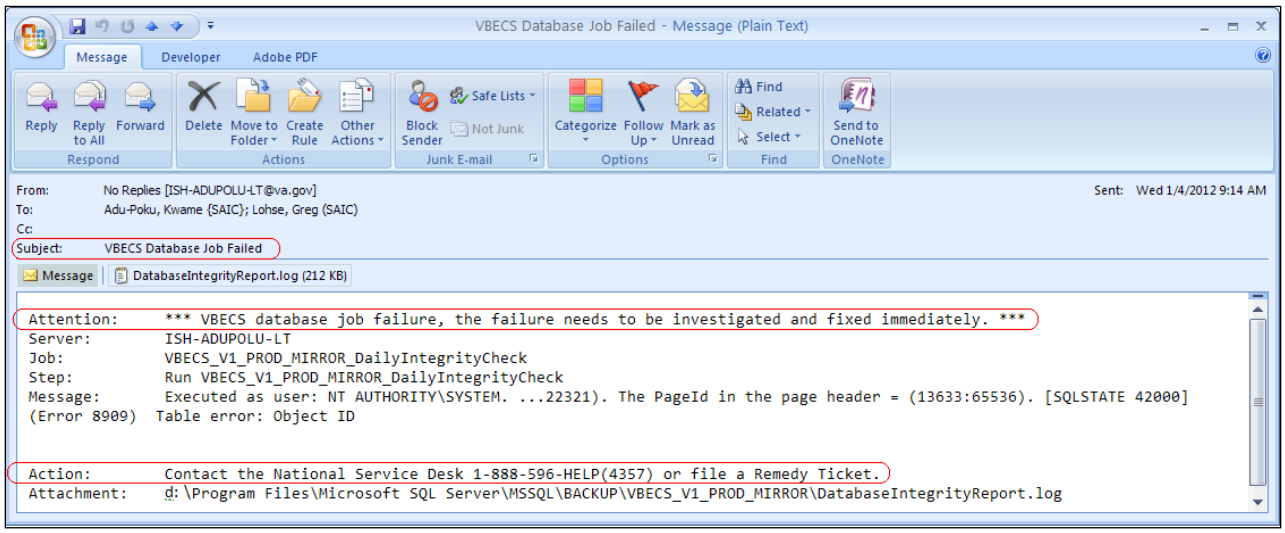
Figure 31: Example of VBECS Database Integrity Job Email with Errors



If the VBECS database Daily Integrity Check job fails, two email alerts will be received. One will have the subject "**Immediate Attention required! VBECS Database integrity errors detected!**" (Figure 31),

and the other will have the subject "**VBECS Database Job Failed**" (Figure 32). Both will have the log file (DatabaseIntegrityReport.log) attached to the email. Contact the National Service Desk or file a Remedy ticket.

Figure 32: Example of VBECS Database Integrity Job Failed Email



Backup Archiving Jobs

To assist recovery and support options, every backup file and *DatabaseIntegrityReport.log* is copied ("archived") nightly via the SQL job: **Copy VBECS DB Backups to L Drive**. As each database backup and integrity log file is copied to the L:\Program Files\Microsoft SQL Server\MSSQL\BACKUP\<*database name*> folder, the files names are appended with the current date (e.g., *filename_20110420* for files copied on April 20, 2011). These "archive" files are retained for seven days, at which time the daily SQL job, **L Drive Delete old Backup files**, deletes them from the L drive. The seven-day retention period is contained within the code of the **L Drive Delete old Backup files** job.

Windows Updates

If your servers reside at a data center that has its own update distribution system, please refer to Appendix E: Data Center Instructions.

The VBECS development team must test every Microsoft Windows update. Once the development team is satisfied that the update causes no adverse effects, they will notify sites that there are Windows updates. A VistA information patch in the VBEC namespace will be created by the VBECS team each time an update is available describing where to obtain the update and how to apply it. The patch will be released to customers by VA Product Support.

Updates are approved with Windows Software Update Service. Approved updates will be downloaded to your servers automatically. However, a server administrator must install the updates manually on each server.

VA Product Support will notify the sites of updates required for installation.

ePolicy and Virus Definitions

The VBECS development team must test virus definitions before they are applied to the servers. The VBECS development team will send the virus definitions: do not apply virus definitions locally.

 *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.*

Commonly Used System Rules

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

- Only one instance of the VBECS Administrator can run at a time.
- VBECS captures changes to verified data for inclusion in the Audit Trail Report.
- VBECS protects application data through encapsulation. Encapsulation promotes data security by hiding the implementation details.

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

Firmware Updates

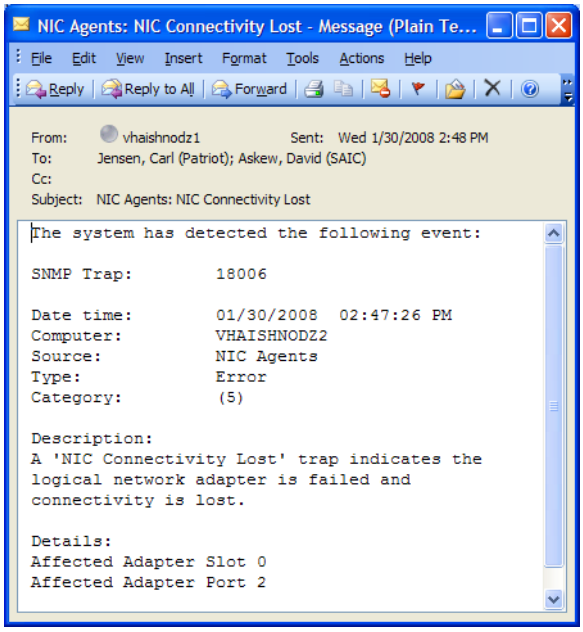
Occasionally, hardware including the server components, printers and scanners require firmware updates. Forum informational patch messages are posted when the updates have been tested and approved for installation.

Hardware Utilities and Backup Exec Alerts

HP Event Notifier

Hardware alerts are generated with HP Event Notifier. Event Notifier will generate email alerts whenever a hardware failure occurs. Examples of hardware failures include, but are not limited to; controller, network interface card and fan failures. An example of a network interface card losing connectivity is displayed in Figure 33.

Figure 33: Example of an Email Alert from Event Notifier



When an alert is received, a server administrator should investigate the problem as soon as possible in order to prevent VBECS downtime. If necessary, contact HP support for assistance at 800.633.3600.

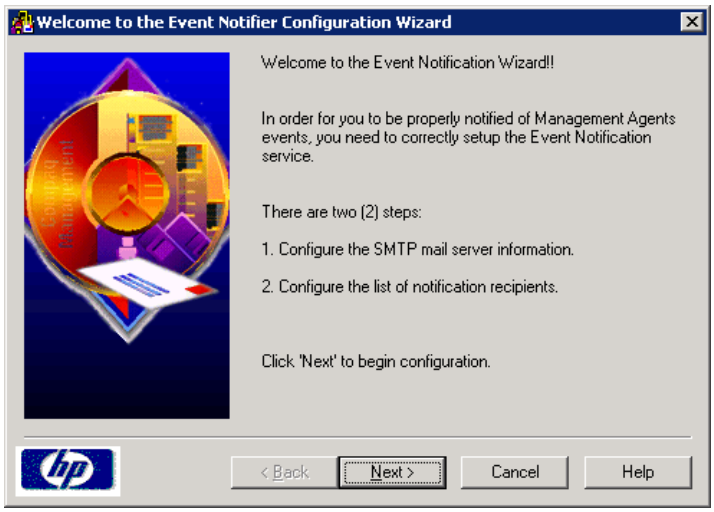
Configuring Event Notifier

To add or modify hardware alerts on servers, take the following steps:

1) Log into the server with administrative rights.
2) Click **Start**, **HP Management Agents**, **Event Notifier Config**.

3) Click **Next** (Figure 34).

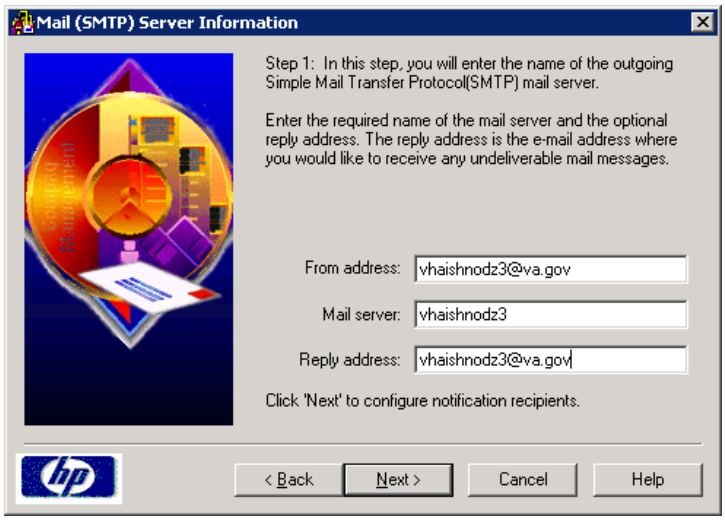
Figure 34: Example of Welcome Screen



4) Enter the following (Figure 35):
   - From address: <servername>@va.gov
   - Mail server: <servername>
   - Reply address: <servername>@va.gov

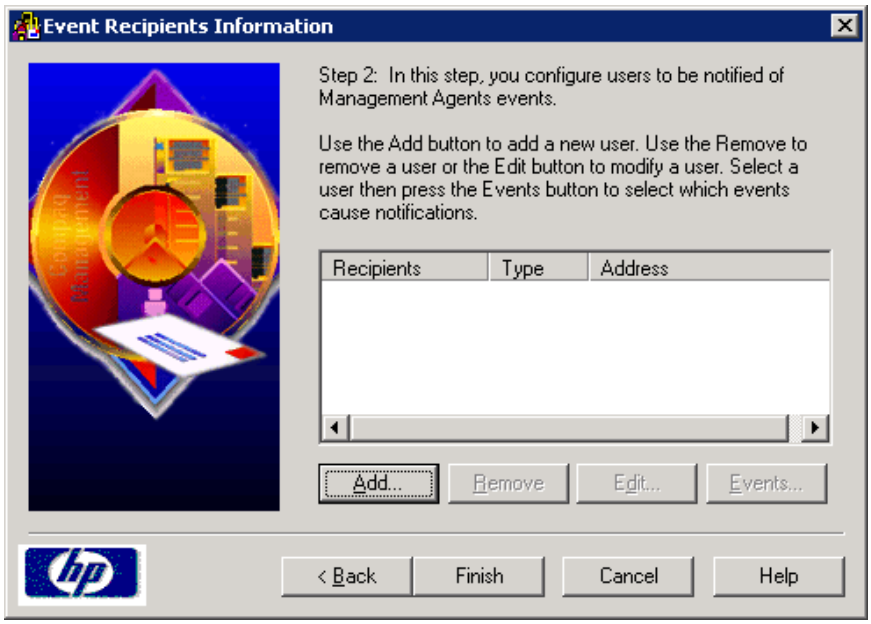
   Click **Next**.

Figure 35: Example of SMTP Configuration



5) Click **Add** (Figure 36). Note that **Remove** or **Edit** can be used for modification and deletion of existing groups respectively.

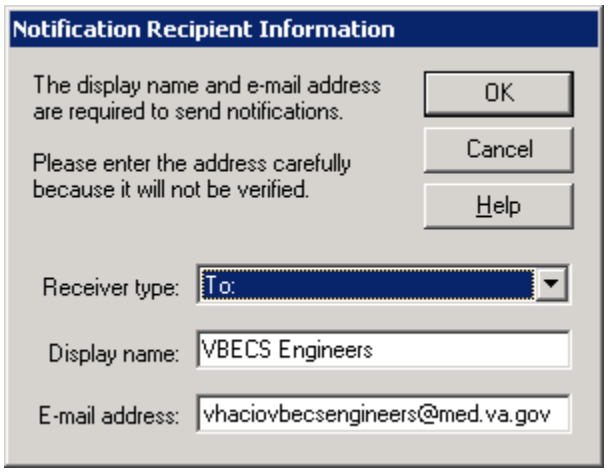
Figure 36: Example of Recipients



6) Enter the following (Figure 37):
   - Display name: Arbitrary name that describes the email group being entered.
   - E-mail address: Email group address of support personnel. Note: Use the support email address that was defined in the *VBECS Installation Guide* (Appendix E: Contact Information).

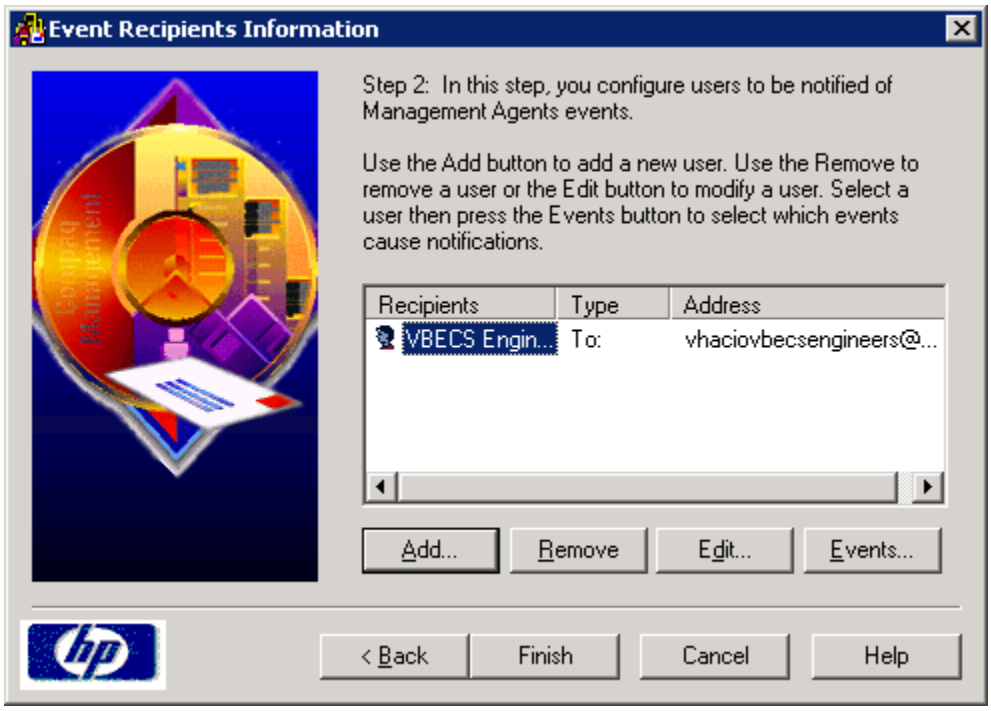
   Click **OK**.

Figure 37: Example of Notification Recipient Information



7) Click **Finish** (Figure 38). Repeat these instructions on the other server.

Figure 38: Example of Event Recipients Information



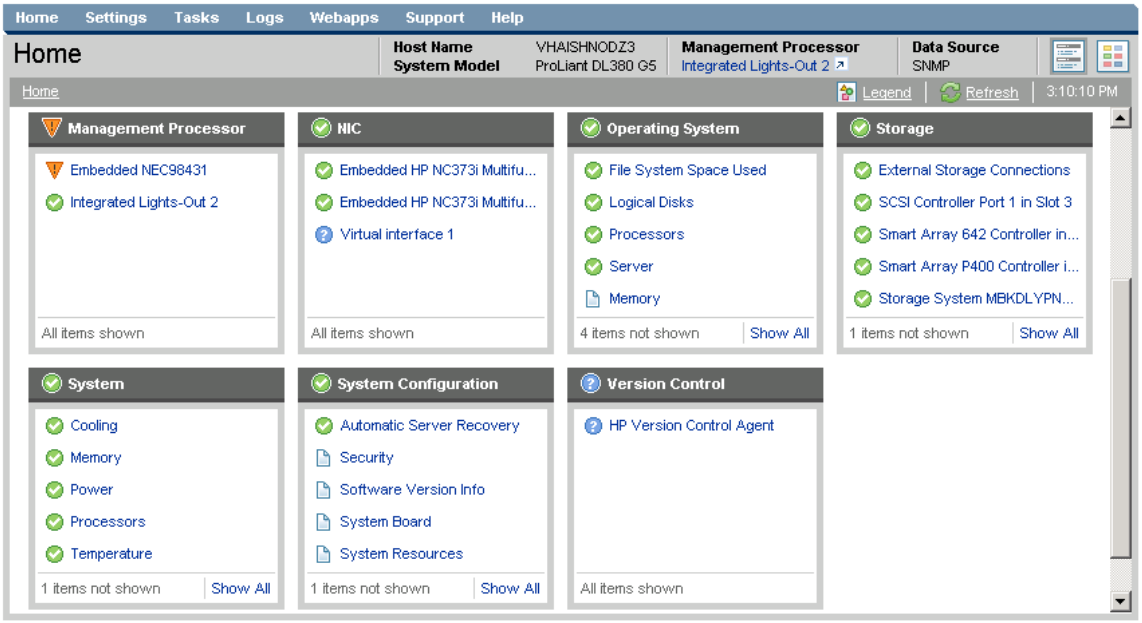
HP System Utilities

There are several pre-installed utilities on the system that are useful when checking hardware health and diagnosing problems. All of these tools are launched from the **Start** menu and all require administrative rights. Please see HP documentation for specific information regarding further use of any of these tools.

HP System Management Homepage

This tool quickly lets the administrator see the status of all major components of the system including the shared array (Figure 39).

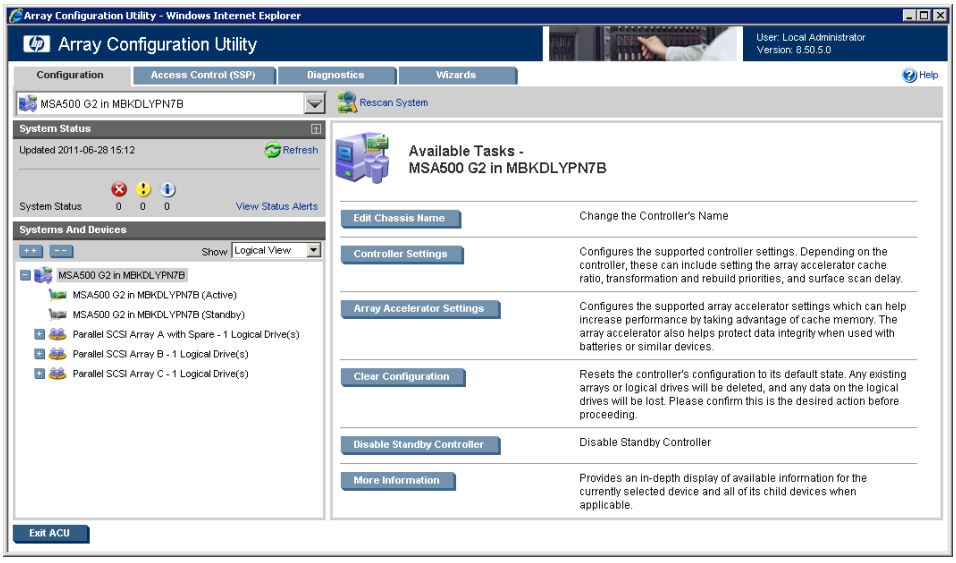
Figure 39: Example of System Management Homepage



HP Array Configuration Utility

This tool shows the state of disks, both server and shared array (Figure 40).

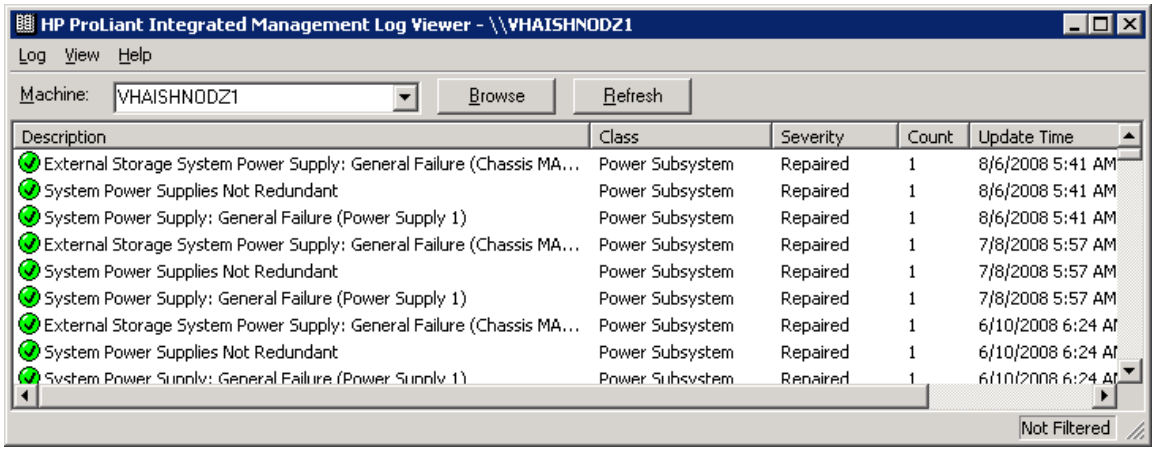
Figure 40: Example of Array Configuration Utility



HP ProLiant Integrated Log Viewer

All hardware related issues are logged here (Figure 41).

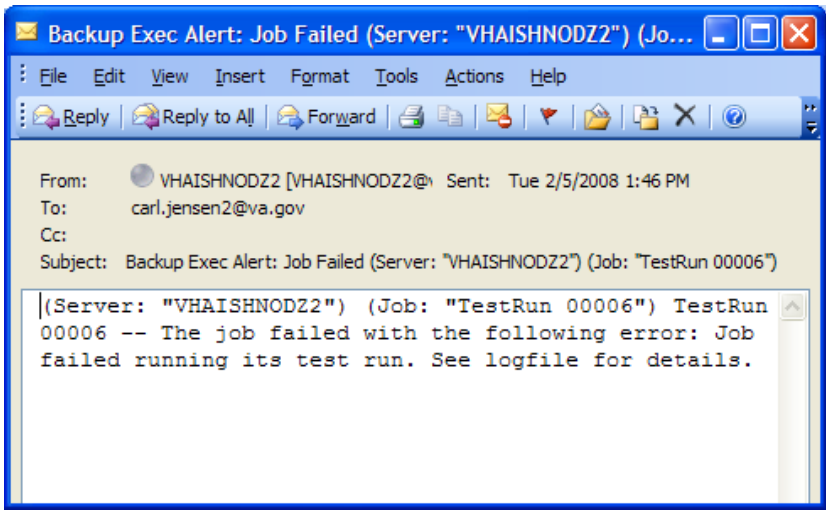
Figure 41: Example of HP ProLiant Integrated Management Log Viewer



Backup Exec Alerts

Backup Exec job failure alerts are sent by Backup Exec. Whenever the nightly job fails, an alert will be sent. An example of one of these alerts is displayed in the screen capture below (Figure 42).

Figure 42: Example of an Email Alert from Backup Exec



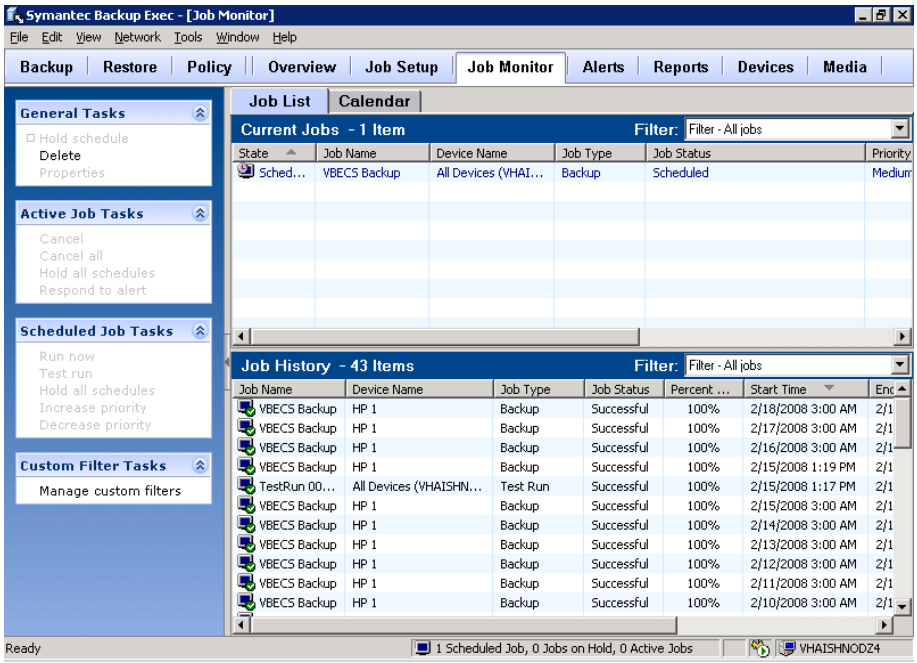
When an alert is received, a server administrator should investigate the problem as soon as possible in order to ensure proper data backup.

Configure Backup Exec Alerts

To add or modify Backup Exec Alerts on servers, take the following steps:

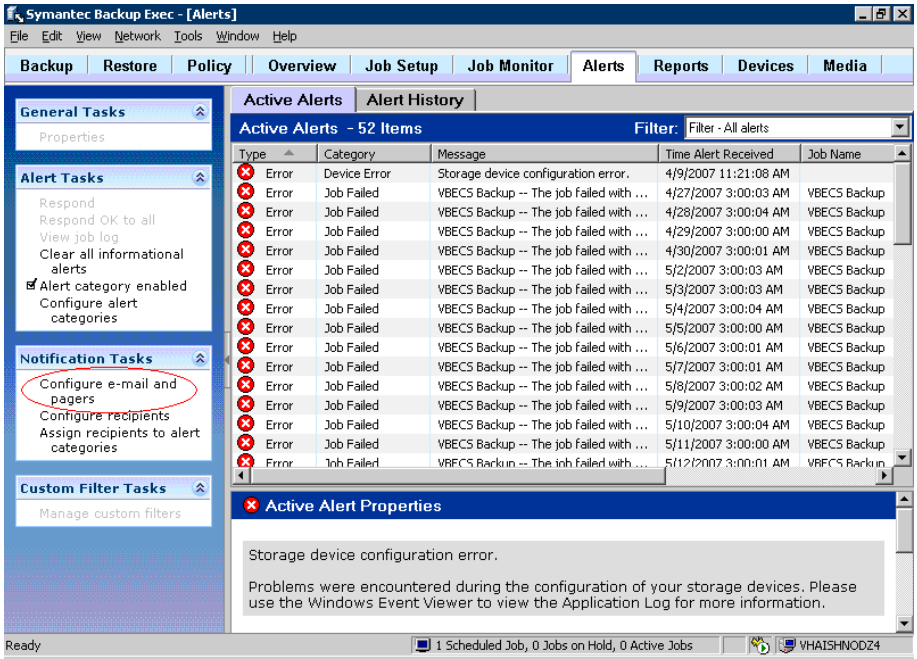
1) Log into the server (not the cluster) that has Backup Exec installed with administrative rights.
2) Click **Start**, **All Programs**, **Symantec Backup Exec 10d for Windows Servers.**
3) Click **Alerts** (Figure 43).

Figure 43: Example of Backup Exec Main Screen



4) Click **Configure e-mail and pagers** (Figure 44).

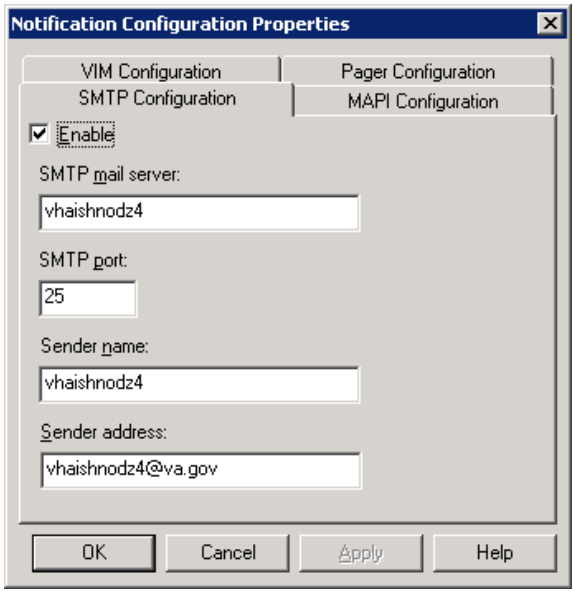
Figure 44: Example of Alerts



5) Enter the following (Figure 45):
   - Check the **Enable** box
   - SMTP mail server: <server name>
   - Sender name: <server name>
   - Sender address: <server name>

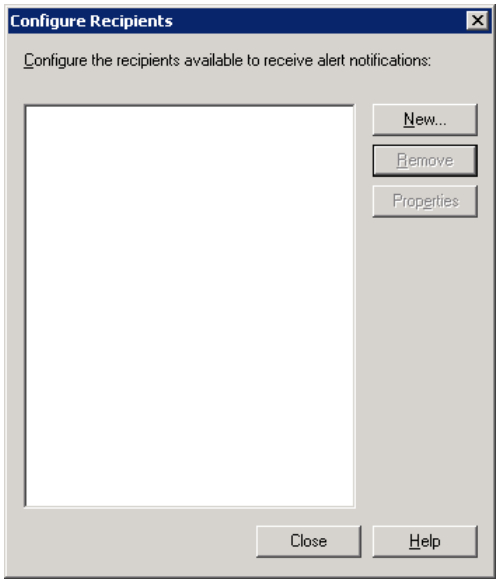
Click **OK**.

Figure 45: Example of SMTP Configuration



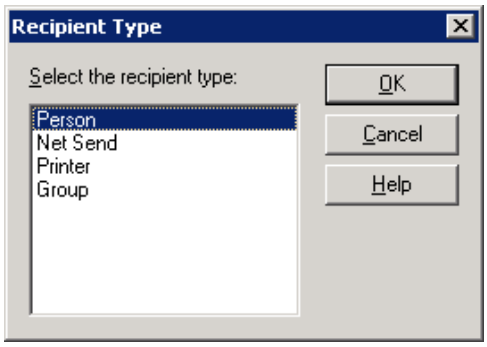
6) Click **Configure recipients** on the main Alerts screen. Click **New** (Figure 46). Note that **Remove** or **Properties** is used for deletion and modification of existing groups respectively.

Figure 46: Example of Configure Recipients



7) Click **OK** to select Person (Figure 47).

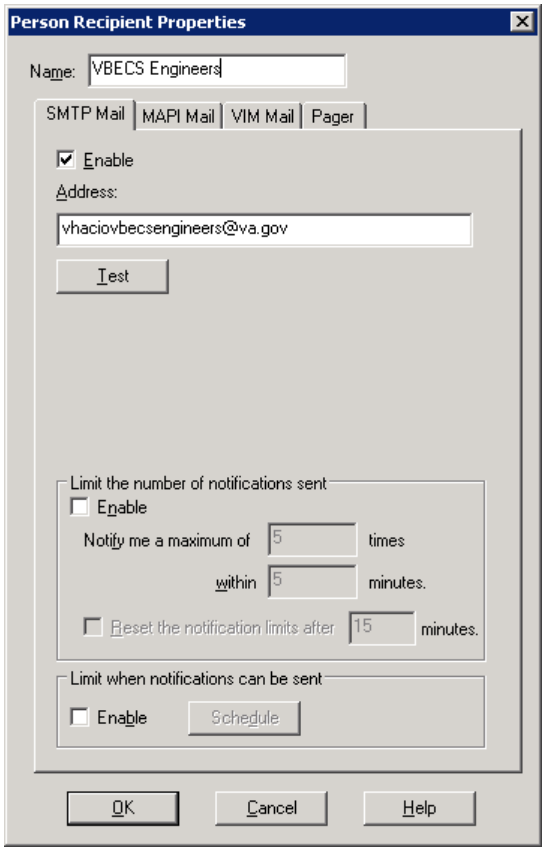
Figure 47: Example of Recipient Type



8) Enter the following (Figure 48):
   - Name: Arbitrary name that describes the email group being entered.
   - Check the **Enable** box.
   - Address: Email group address of support personnel (Note: Use the support email address that was defined in the *VBECS Installation Guide* (Appendix E: Contact Information).

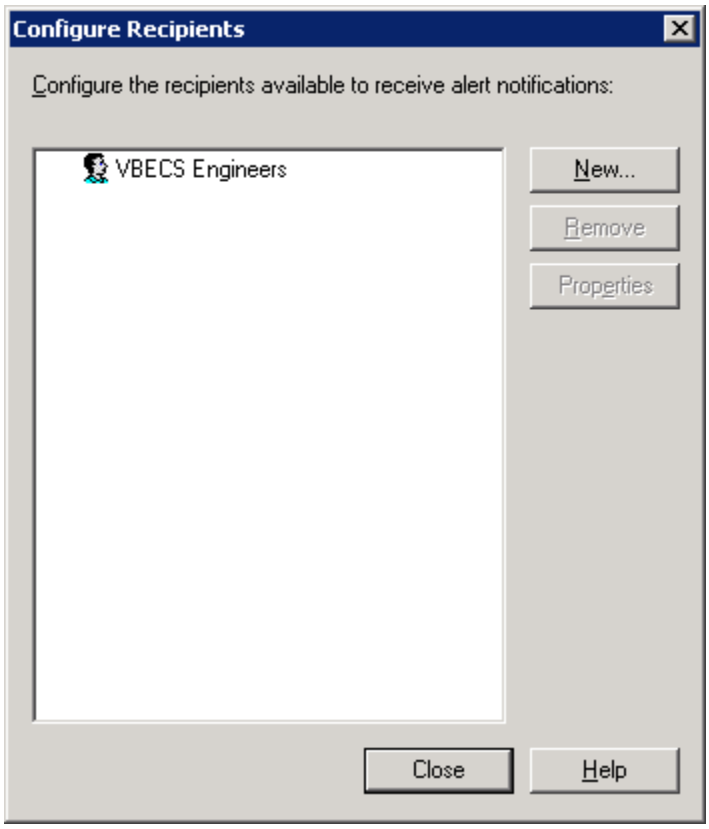
Click **OK**.

Figure 48: Example of Recipient Properties



9) Click **Close** (Figure 49).

Figure 49: Example of Configure Recipients



Integrated Lights Out

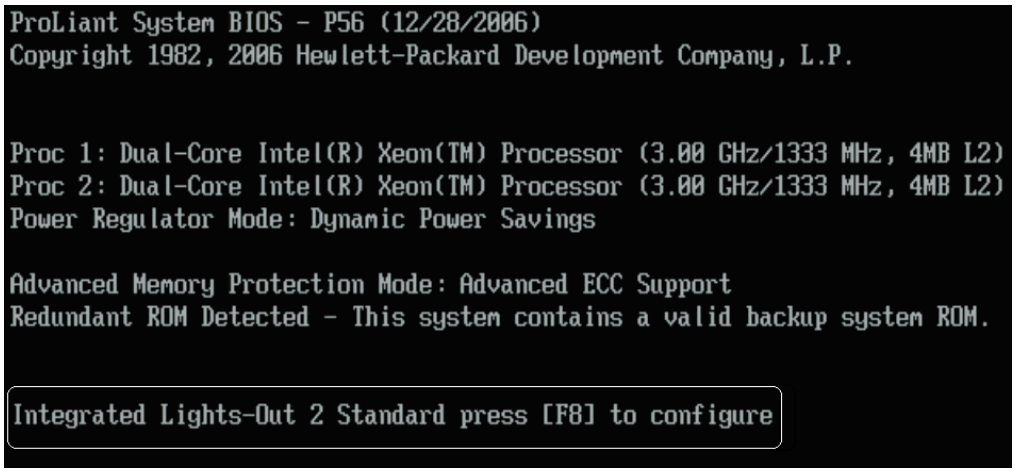
Integrated Lights Out (iLO) is a separate hardware component of the server that allows for increased remote administrative capabilities via a separate network connection. For example, the server can be turned on and diagnostic information can be viewed through the iLO console. For instructions on installing iLO and defining users, please see Appendix L: Implementing Integrated Lights Out of the *VBECS Installation Guide*. This section assumes you have already executed those instructions.

To install iLO

1) Attach the iLO ports on the back of each server to the VA network with an Ethernet cable.
2) Record the following information:
   - IP address for iLO port on cluster node 1: _____
   - IP address for iLO port on cluster node 1: _____
   - Default Gateway: _____
   - Subnet Mask: _____
   - DNS: _____
   - WINS (if applicable): _____

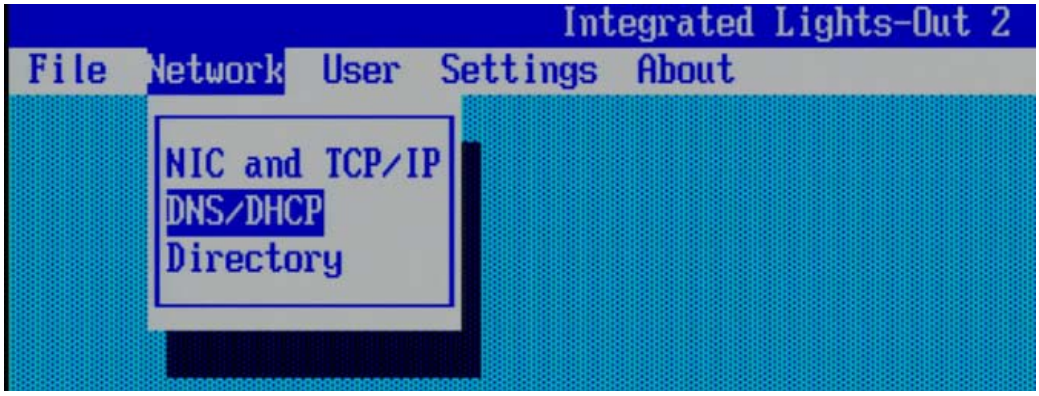
3) Log into cluster node 1 with your Windows ID. Reboot and watch the startup sequence. Press **F8** when prompted (Figure 50).

Figure 50: Press F8



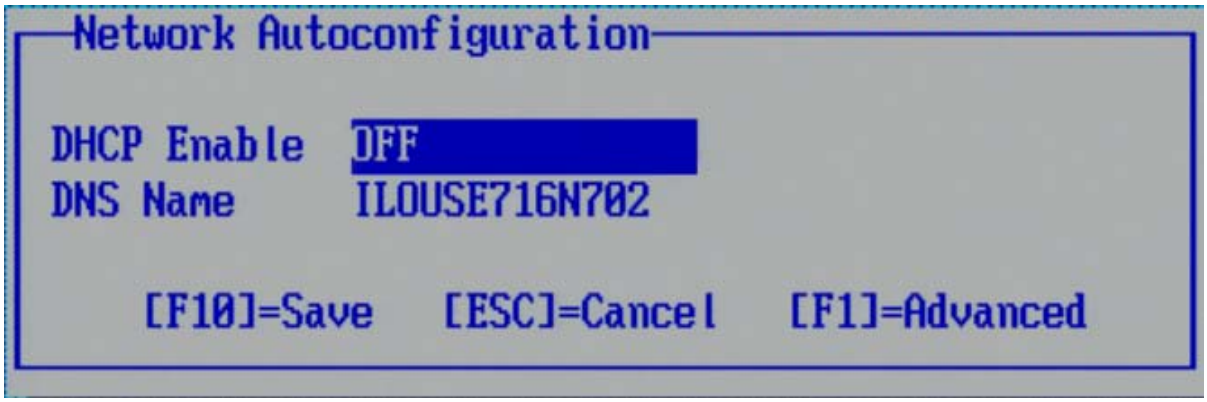
4) The iLO configuration screen will appear. With the arrow keys, select **Network**, **DNS/DHCP** and click **Enter** (Figure 51).

Figure 51: DNS/DHCP



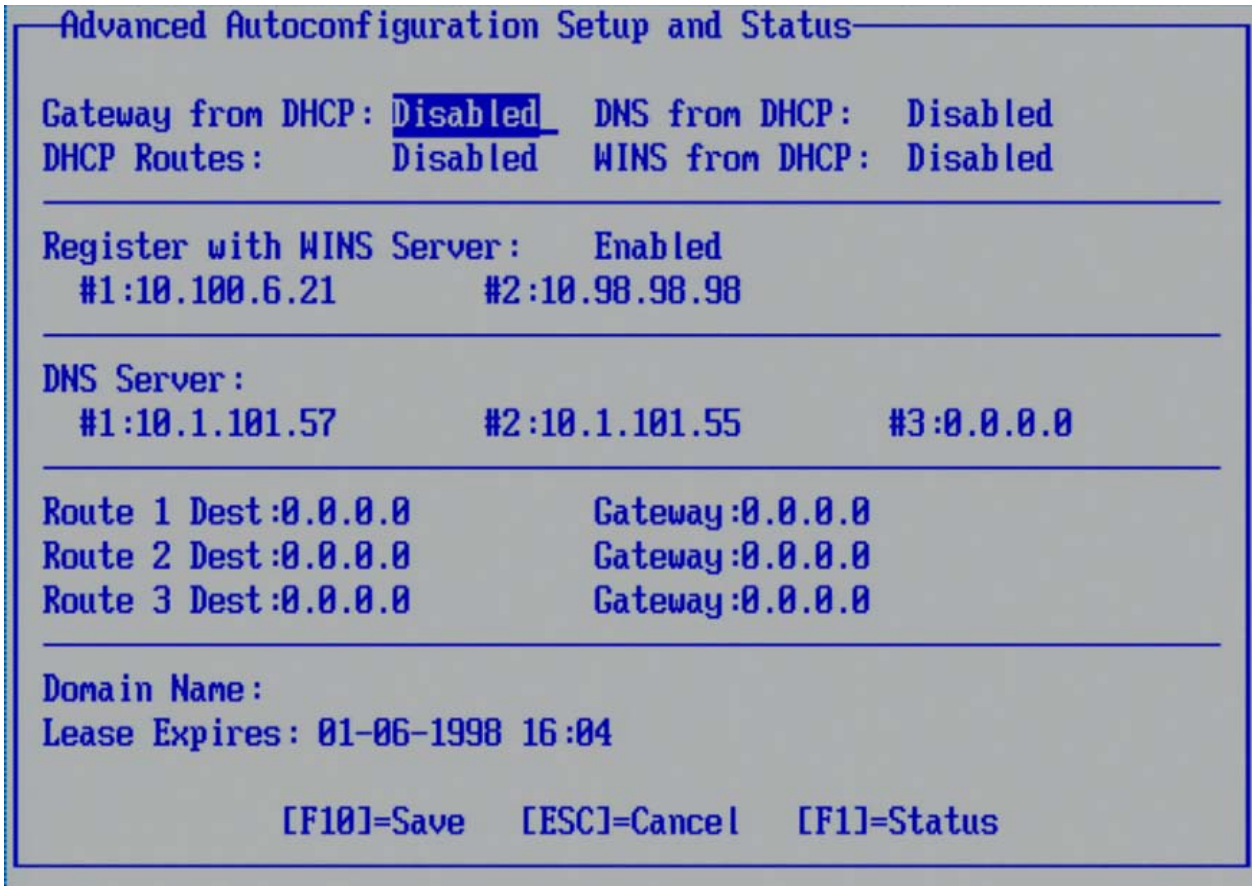
5) The Network Autoconfiguration screen launches. Turn off DHCP by pressing the space bar. Press **F1** to launch Advanced options (Figure 52).

Figure 52: Disable DHCP



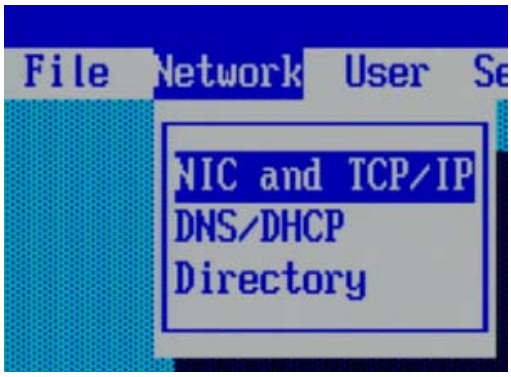
6) Disable DHCP in all four options in the top panel. Enter WINS from Step 2 (if applicable) addresses. Enter DNS server addresses from Step 2. Press **F10** to save (Figure 53).

Figure 53: Advanced



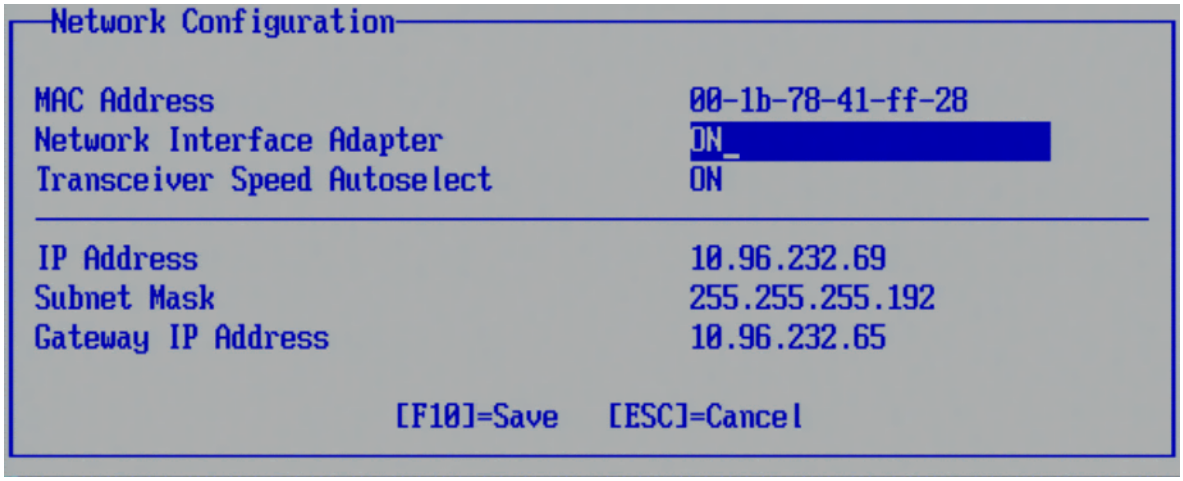
7) Select **Network**, **NIC and TCP/IP** and click **Enter** (Figure 54).

Figure 54: TCP/IP



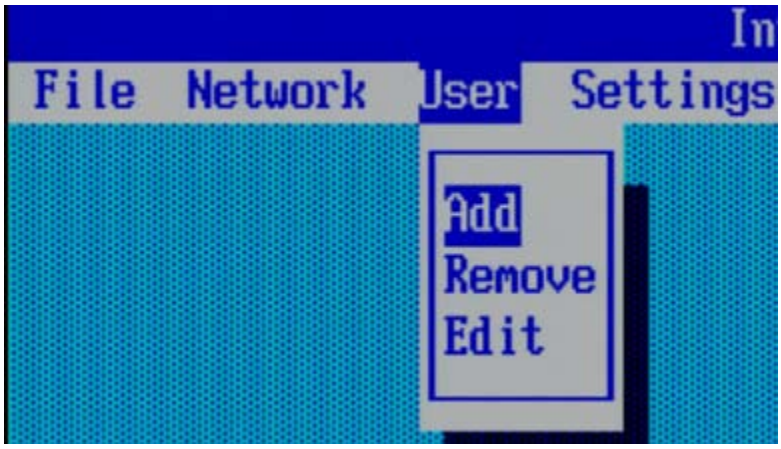
8) Enter a static IP address, subnet mask and default gateway (from Step 2). Press **F10** to save (Figure 55).

Figure 55: Network



9) Select **User**, **Add** (Figure 56).

Figure 56: Add user



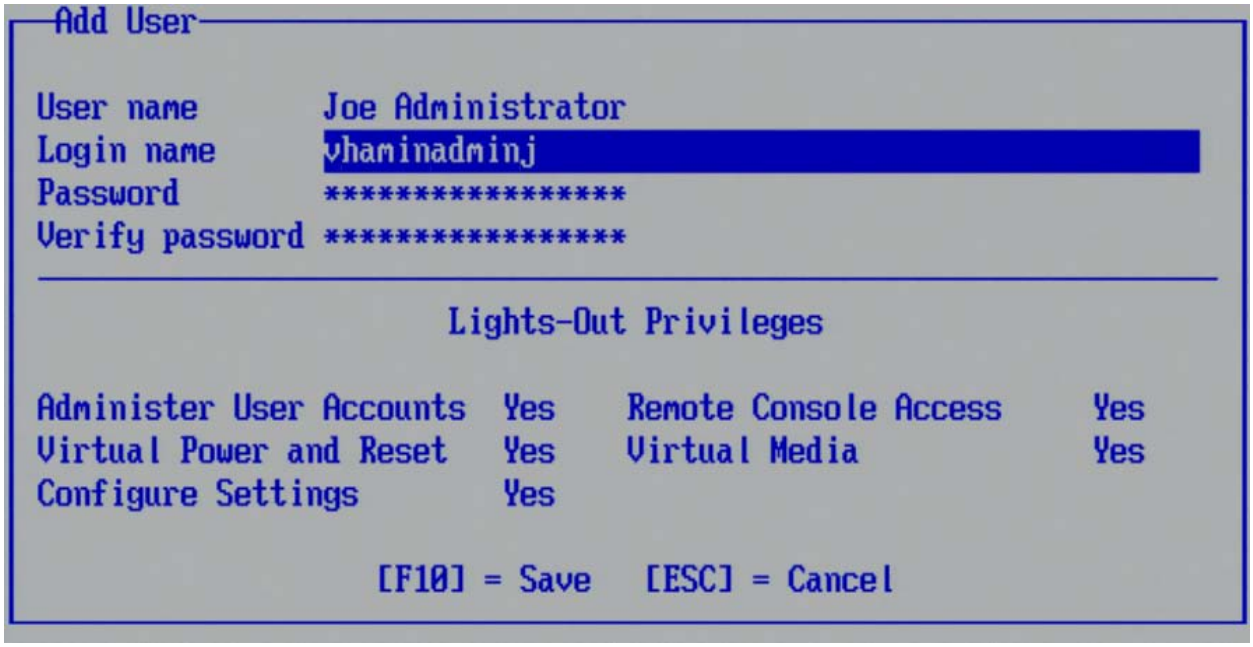
10) Enter the following (Figure 57):

- User name: Administrator's first and last name
- Login name: Network ID of the administrator
- Password: A complex password consisting of letters, number and special characters with a minimum length of eight.

Press **F10** to save.

Note that the iLO ID and password operate independently of the Windows credentials. Changing the Windows password will not affect the iLO password!

Figure 57: Add a user



11) Repeat Steps 9 and 10 to add additional administrators.
12) Press **Escape** to close the iLO configuration.
13) Repeat this entire section on Server 2.

To access iLO

1) From any computer in the VA Wide Area Network (WAN), launch a web browser and enter the iLO IP address of the server you would like to administer (Figure 58). Press **Enter**.

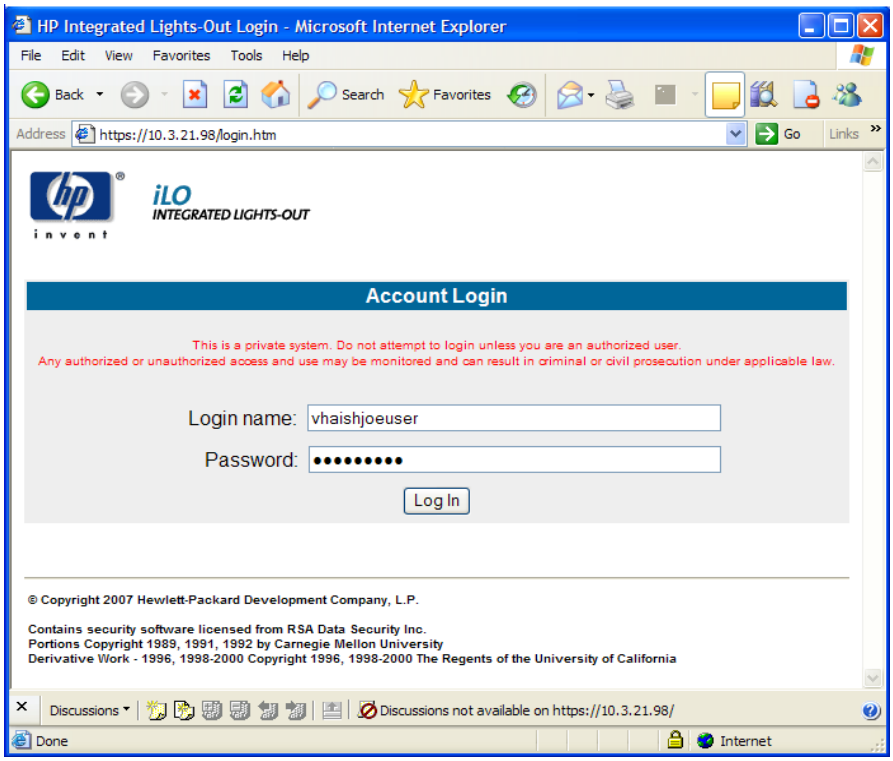
Figure 58: Example of Internet Explorer

2) Click **Yes** to proceed (Figure 59).

Figure 59: Example of Security Alert

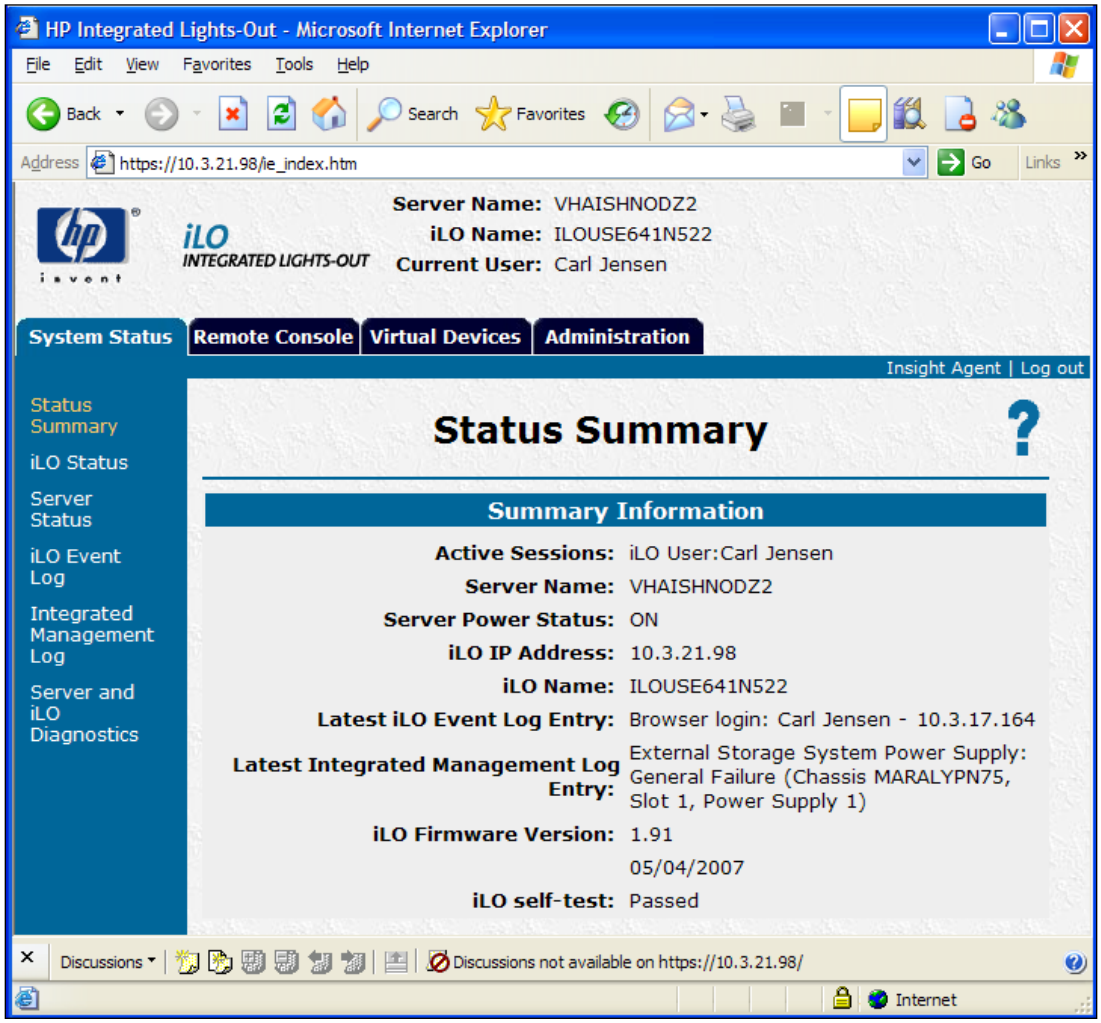
3) Enter your iLO username and password and click **Log In** (Figure 60).

Figure 60: Example of iLO Login



4) The iLO summary page is displayed (Figure 61).

Figure 61: Example of iLO Summary Page



System Status tab (Figure 61)

Brief explanation of iLO menu items:

- Status Summary: Basic iLO configuration
- iLO Status: Indicates current condition of iLO
- Server Status: Server configuration and status
- iLO Event Log: Events related to iLO
- Integrated Management Log: Log showing server events and error conditions
- Server and iLO Diagnostics: Results of automatic diagnostic tests

Remote Console tab

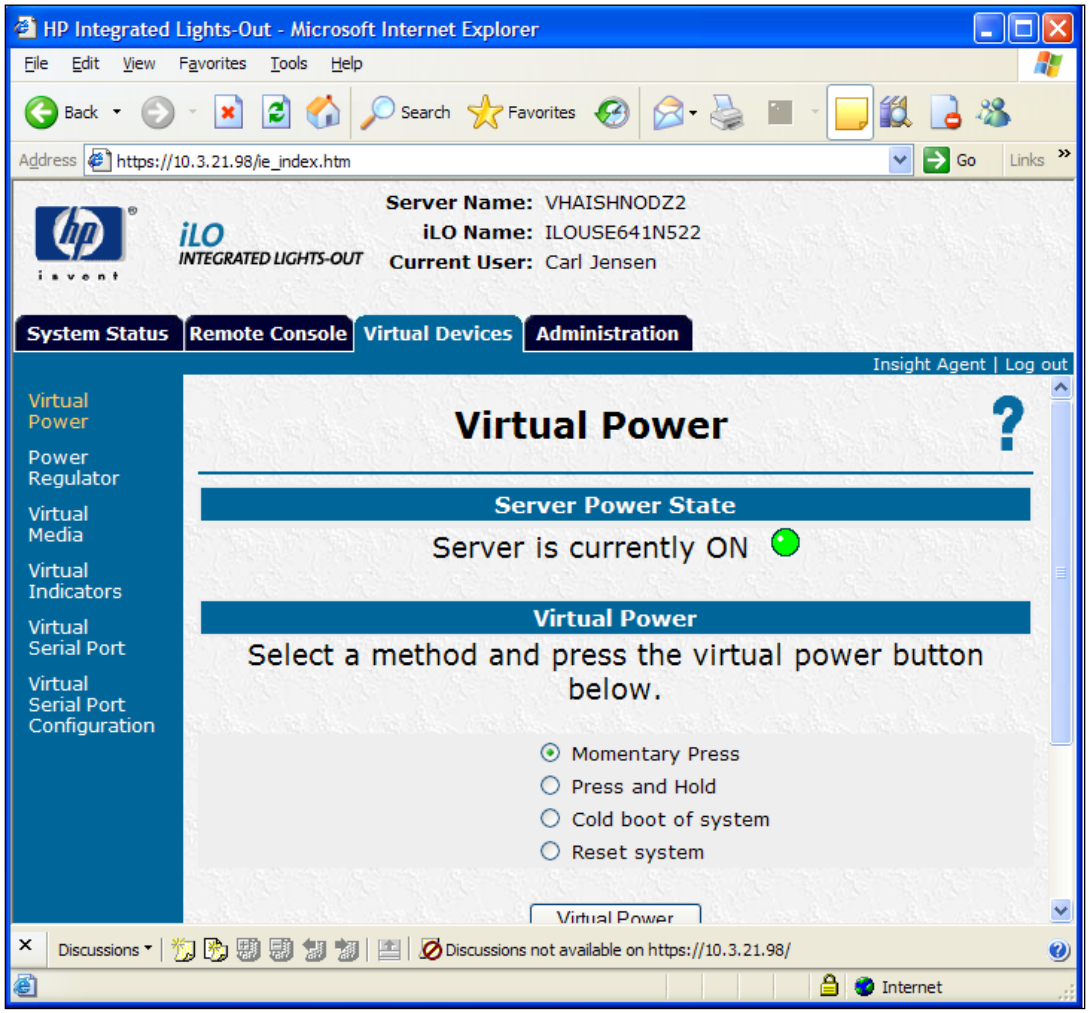
Options in this tab are unavailable at this time.

Virtual Devices tab (Figure 62)

Options in this tab allow you to accomplish tasks remotely that would normally require you to be at the server console.

- Virtual Power: Turn the server on or off
- Power Regulator: Adjust power settings
- Virtual Media: Connect to a drive on a remote machine
- Virtual Indicator: Control Server Unit ID light
- Virtual Serial Port: Virtual serial port status
- Virtual Serial Port Configuration: Virtual Serial Port Configuration

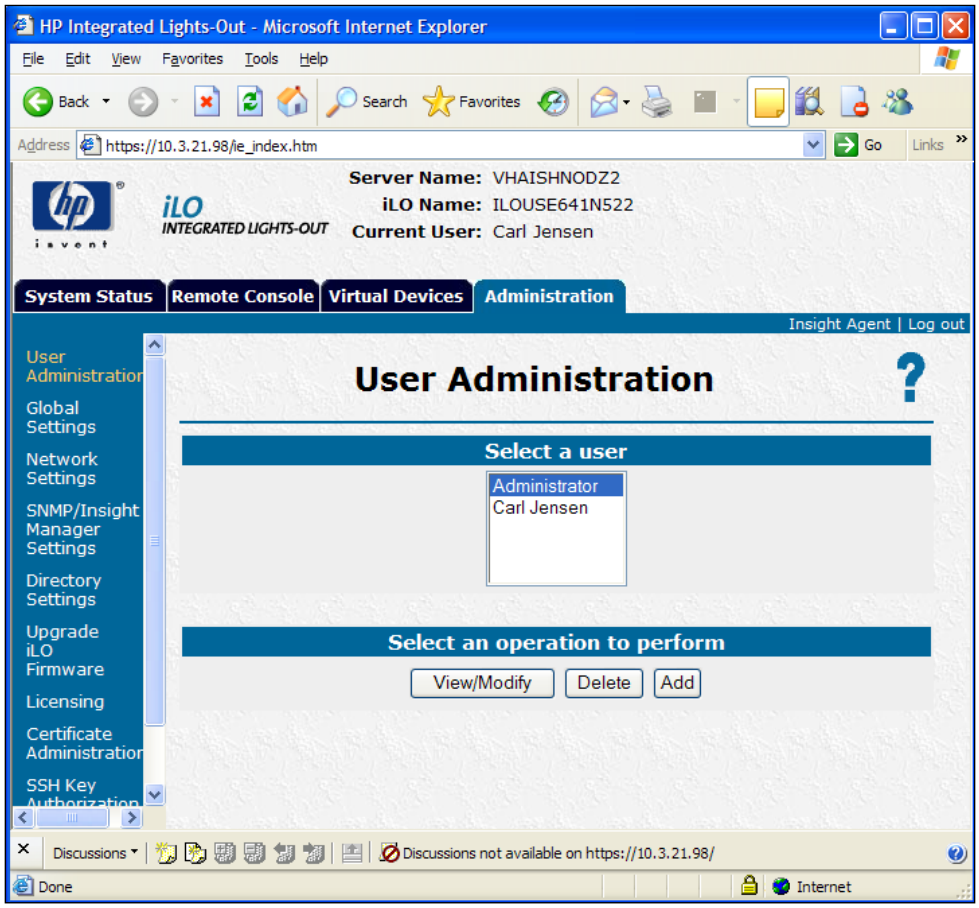
Figure 62: Example of Virtual Devices Tab



Administration tab

The **User Administration** item is used to configure iLO users (Figure 63). The other options are not being used at this time.

Figure 63: Example of Administration Tab



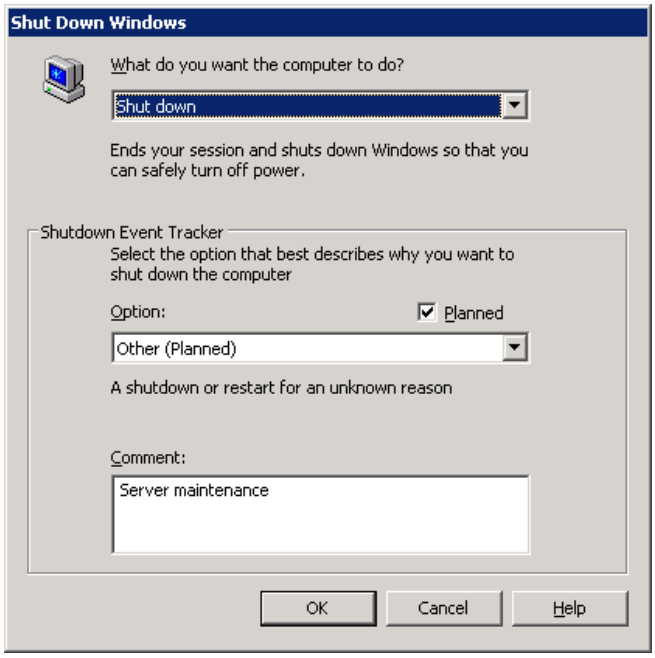
System Shut Down and Restart Instructions

The system may need to be shut down occasionally for maintenance. Because of the clustered nature of VBECS, the system has to be shut down in a specific order. Shutting down the system requires that a user be physically present at the VBECS system.

To shut down the system

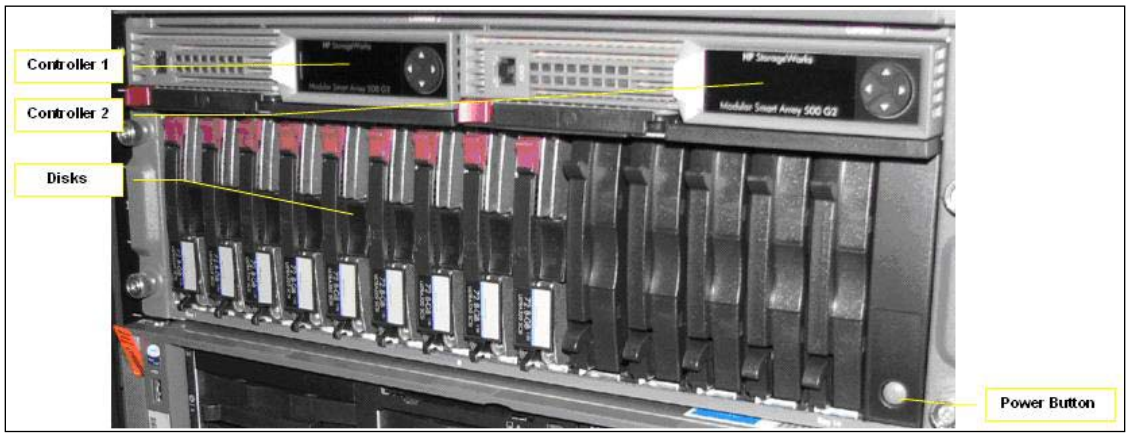
1) Log into either of the servers. Click **Start**, **Shut Down**. Enter a comment in the **Comment** field and click **OK** (Figure 64).

Figure 64: Example of Shut Down Window



2) After the first server is completely shut down, log into the other server and click **Start**, **Shut Down**. Enter a comment and click **OK** (Figure 64).
3) After both servers are completely shut down, the shared storage may be shut down by pressing the power button in the lower right corner (Figure 65).

Figure 65: Shared Disks



To start the system

1) Press the power button on the mass storage array. Wait until both controllers display a message of **Startup Complete** before continuing.
2) Start up one of the servers and allow it to come to the log on screen before continuing. This one will become the active node.
3) Start up the other server.

This page intentionally left blank.

Maintenance Operations

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

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

Configured options will be available at startup to perform maintenance operations.

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.

- VistALink is installed and running on the associated VistA system.
- The user is defined in VistA, and has a DUZ and Access and Verify Codes necessary to establish a VistA connection.
- The user has a valid Windows account and is defined as a member of the Active Directory (AD) domain group (see Add and Maintain Users in Active Directory).
- The user is defined as a member of the Windows Administrator group on the Active Directory domain group.
- The VBECS database is installed and operational.

Outcome

- Parameters necessary to establish the connection to VistA through VistALink are available to the main VBECS application, as defined in the Configure Interfaces option.
- VBECS-VistA HL7 interface parameters are defined in the Configure Interfaces option.
- One or more divisions are defined for use in VBECS in the Configure Divisions option.
- One or more divisions are activated as local facilities in VBECS in the Configure Divisions option.
- The System Administrator has VBECS login[1] access to all active divisions.
- VBECS users are defined and able to use VBECS in the Configure Users option.

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

Limitations and Restrictions

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

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

Additional Information

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

User Roles with Access to This Application

VBECS Administrator

Log into VBECS Administrator

User Action	VBECS Administrator
1. To log into VBECS Administrator, double-click (the **Remote Desktop Connection icon**). Enter your password.	Displays the user and server names.
2. Double-click the **VBECS Administrator icon**.	Opens VBECS Administrator. **NOTES** When the user logs into VBECS Administrator for the first time to set VistALink parameters, the system does not display the VistA Logon – Authorization screen. Continue at Step 6.
3. Continue to the VistA logon screen (Figure 66).	Opens the VistA Logon – Authorization screen. The user may log onto VistA or continue and log on as needed. **NOTES** The VistA logon screen is displayed only after initial setup of VistALink parameters.
4. Log onto VistA when VBECS Administrator starts up or at the invocation of any option that uses VistALink when VistALink is not connected.	Allows a user to log on by entering VistA Access and Verify Codes, separated by a semicolon (;), in the Access Code data entry field. When a user accesses an option that requires a VistALink connection and the connection becomes unavailable, allows the user to restore the connection. When a reconnection attempt is successful, VBECS closes the connection status window and returns to the desktop. The VistALink Connected icon in the status bar indicates a successful connection. When a reconnection attempt is unsuccessful, attempts to reconnect to VistALink until the user cancels.

User Action	VBECS Administrator
	NOTES When a user logs into VBECS Administrator, the connection to VistA is established through VistALink. When the VistALink connection is not restorable, VBECS Administrator displays a message that the requested use cannot be executed because VistALink is unavailable.
5. Enter the VistA Access and Verify Codes.	Verifies that user credentials for the VBECS Administrator and VistA Access and Verify Codes belong to the same user.
6. Continue working in VBECS Administrator (Figure 67).	Displays the main menu.

Figure 66: Example of VistA Logon

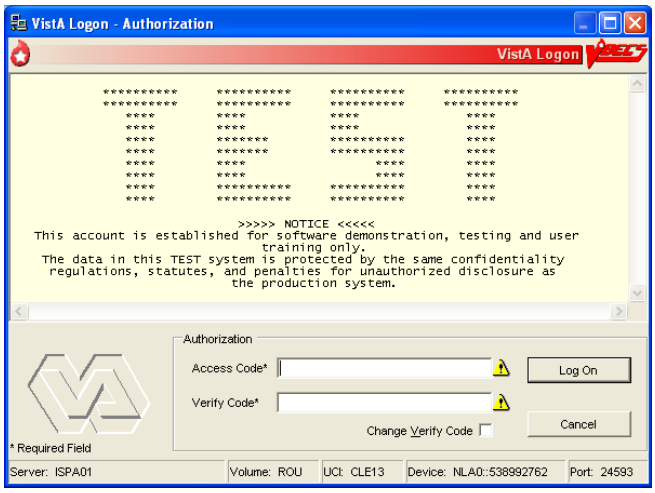
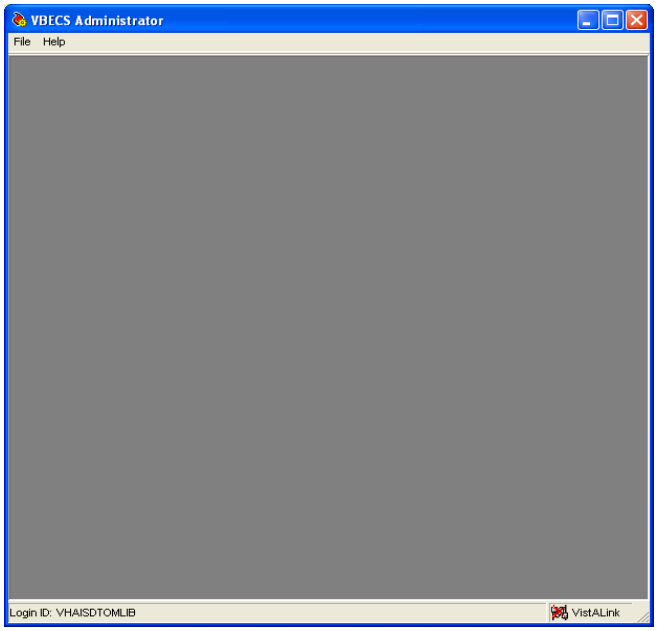


Figure 67: Example of VBECS Administrator



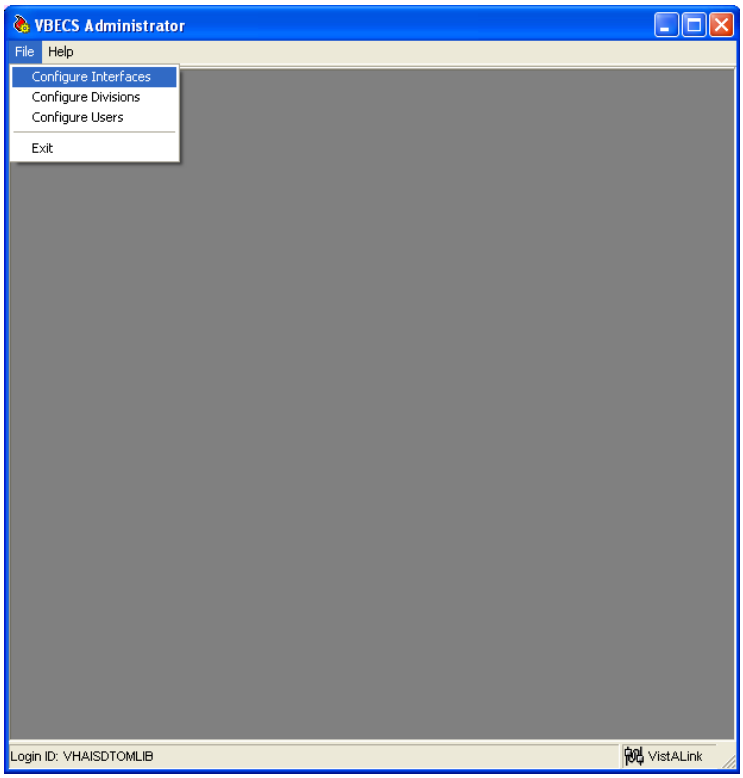
Configure Interfaces

Printer IP address must be added to the Access Control List (ACL).

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

User Action	VBECS Administrator
1. To configure VBECS VistALink and HL7 interface parameters, click **File** on the main menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces** (Figure 68).	Displays the VBECS Configure Interfaces dialog for data entry.

Figure 68: Example of Configure Interfaces

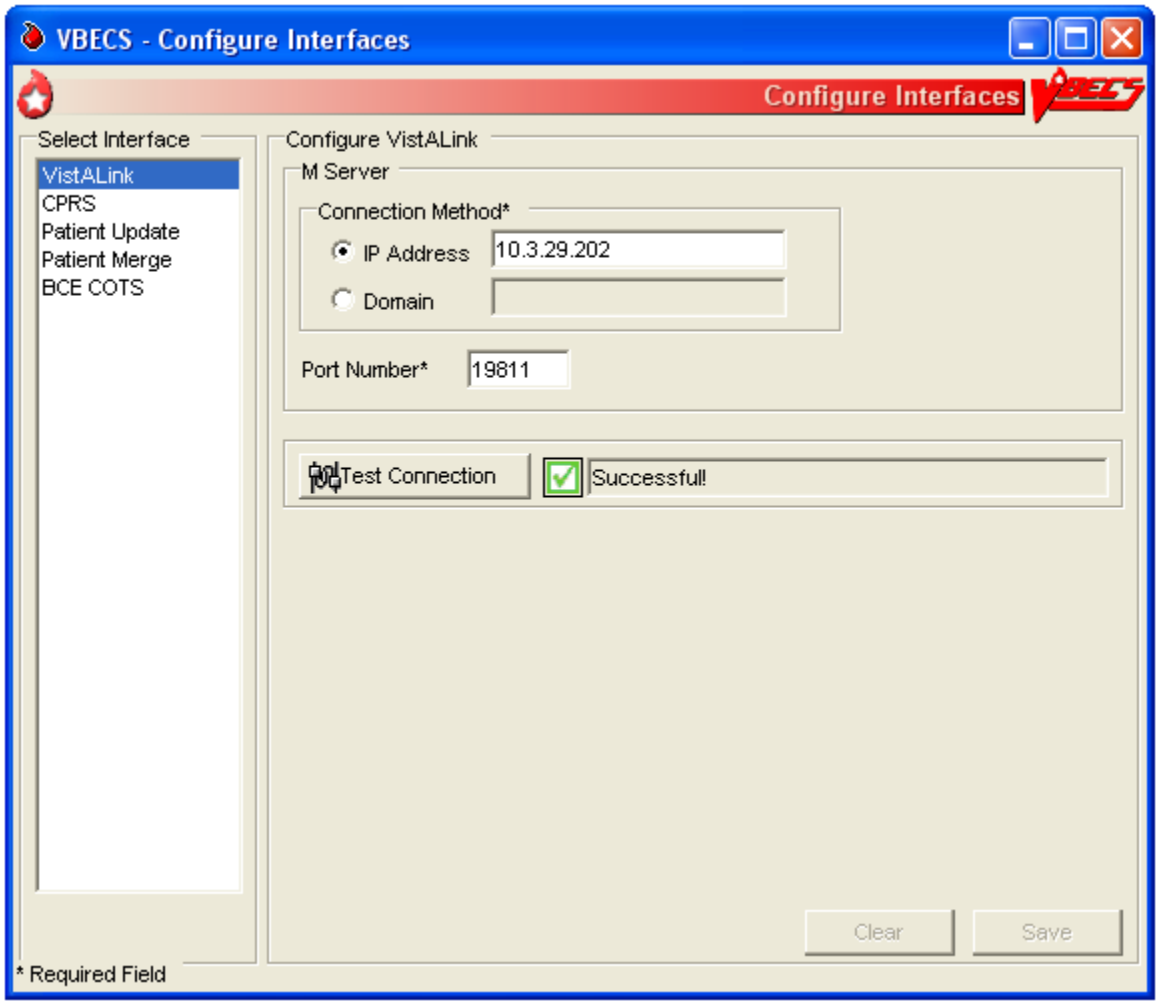


Configure VistALink Parameters

User Action	VBECS Administrator
1. To configure VistALink Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure VistALink parameters, select **VistALink** from the Select	Displays the Configure VistALink group and allows data entry of the IP address (or domain name) and port number of the VistA system VistALink

User Action	VBECS Administrator
Interface list box (Figure 69).	listener. Allows the user to test the VistALink connection parameters. **NOTES** The user may modify the IP address (or domain name) and port number, as required.
4. Enter a valid IP address (or domain name) and port number of the VistA system VistALink listener in the M Server group box fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1) or that the Domain field was filled in. Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VistALink IP address to which VBECS will direct messages. Refer to the Hardware Information section of Appendix B, row 6 for test, and row 7 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. The Port Number field represents the VistALink port number to which VBECS will direct messages. Refer to the Hardware Information section of Appendix B, row 8 for test, and row 9 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.
5. Click **Test Connection**. Capture a screen shot.	**NOTES** The Test Connection button is enabled only when valid entries exist in the IP Address (or Domain) and Port Number fields. If connection to the VistA system is successful, the VistA Logon – Authorization dialog is displayed and the user is required to enter valid Access and Verify Codes. If connection to the VistA system is unsuccessful, hover over the red square and a detailed error message will display.
6. Click **Save** to save changes.	Displays a confirmation dialog.
7. Click **Yes** to commit changes to the database.	Changes are saved to the VBECS database.

Figure 69: Example of Configure Interfaces: VistALink



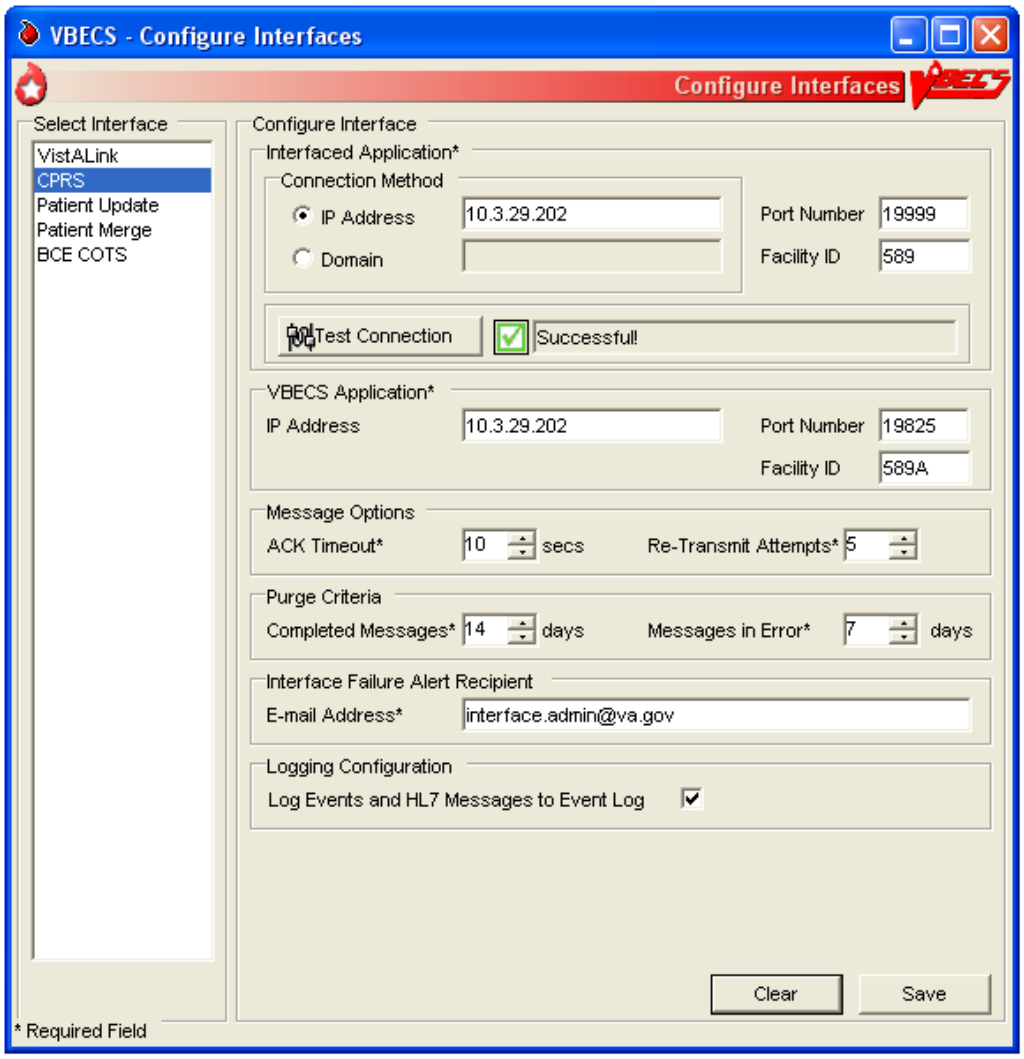
Configure CPRS HL7 Interface Parameters

User Action	VBECS Administrator
1. To configure CPRS HL7 Interface Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure CPRS HL7 Interface Parameters, select **CPRS** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 70).	Displays the Configure Interface group and allows data entry of HL7 interface-related parameters.
4. To configure Interfaced Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1) or that the Domain field was filled in. Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VistA CPRS IP address to which VBECS will direct messages. The Domain name field represents the fully qualified domain name to which VBECS will direct messages. Refer to the Hardware Information section of Appendix B, row 6 for test, and row 7 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. The Port Number field represents the VistA CPRS port number to which VBECS will direct messages. Refer to the Hardware Information section of Appendix B, row 10 for test, and row 11 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. The Facility ID is used in the MSH segment of the HL7 interface to help identify the system. This free-text field is usually set to the primary site's station number. Messaging to VBECS will fail if this Facility ID is not supplied.
5. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS cluster server IP address to which CPRS will direct messages. Refer to the Hardware Information section of Appendix B: Configuration Worksheet, row 1 in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. The Port Number field represents the VBECS cluster server port number to which CPRS will direct messages. Refer to the Hardware Information section of Appendix B, row 4 for test, and row 5 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.

User Action	VBECS Administrator
	The VBECS Facility ID must be different from the VistA. The Facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. Messaging to VBECS will fail if this Facility ID is not supplied. Refer to the Hardware Information section of Appendix B: Configuration Worksheet, rows 4 and 5 in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.
6. Click **Test Connection**.  Capture a screen shot.	**NOTES** The Test Connection button is enabled only when valid entries exist in the IP Address (or Domain) and Port Number fields. If connection to the VistA system is successful, the VistA Logon – Authorization dialog is displayed and the user is required to enter valid Access and Verify Codes. If connection to the VistA system is unsuccessful, hover over the red square and a detailed error message will display.
(This step is optional.) 7. To configure Message Options group parameters, enter an ACK timeout period and a number of retransmission attempts in the related data fields.	Validates that the ACK timeout period is a whole number from 1 to 999 (seconds) (default: 10). Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5).
(This step is optional.) 8. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields.	Validates that purge periods are whole numbers from 1 to 30 (days) (default: 7).
9. To configure the Interface Failure Alert Recipient group parameter, enter a valid **Administrator distribution (Active Directory) group** email address in the related data field.	Validates that the interface administrator's email address is entered e.g. firstname.lastname@va.gov. **NOTES** Only one email address can be entered. VBECS Windows Services uses this email address to notify local IRM support or the Blood Bank ADPAC when interface errors occur. Note: Use the support email address that was defined in the VBECS Installation Guide (Appendix E: Contact Information).
10. To configure the Logging Configuration group parameter, click or clear the **Log Events and HL7 Messages to Event Log** check box.  Capture a screen shot.	**NOTES** This check box indicates whether to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Cluster Server. (This is the only way to view VBECS HL7 messages on the VBECS server.)

User Action	VBECS Administrator
11. Click **Save** and **Yes** to confirm the save.	Changes are saved to the VBECS database.
12. To close the VBECS – Configure Interfaces dialog, click in the upper right corner.	Validates that the data was saved.

Figure 70: Example of Configure Interfaces: CPRS

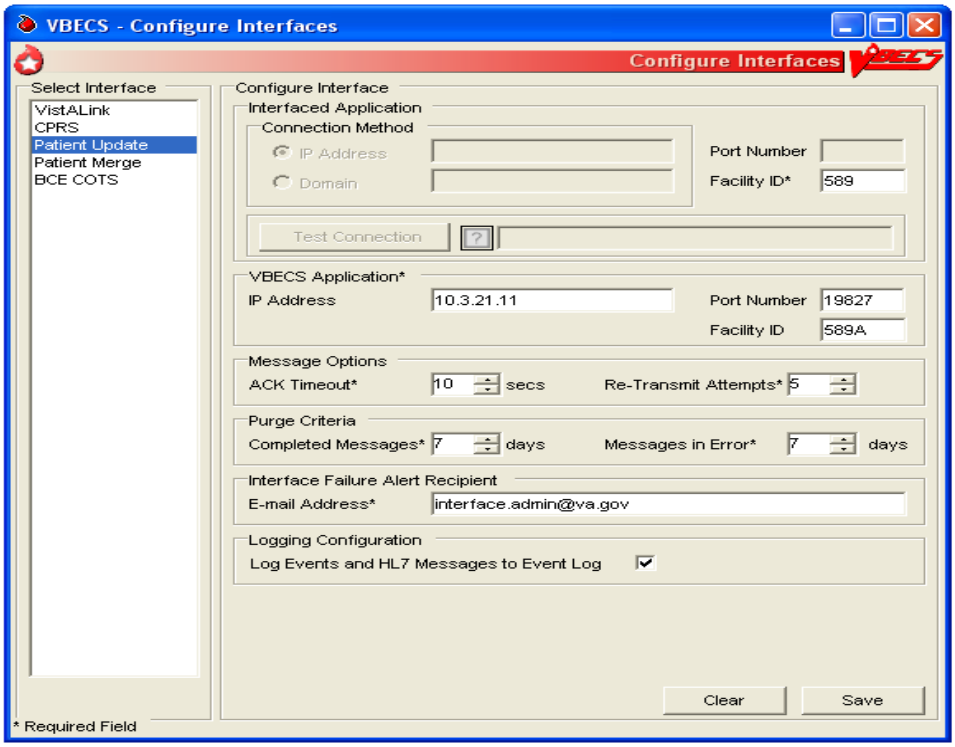


Configure Patient Update HL7 Interface Parameters

User Action	VBECS Administrator
1. To configure Patient Update HL7 Interface Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure Patient Update HL7 Interface Parameters, select **PatientUpdate** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 71).	Displays the Configure Interface group and allows data entry of HL7 interface-related parameters.
4. To configure Interfaced Application group parameters, enter a facility ID in the related data fields.	**NOTES** The IP Address and Port Number fields are disabled: no outbound messages are sent to VistA for this interface. The facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. Messaging to VBECS will fail if this Facility ID is not supplied.
5. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS cluster server IP address to which VistA will direct messages. Refer to the Hardware Information section of Appendix B: Configuration Worksheet, row 1 in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. The Port Number field represents the VBECS cluster server port number to which VistA will direct messages. Refer to the Hardware Information section of Appendix B, row 4 for test, and row 5 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.
(This step is optional.) 6. To configure Message Options group parameters, enter an ACK Timeout period and number of retransmission attempts in the related data fields.	Validates that the ACK timeout period is a whole number from 1 to 999 (seconds) (default: 10). Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5).
(This step is optional.) 7. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database	Validates that the purge periods are whole numbers from 1 to 30 (days) (default: 7).

User Action	VBECS Administrator
in the related data fields.	
8. To configure the Interface Failure Alert Recipient group parameter, enter a valid **Administrator distribution (Active Directory) group** email address in the related data field.	Validates that the interface administrator's email address is entered e.g. firstname.lastname@va.gov. **NOTES** Only one email address can be entered. VBECS Windows Services uses this email address to notify local IRM support or the Blood Bank ADPAC when interface errors occur. Note: Use the support email address that was defined in the VBECS Installation Guide (Appendix E: Contact Information).
9. To configure the Logging Configuration group parameter, click or clear **the Log Events and HL7 Messages to Event Log** check box. Capture a screen shot.	**NOTES** This check box indicates whether to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Cluster Server. (This is the only way to view VBECS HL7 messages on the VBECS server.)
10. Click **Save** and **Yes** to confirm the save.	Changes are saved to the VBECS database.
11. To close the VBECS – Configure Interfaces dialog, click in the upper right corner.	Validates that the data was previously saved.

Figure 71: Example of Configure Interfaces: PatientUpdate

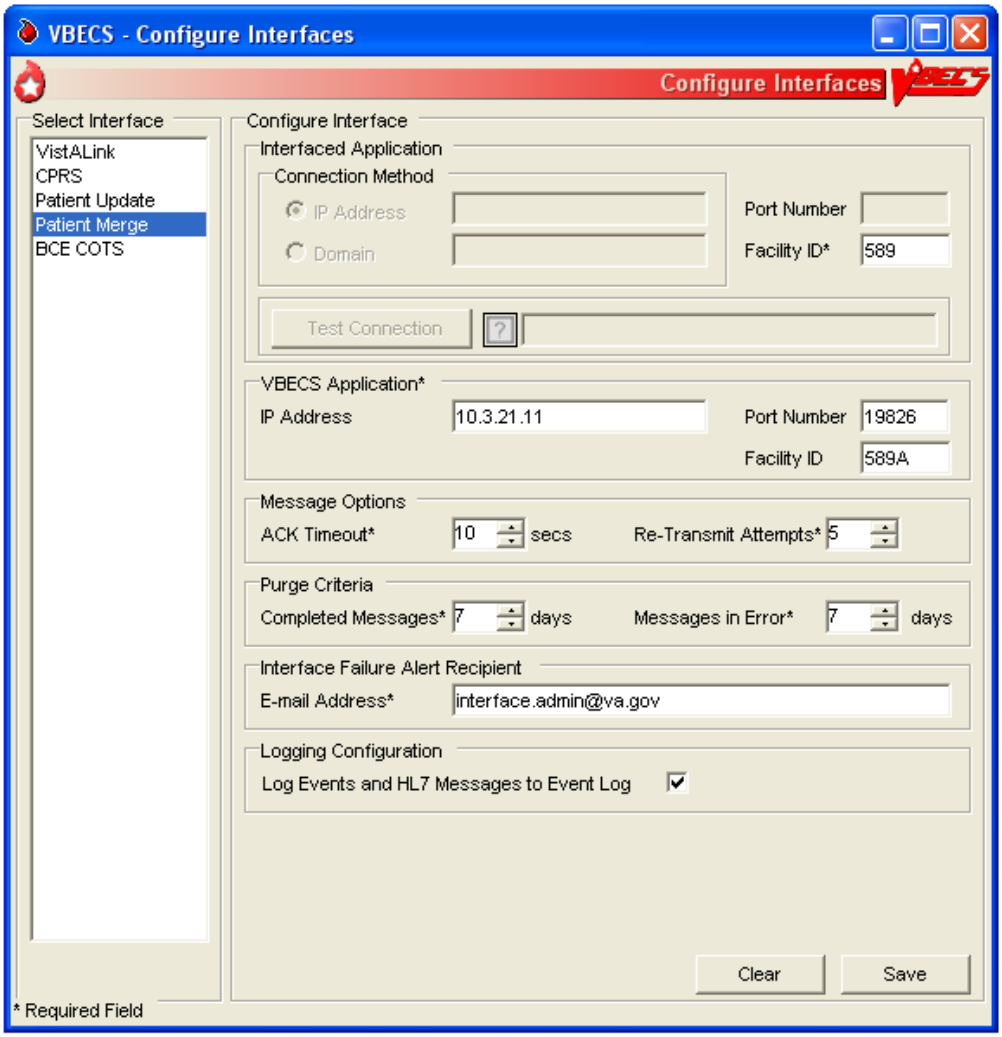


Configure Patient Merge HL7 Interface Parameters

User Action	VBECS Administrator
1. To configure Patient Merge HL7 Interface Parameters, click **File** on the menu of the VBECS Administrator software.	Displays the menu options used to configure VBECS.
2. Click **Configure Interfaces**.	Displays the VBECS Configure Interfaces dialog for data entry.
3. To configure Patient Merge HL7 Interface Parameters, select **PatientMerge** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 72).	Displays the Configure Interfaces group and allows data entry of HL7 interface-related parameters.
4. To configure Interfaced Application group parameters, enter a facility ID in the related data field.	**NOTES** The IP Address and Port Number fields are disabled: no outbound messages are sent to VistA for this interface. The facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. Messaging to VBECS will fail if this Facility ID is not supplied.
5. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS cluster server IP address to which VistA will direct messages. Refer to the Hardware Information section of Appendix B, row 1: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. The Port Number field represents the VBECS cluster server port number to which VistA will direct messages. Refer to the Hardware Information section of Appendix B, row 4 for test, and row 5 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.
(This step is optional.) 6. To configure Message Options group parameters, enter an ACK Timeout period and number of retransmission attempts in the related data fields.	Validates that the ACK Timeout period is a whole number from 1 to 999 (seconds) (default: 10). Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5).
(This step is optional.) 7. To configure Purge Criteria group parameters, enter the number of days after which completed	Validates that the purge periods are whole numbers from 1 to 30 (days) (default: 7).

User Action	VBECS Administrator
messages and messages in error are to be purged from the database in the related data fields.	
8. To configure the Interface Failure Alert Recipient group parameter, enter a valid **Administrator distribution (Active Directory) group** email address in the related data field.	Validates that the interface administrator's email address is entered e.g. firstname.lastname@va.gov. **NOTES** Only one email address can be entered. Create one distribution group and add members to the group. VBECS Windows Services uses this email address to notify local IRM support or the Blood Bank ADPAC when interface errors occur. Note: Use the support email address that was defined in the VBECS Installation Guide (Appendix E: Contact Information).
9. To configure the Logging Configuration group parameter, click or clear the **Log Events and HL7 Messages to Event Log** check box.  Capture a screen shot.	**NOTES** This check box indicates whether to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Cluster Server. (This is the only way to view VBECS HL7 messages on the VBECS server.)
10. Click **Save** and **Yes** to confirm the save.	Changes are saved to the VBECS database.
11. To close the VBECS – Configure Interfaces dialog, click  in the upper right corner.	Validates that the data was previously saved.

Figure 72: Example of Configure Interfaces: PatientMerge



Configure BCE COTS Interface Parameters

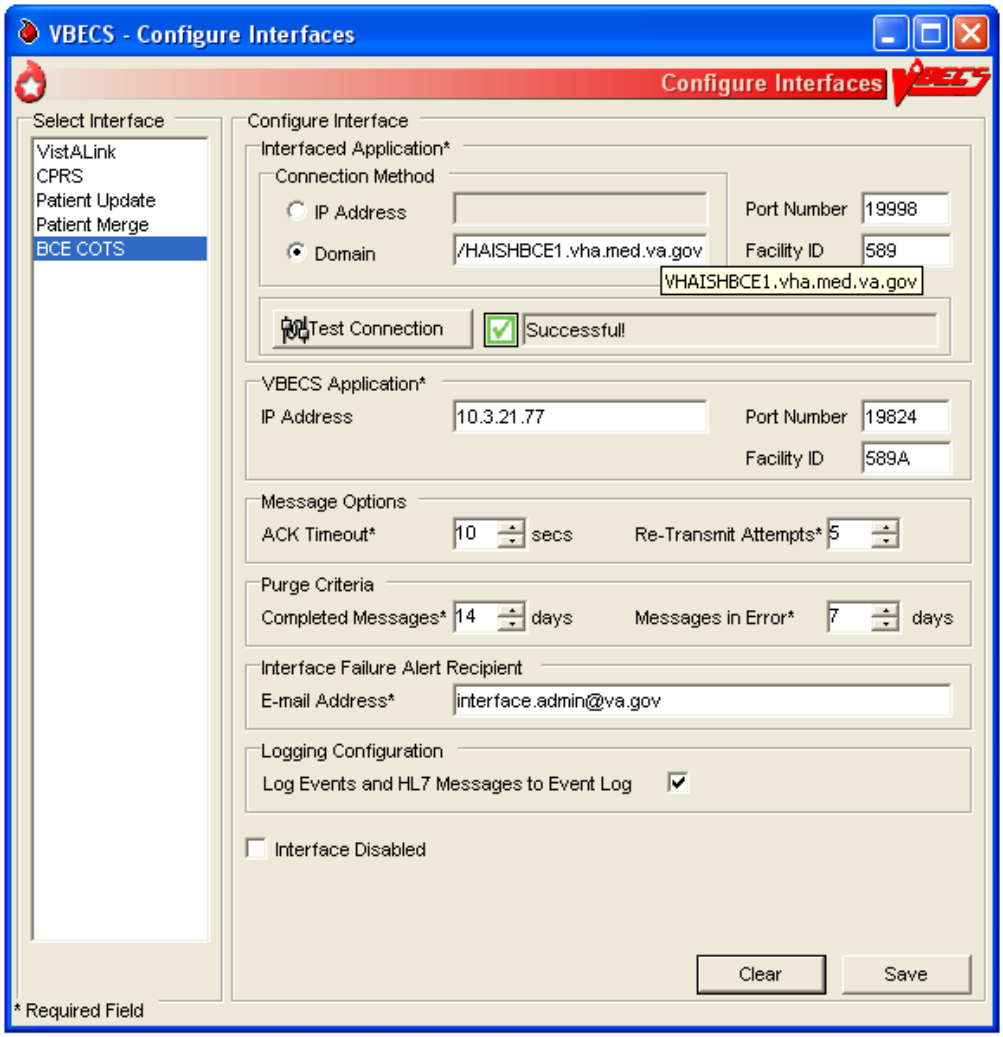
Do not configure this interface until the BCE COTS software is available.

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

User Action	VBECS Administrator
dialog (Figure 73).	
4. To configure Interfaced Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1) or that the Domain field was filled in. Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the BCE COTS IP address to which VBECS will direct messages. The Domain name field represents the fully-qualified domain name to which VBECS will direct messages. The Port Number field represents the BCE COTS port number to which VBECS will direct messages. The Facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field that is usually set to the primary site's station number. This field is typically validated only when using an interface engine to assist with routing HL7 messages. The VBECS HL7 interfaces do not currently require the use of an interface engine. Refer to the Hardware Information section of Appendix B: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.
5. Click **Test Connection**.	**NOTES** The Test Connection button is enabled only when valid entries exist in the IP Address (or Domain) and Port Number fields. If connection to the VistA system is successful, the VistA Logon – Authorization dialog is displayed and the user is required to enter valid Access and Verify Codes.
6. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields.	Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1). Validates that the port number is a whole number from 1024 to 65535. **NOTES** The IP Address field represents the VBECS cluster server IP address to which BCE COTS will direct messages. The Port Number field represents the VBECS cluster server port number to which BCE COTS will direct messages. The facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. This field is validated only when using an interface engine to assist with routing HL7 messages. The VBECS HL7 interfaces do not require the use of an interface engine. Refer to the Hardware Information section of Appendix B: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.

User Action	VBECS Administrator
(This step is optional.) 7. To configure Message Options group parameters, enter an ACK timeout period and a number of retransmission attempts in the related data fields.	Validates that the ACK timeout period is a whole number from 1 to 999 (seconds) (default: 10). Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5).
(This step is optional.) 8. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields.	Validates that purge periods are whole numbers from 1 to 30 (days) (default: 7). Note: Error message purging functionality will be added in a future release.
9. To configure the Interface Failure Alert Recipient group parameter, enter a valid **Administrator distribution (Active Directory) group** email address in the related data field.	Validates that the interface administrator's email address is entered e.g. firstname.lastname@va.gov. **NOTES** Only one email address can be entered. Create one distribution group and add members to the group. VBECS Windows Services uses this email address to notify local IRM support or the Blood Bank ADPAC when interface errors occur. Note: Use the support email address that was defined in the VBECS Installation Guide (Appendix E: Contact Information).
10. To configure the Logging Configuration group parameter, click or clear the **Log Events and HL7 Messages to Event Log** check box.  Capture a screen shot.	**NOTES** This check box indicates whether or not to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Cluster Server. (This is the only way to view VBECS HL7 messages on the VBECS server.)
11. To enable the BCE COTS interface the **Interface Disabled** check box must be unchecked.	**NOTES** The BCE COTS interface is enabled\disabled via this check box. When enabled the fields on the screen become enabled for the BCE COTS interface. When disabled, no BCE messages will be sent or received from BCE. When enabled, the BCE interface will still not receive any BCE messages until you stop and start the VBECS CPRS HL7 Client Monitor service.
12. Click **Save** and **Yes** to confirm the save.	Changes are saved to the VBECS database.
13. To close the VBECS – Configure Interfaces dialog, click  in the upper right corner.	Validates that the data was saved.

Figure 73: Example of Configure Interfaces: BCE COTS



Configure Divisions

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

Assumptions

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

Outcome

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

Limitations and Restrictions

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

Additional Information

- A VBECS Administrator/Supervisor may further configure:
  - VBECS users in Update User Roles.
  - VBECS division parameters in Configure Division, Product Modifications, and Configure Testing.
- The user must log onto VistA using Access and Verify Codes.

User Roles with Access to This Option

System Administrator

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

Add and Maintain Divisions

The user defines and maintains division attributes.

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

User Action	VBECS Administrator
1. To add and maintain divisions in VBECS, click **File** on the main menu of the VBECS Administrator software.	• Displays the menu options used to configure VBECS.
2. Select **Configure Divisions** (Figure 74).	• Displays the Configure Division dialog and allows entry of division parameters.
3. To edit a defined division, click the **Division Identification** tab (Figure 75). Select a division code or name from the drop-down menu or, to configure a new division, click the **ellipsis** button. Select a division from the list (Figure 76).	**NOTES** The user may not edit the division code or name. A division may be full service (default) or transfusion only. When a unit not in a final status exists, a user may not change the type of transfusion service. When a division is transfusion only, VBECS disables electronic crossmatch. When a division changes from full service to transfusion only, units already in inventory are not restricted to patients and must be returned to the blood center. When a division changes from transfusion only to full service, inventory units are restricted to patients without ABO/Rh confirmation. The facility must decide how to handle this existing inventory. VBECS prevents the user from changing a division from full service to transfusion only or from transfusion only to full service when there are open or partially completed worksheets or processes in the division. The Division Name and Division Code are identified in the VistA INSTITUTION file (#4). The Division Name stored in VBECS is the INSTITUTION file NAME field (#.01); the Division Code stored in VBECS is the STATION NUMBER field (#99). When either value change in VistA, rerun these steps to update the VBECS database with the current values from VistA.

User Action	VBECS Administrator
4. To receive orders from VistA Institutions to the selected Division, check the Map orders from VistA institutions check box. Click the Active checkbox for each institution that applies.	**NOTES** Changes made to institution mappings require a restart of the VBECS HL7 Multi Listener service. For more information, see Table 8 in the VBECS Windows Services section. One or more VistA institutions from the list of valid institutions retrieved from VistA may be associated with the selected VBECS division from the list of valid institutions retrieved from VistA. A VistA institution may be associated with only one VBECS division. A VistA institution defined as a VBECS division is not eligible for selection as an associated institution to a different VBECS division. To associate additional institutions, enable an optional VistALink query to retrieve a list of all institutions associated with the VistA site that are currently defined within the VistA database but not in the selected VBECS division. VBECS displays the list to the user for selection.
5. Select the FDA Registered Facility associated with the division or, to search for the facility by name or FDA Registration Number, click the **ellipsis** button (Figure 75).	• Allows the user to associate a division with a facility from the National Facility Table. **NOTES** The user must associate a division with a facility from the National Facility Table. If there is no matching facility, VBECS Administrator asks the user to contact the VA Service Desk. When this occurs, wait for customer support to respond or, to continue establishing a division, select and configure any facility from the National Facility Table. When the configuration is complete, use the Local Facilities option in VBECS to define the local facility that matches the information missing from the National Facility Table. Return to Configure Divisions to re-associate your division with the newly entered local facility. When a division is configured, VBECS displays, “I certify that the blood products listed were properly maintained, in accordance with the Code of Federal Regulations, while in storage at this institution. Components were inspected when packed for shipment and found to be satisfactory in color and appearance.”
6. Select the VistA Lab Blood Bank Accession Area associated with the selected division from the drop-down menu (Figure 75).	**NOTES** The Lab package uses the Accession Area to track blood bank-related workload for the division.
7. Enter the desired number of minutes in the Lock Inactivity Timeout field.	• Allows the user to set the lock inactivity timeout period (5 to 15 minutes) (default: 5 minutes). **NOTES** The lock inactivity timeout period specifies how long a user can

User Action	VBECS Administrator
	be idle and in control of data being edited. VBECS warns the user 60 seconds before the lock inactivity period expires that he will lose priority for the data. When he responds within 60 seconds, VBECS clears the warning and resets the lock activity timer. Otherwise, VBECS informs him that his lock was released and he must reenter his changes. VBECS uses optimistic and pessimistic locking to prevent data corruption. If a user attempts to edit data locked by another user, VBECS alerts him that the record is in use and prevents access (pessimistic locking). If more than one user attempts to change data simultaneously, VBECS accepts only the first update and warns the other users that the record changed (optimistic locking, which is non-configurable and a fail-safe to pessimistic locking).
8. To activate or inactivate the division, click or clear the **Active VBECS Division?** check box (Figure 75). Capture a screen shot.	• When the user saves a previously active division as inactive, inactivates user roles for that division. **NOTES** The system will not allow the user to activate a division that has orders mapped to another VBECS division. VBECS displays, "Unable to activate. The VBECS division currently has orders mapped to another VBECS division." The system will not allow the user to inactivate a division that has orders mapped to it. VBECS displays, "Unable to inactivate. This VBECS division currently has orders mapped to it. Release this mapping prior to inactivation,"
9. Click the **Service Type tab**. Click the **Full-Service Facility** or **Transfusion-Only Facility** radio button (Figure 78). Capture a screen shot.	• Allows the user to identify the facility as full service or transfusion only. **NOTES** When the division changes from full service to transfusion only or from transfusion only to full service, information must be in a final state. VBECS does not check for pending orders or active units in inventory, so there is a risk of corrupting information. There is a risk of having unconfirmed units available for transfusion if any are issued.
10. Click the **Printers tab**. Clear or click the **Division Uses Label Printer** check box. Edit the COM port number and/or the TCP port number. Enter the IP address (Figure 79). Capture a screen shot.	• Allows the user to enter the COM and TCP port numbers and the IP address for the label printer. • Allows the user to select the default printer for the division when more than one printer is installed on the system. **NOTES** Standard values for COM and TCP ports: COM = 2 TCP = 9100
11. Click the **Time Zone tab**.	• Allows the user to set the time zone and daylight saving parameters.

User Action	VBECS Administrator
Select a time zone. In the Daylight Savings field, select **US Standard DST**, **Do not observe DST**, or **Custom DST**. Enter start and end dates for custom DST (Figure 80). Capture a screen shot. Click **Save**.	
12. Click **Save** and **OK** to commit the changes or add the new division to the VBECS database.	• Commits changes and additions to the database. **NOTES** Multidivisional sites must repeat Steps 3–11 for each division. The VBECS Administrator/Supervisor who configured the divisions must add himself as a user to all divisions to enable the functionality of canned comments in the VBECS system.
13. To close the **VBECS** – **Configure Divisions** dialog, click in the upper right corner.	

Figure 74: Example of Configure Divisions

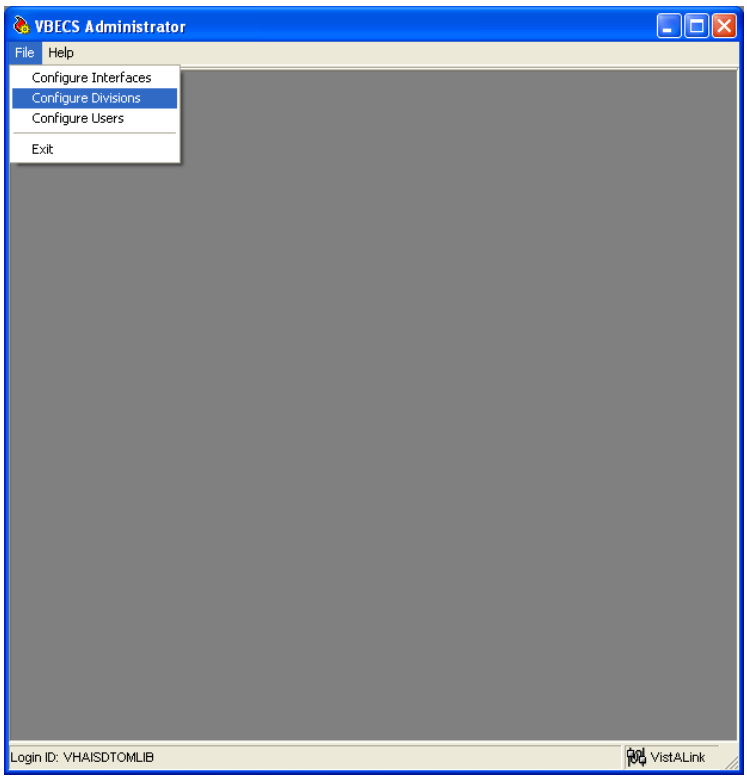


Figure 75: Example of Configure Division: Division Identification

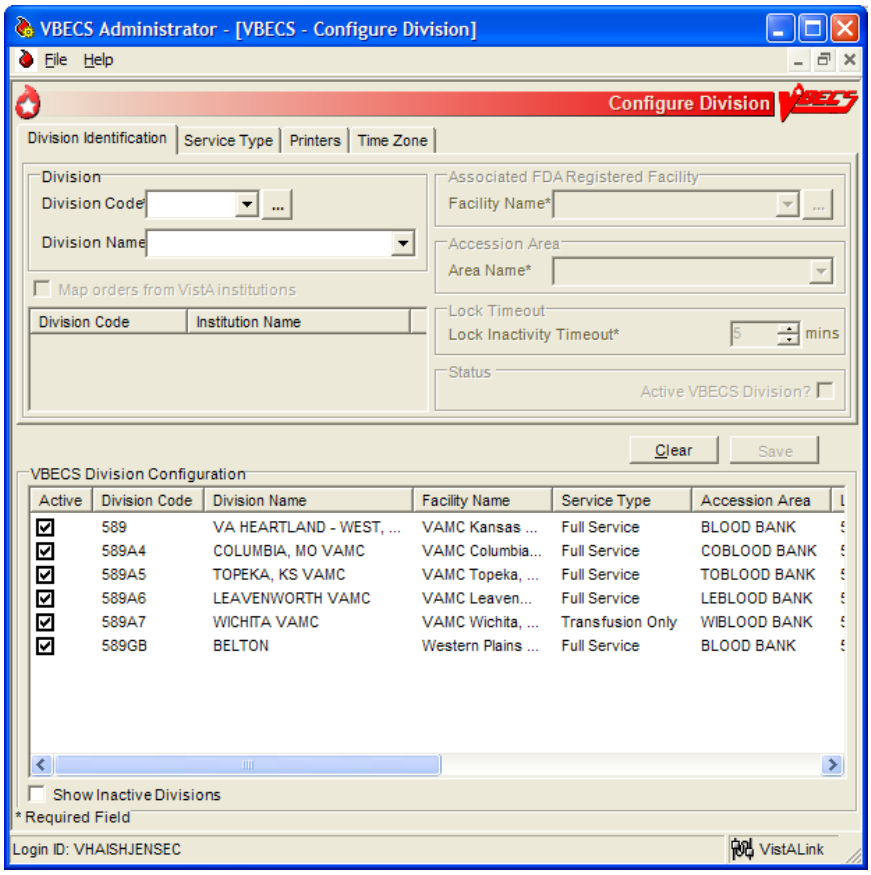


Figure 76: Example of Select VistA Divisions

Figure 77: Example of Facility Search

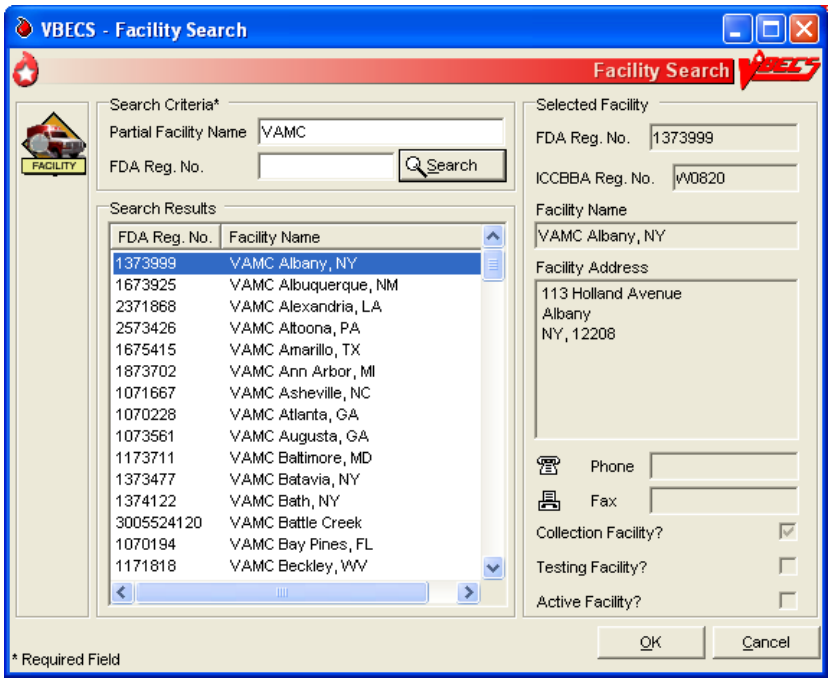


Figure 78: Example of Configure Division: Service Type

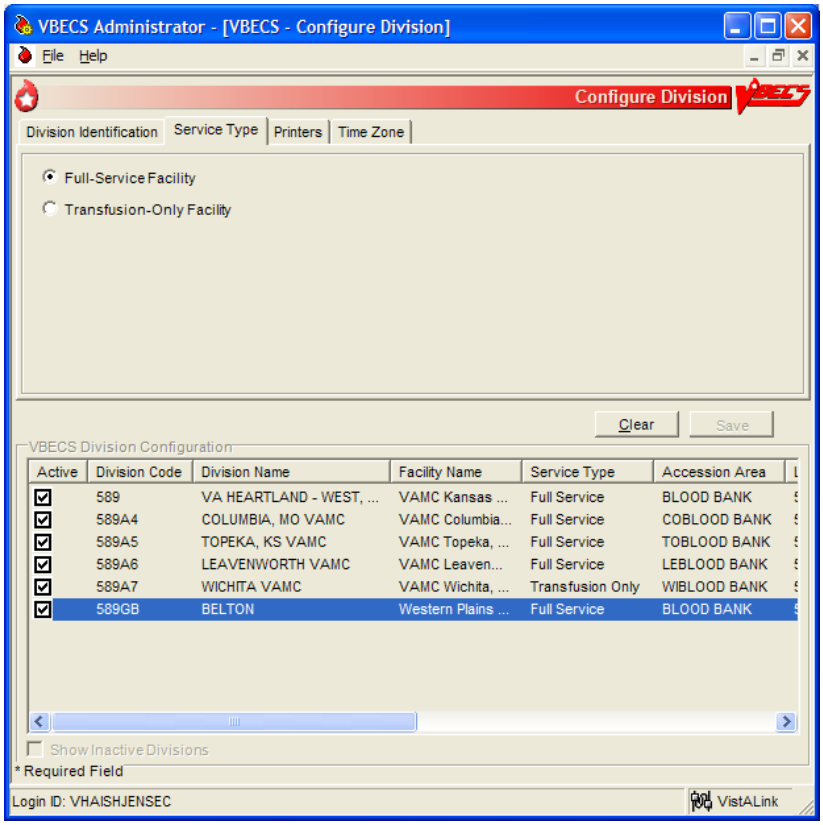


Figure 79: Example of Configure Division: Label Printing

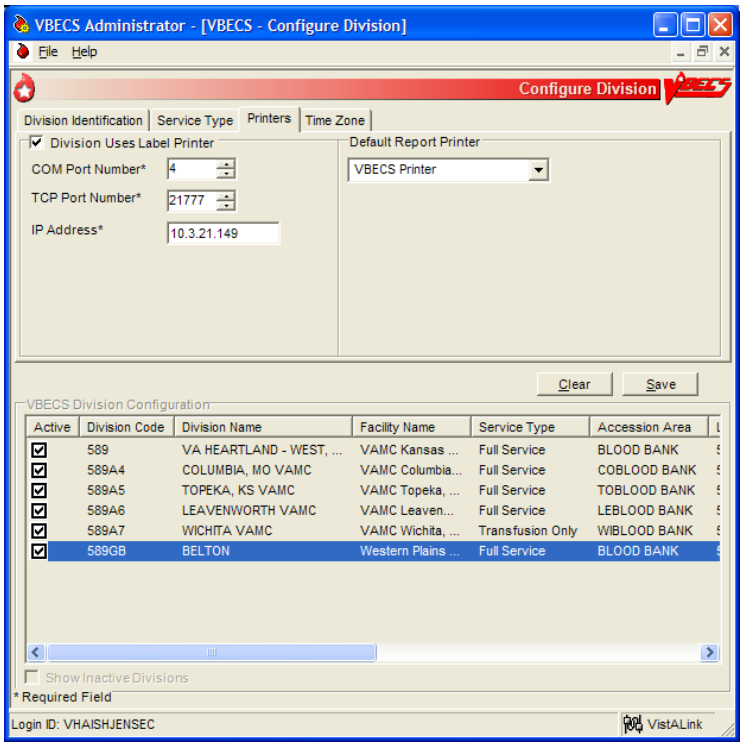
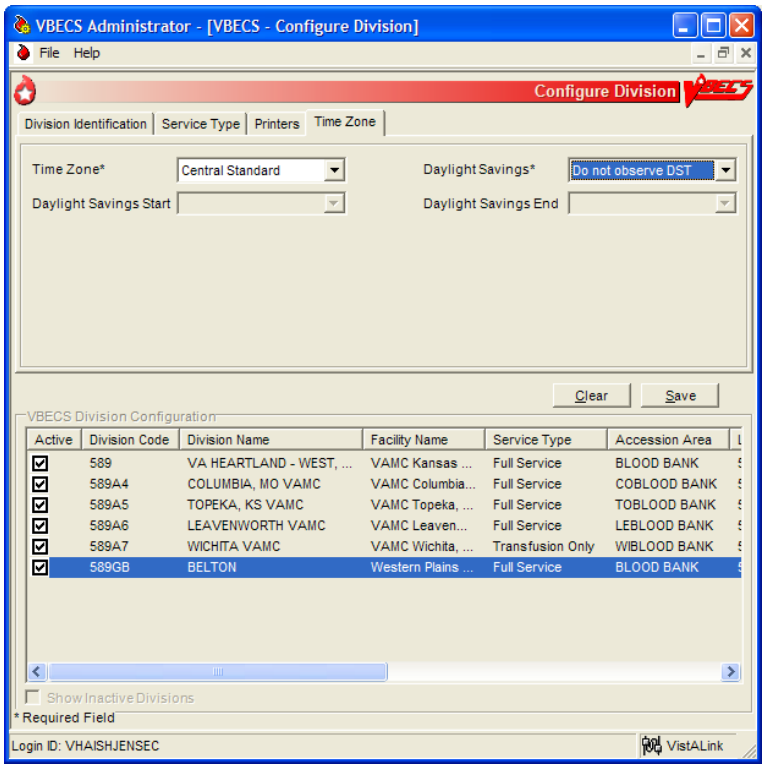


Figure 80: Example of Configure Division: Time Zone



Configure System Administrators

Each non-data center site must assign an onsite system administrator to perform regular maintenance tasks such as applying a Windows update and troubleshooting. If your servers reside at a data center, personnel at that location will be administering the servers and you may skip this section.

Assumptions

- The user has a valid Windows login and was given permission to manage the Active Directory administrator group (set up at installation).
- Users to be configured have a valid Windows account.

Outcome

- Administrators are defined and able to administer the VBECS servers from the client.

Limitations and Restrictions

Each VBECS user must have a unique Windows login ID. If a Windows login ID becomes inactive and is eligible for re-use in Active Directory, do not re-use it for VBECS: it may result in corrupted data in VBECS.

Additional Information

- None

Add or Remove System Administrators

The user adds and inactivates VBECS users.

User Action	Active Directory Users and Computers
1. Install Active Directory tools (on the Administrator's computer only) from the Windows Server 2003 Enterprise Edition installation CD or as a free download from Microsoft.	
2. Open the Control Panel. Double-click **Administrative Tools**. Double-click **Active Directory Users and Computers** (Figure 81).	• Allows the user to view and add users in Active Directory for VBECS.
3. Navigate to the Organizational Unit (OU) in which your VBECS local groups reside. Double-click the name of the user group (on the right) to which you wish to add the user (Figure 82).	• Displays administrator group in the right panel. • Displays the properties window. **NOTES** • Add a user to the administrator group to allow administrative access to the server through Remote Desktop Connection.

User Action	Active Directory Users and Computers
4. Click the **Members** tab (Figure 83). Click **Add** to add a user. To remove a user, select the user name and click **Remove**.	**NOTES** If the Add button is disabled, you do not have access to this group. File a Remedy ticket to gain access.
5. If the From this location field does not display the location of the user to be added, click **Locations** and enter the correct domain (Figure 84).	• Allows the user to enter the domain.
6. In the Enter the object names to select field, enter the Windows login ID for the user to be added. Click **OK**.	**NOTES** Click **Check Names** to verify that the login ID is valid.
7. Click **OK**.	• Closes the Properties window.
8. Exit.	

Figure 81: Example of Active Directory User and Computers Console

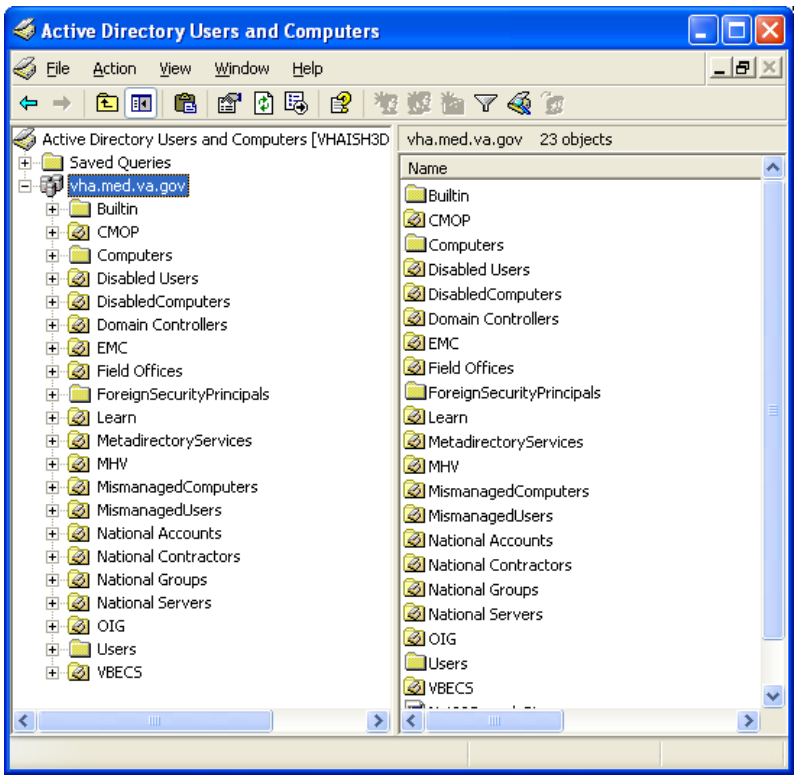


Figure 82: Example of Administrator User Group

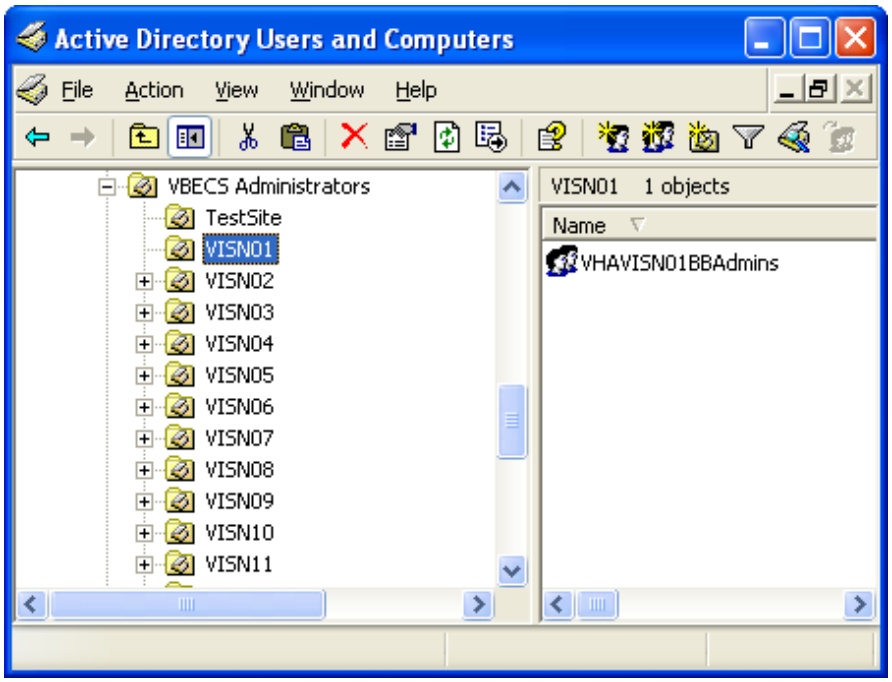


Figure 83: Example of Group Properties

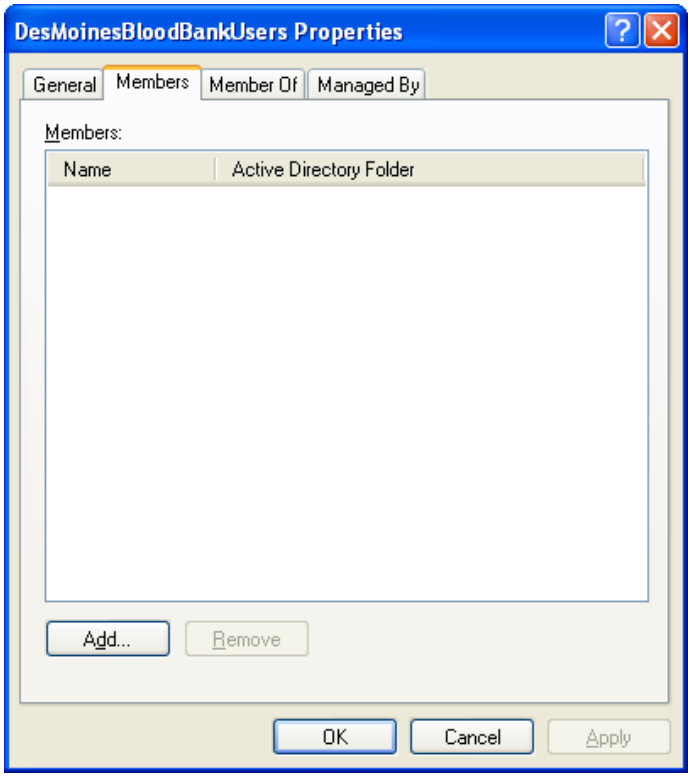
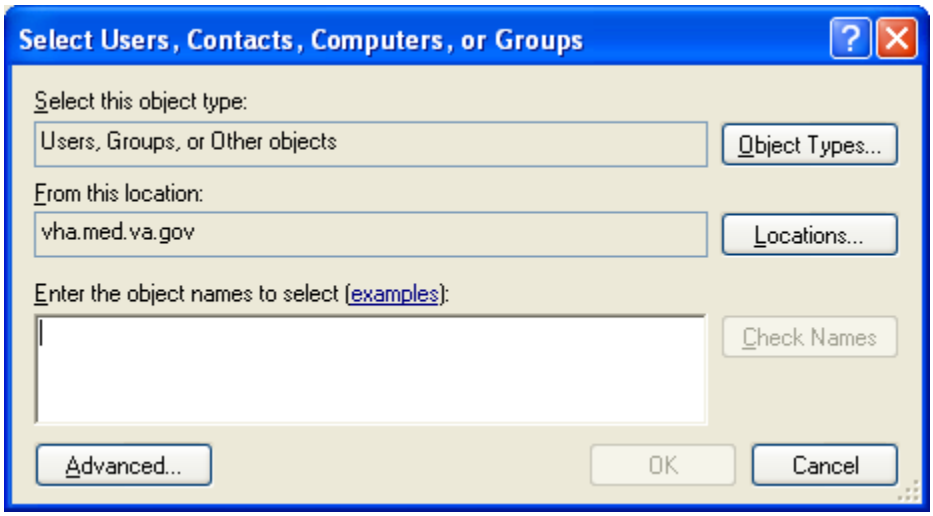


Figure 84: Example of Select Users



Configure Users

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

Assumptions

- The VistA data conversion is complete.
- All VBECS users must have the LRBLOODBANK security key.
- VBECS-VistA connection parameters are set.
- VistALink is installed and running on the associated VistA system.
- VBECS application configuration files have the correct values for Domain and user group fields.
- At least one division in VBECS is configured.
- The user is defined in VistA, and has a DUZ and Access and Verify Codes necessary to establish a VistA connection and has signed on to VistA at least once.
- All users of the Blood Bank medical device software are assigned the VBECS VISTALINK CONTEXT option as a secondary option. VistALink uses the VBECS VISTALINK CONTEXT option to provide user context sign-on security to VistA.
- The user has a valid Windows login and is defined as a member of the Active Directory domain group.
- The System Administrator created Active Directory local groups, as directed in Appendix D: Blood Bank Configuration Checklist, Create Local Groups, in *VistA Blood Establishment Computer Software (VBECS) Installation Guide*.
- The VBECS database is installed and operational.

Outcome

- VBECS users are defined and able to use VBECS.

Limitations and Restrictions

Each VBECS user must have a unique Windows login ID. If a Windows login ID becomes inactive and is eligible for re-use in Active Directory, do not re-use it for VBECS: it may result in corrupted data in VBECS.

A user must not change their Windows login ID after being configured in VBECS. If the user's name changes, the name fields in Active Directory can be modified without changing the login ID.

Additional Information

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

User Roles with Access to This Option

System Administrator

Add and Maintain Users in Active Directory

The user adds and inactivates VBECS users.

User Action	Active Directory Users and Computers
1. Install Active Directory tools (on the Administrator's computer only) from the Windows Server 2003 Enterprise Edition installation CD or as a free download from Microsoft.	
2. Open the Control Panel. Double-click **Administrative Tools**. Double-click **Active Directory Users and Computers** (Figure 85).	• Allows the user to view and add users in Active Directory for VBECS.
3. Navigate to the OU in which your VBECS local groups reside. Double-click the name of the user group (on the right) to which you wish to add the user (Figure 86).	• Displays two user groups in the right panel, one for VBECS Administrator and one for VBECS. • Displays the properties window. **NOTES** The VBECS local groups (V*nnxxx*VbecsUsers and V*nnxxx*VbecsAdministrators, where *nn* is your VISN number and *xxx* is your site identifier) were created in Appendix : Blood Bank Configuration Checklist, Create Local Groups, in *VistA Blood Establishment Computer Software (VBECS) Installation Guide*. The VBECS Administrator/Supervisor who configured the divisions must add himself as a user to all divisions to enable the functionality of canned comments in the VBECS system. He may inactivate himself later without affecting canned comments. • Add a user to either group to allow access to the server through

User Action	Active Directory Users and Computers
	Remote Desktop Connection and to VBECS Administrator or VBECS (depending on the group).
4. Click the **Members** tab (Figure 87). Click **Add** to add a user. To remove a user, select the user name and click **Remove**.	**NOTES** If the Add button is disabled, you do not have access to this group. File a Remedy ticket to gain access.
5. If the From this location field does not display the location of the user to be added, click **Locations** and enter the correct domain (Figure 88).	• Allows the user to enter the domain.
6. In the Enter the object names to select field, enter the Windows login ID for the user to be added. Click **OK**.	**NOTES** Click **Check Names** to verify that the login ID is valid.
7. Click **OK**.	• Closes the Properties window.
8. Exit.	

Figure 85: Example of Active Directory Users and Computers

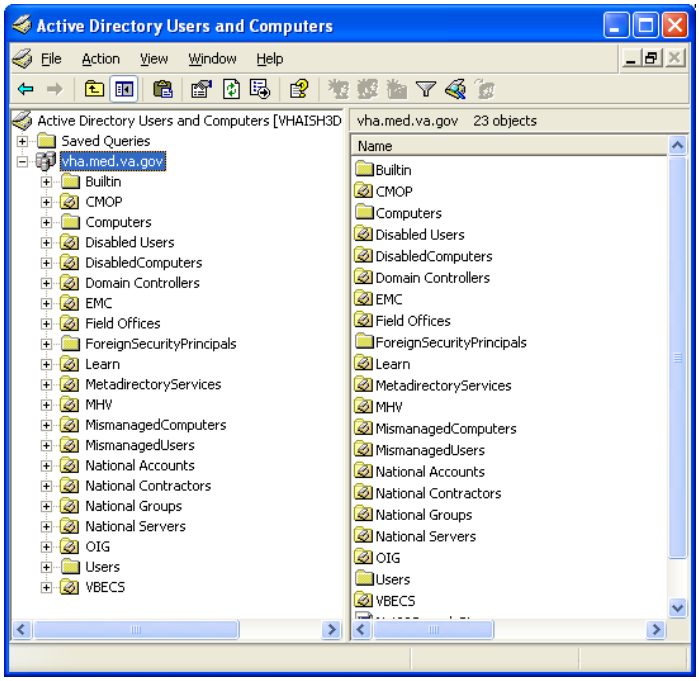


Figure 86: Example of Active Directory Users

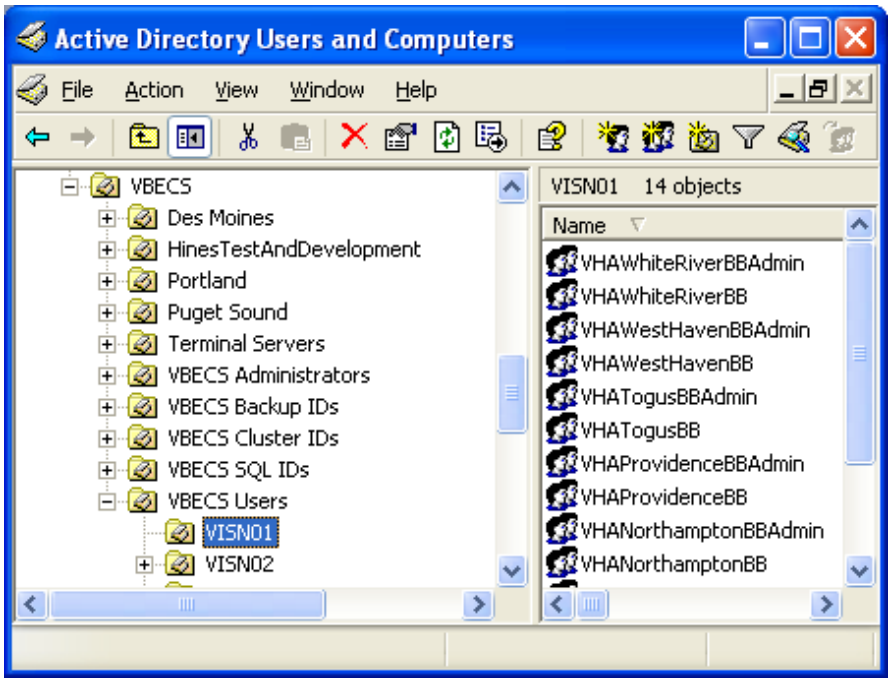


Figure 87: Example of Group Properties

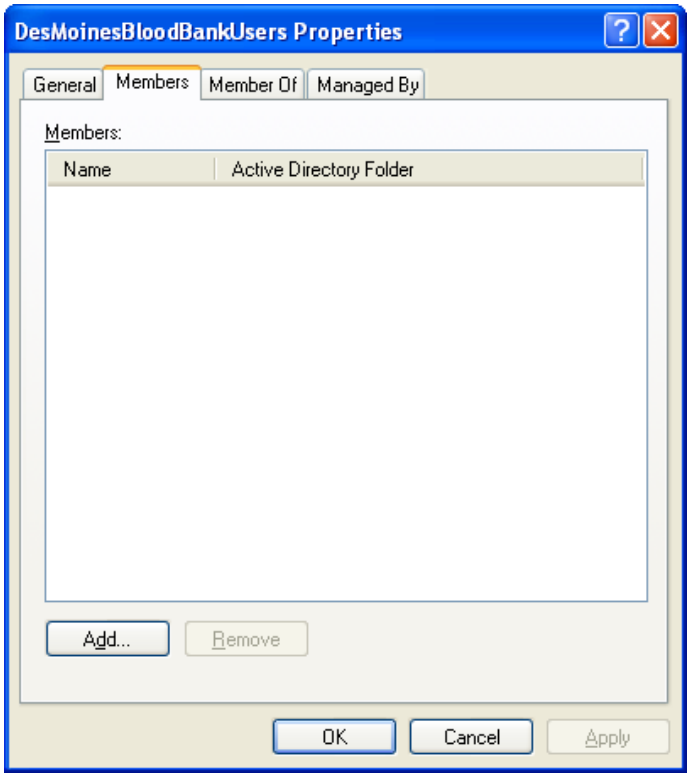
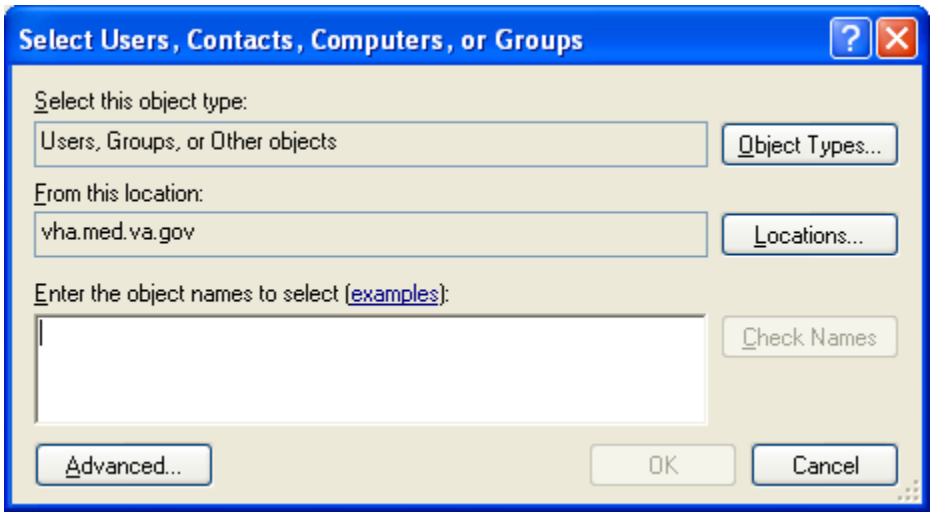


Figure 88: Example of Select Users



Configure VBECS Users

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

User Action	VBECS Administrator
1. To add and maintain users in VBECS, click **File** on the main menu of the VBECS Administrator software.	• Displays the menu options used to configure VBECS.
2. Select **Configure Users** (Figure 89).	• Allows the user to enter or edit user information.
3. To edit an existing user, select a user ID from the drop-down list (Figure 90) or, to search for a new user ID to add to VBECS, click the **ellipsis** button to the right of the drop-down list (Figure 91). Enter user parameters. For each user, VBECS stores: • VistA DUZ • Windows Login ID • Windows Username • Email Address (optional) • User Initials • Active Status • Division Code • User Role • Division Active Status	• Displays the Windows user ID and name. **NOTES** VistALink lists active VistA Blood Bank users. VistA Blood Bank users are identified by the LRBLOODBANK and LRBLSUPER security keys. When VBECS finds users that are inactive in VistA, it asks whether the user wishes to inactivate them in VBECS. **Yes** inactivates the VBECS users. **No** allows the user to continue without inactivating the users (Figure 94). The user may not edit the VistA DUZ or user name, the Windows login ID or user name, or the division code or name. There is a one-to-one correspondence between Windows and VistA users. A VistA DUZ may be associated with only one Windows login ID and vice versa. The user may: Activate or inactivate but not delete a defined user from VBECS. Rescind a defined user's access privileges at one or more divisions but not delete his record or ID from the database. The user ID stored in VBECS is the user's Windows Logon ID.

User Action	VBECS Administrator
	VBECS displays the data that a user enters in a session. The user may edit and save the data. When a user cancels, VBECS warns that it will not save the data. VBECS closes the form and returns the user to the main menu screen that may include unrelated open windows. VBECS associates the technologist ID, date, time, and division with each process for retrieval by division.
4. To search for a VistA user, click the **ellipsis** button to the right of the VistA DUZ field (Figure 92).	• Allows the user to search for VistA Blood Bank users by name or DUZ. **NOTES** The user may not edit the VistA DUZ or user name, the Windows login ID or user name, or the division code or name.
5. Enter the email address of the user in the E-mail field in the Additional Info group. VistA provides the initials, if available. If not, enter them.	• Allows the user to enter Additional Information about the user for identification. **NOTES** User initials may be loaded from VistA. VBECS requires unique user initials for use as the technologist ID.
6. To select a VistA division to associate with the user, click the **ellipsis** button to the right of the Division Code drop-down menu (Figure 93).	• Allows the user to select a division to associate with the user **NOTES** A single user may be associated with multiple divisions.
7. Select a user role from the User Role drop-down menu. Click or clear the **Active Role?** check box to activate or inactivate the role.	• Allows the user to assign security roles to the Blood Bank user. • If a user was removed from the role of Administrator/Supervisor and was the only Administrator/Supervisor user left for a division, displays "You are trying to remove the last Administrator/Supervisor for your division, which would disallow system configuration in the future. You may not proceed." If all entered data is satisfactory, saves user details and access changes to the file and adds or updates the user information in the list view. **NOTES** One role at a time may be assigned to a user at a division. A user may have only one active user role per division. VBECS allows the assignment of a security level to one or more users at a time. VBECS warns that there must be at least one level 6 VBECS Administrator/Supervisor in the division and does not allow the user to change the last Administrator/Supervisor.
8. Click **Update** and **Save**.	• Displays a confirmation dialog.
9. Click **Yes** to commit changes to the database.	• Click **Yes** to commit changes to the database.
10. To close the Edit Users dialog box, click  in the upper right corner.	

Figure 89: Example of Configure Users

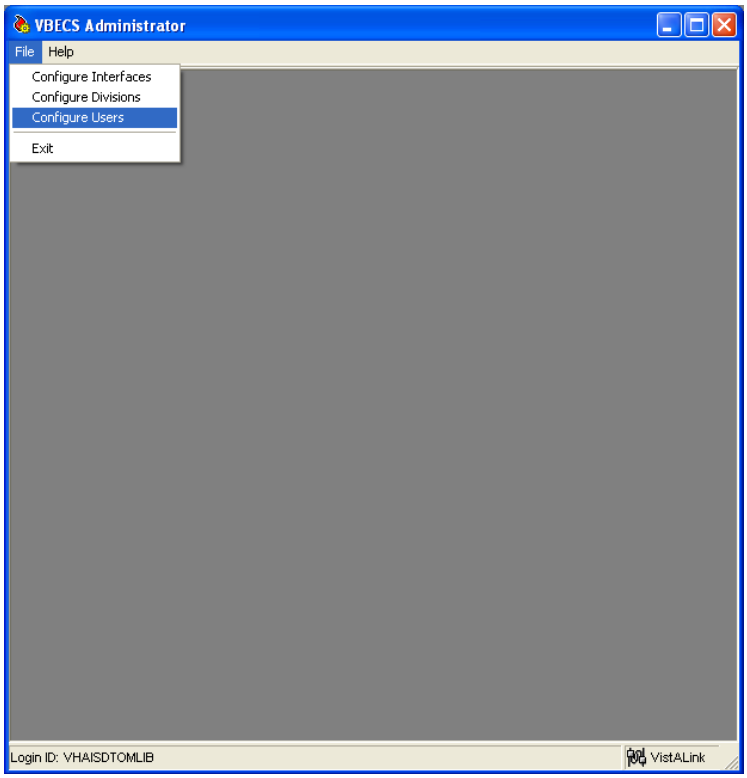


Figure 90: Example of Edit User

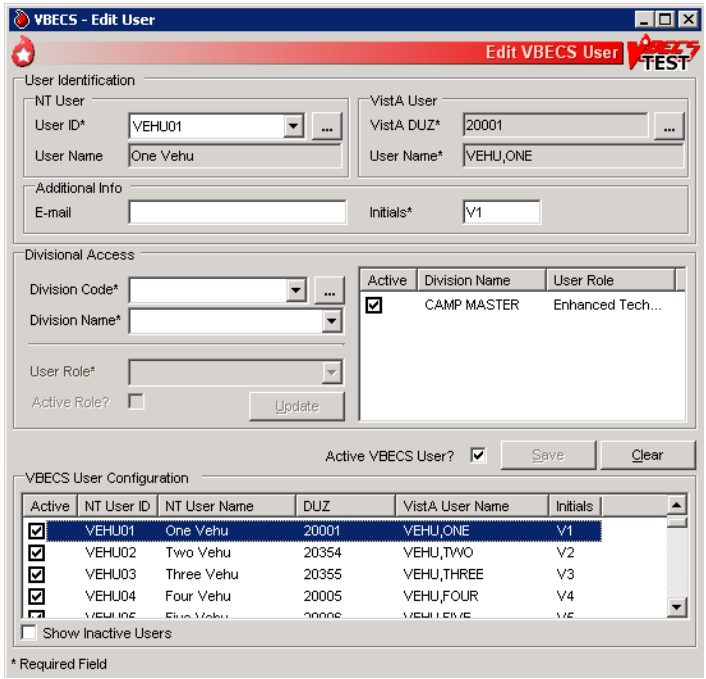


Figure 91: Example of Windows Users

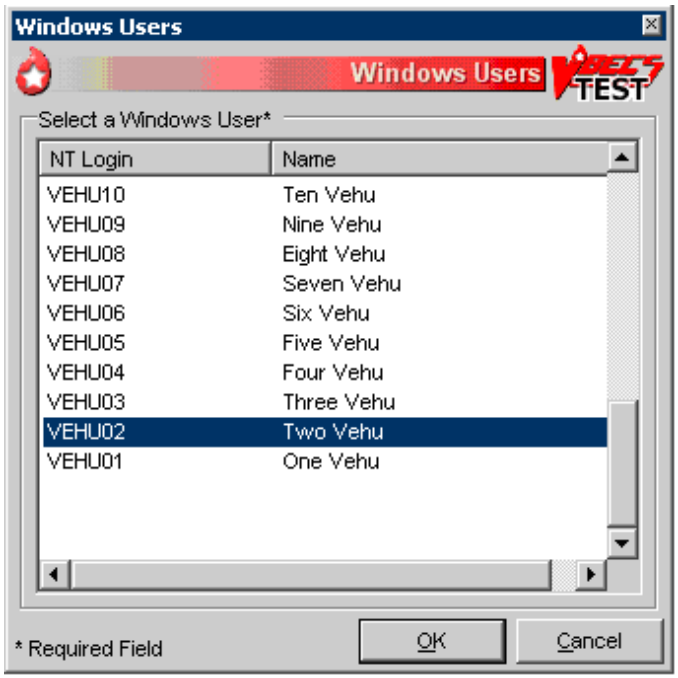


Figure 92: Example of VistA Users

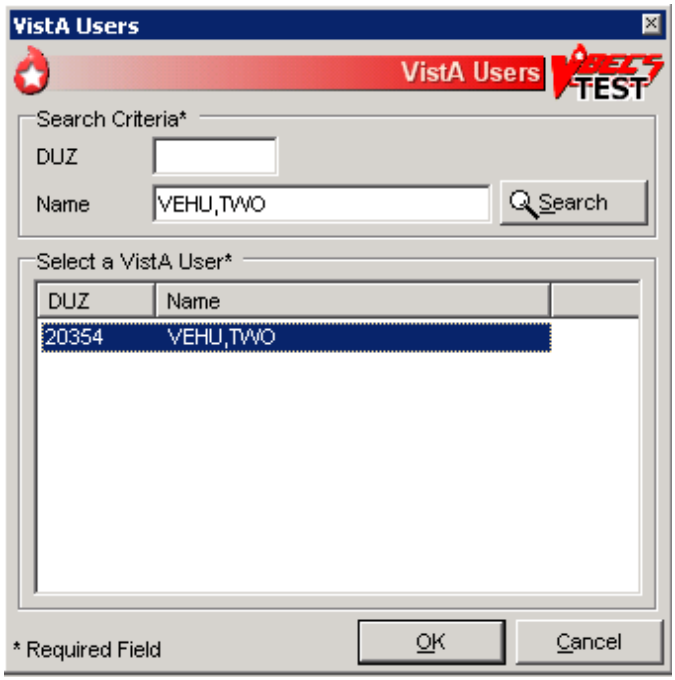


Figure 93: Example of VistA Divisions

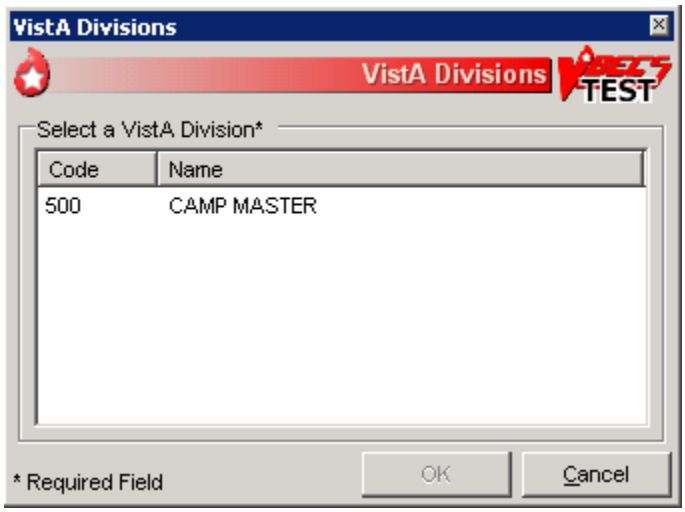
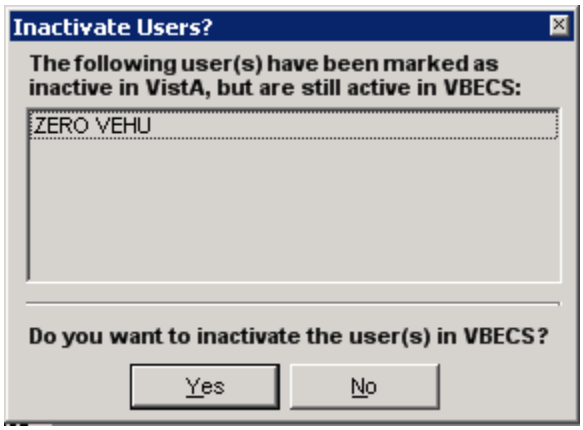


Figure 94: Example of Inactive Users



Transmit Workload Data

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

Assumptions

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

Outcome

- Information was transmitted to VistA for inclusion in appropriate reports.

Limitations and Restrictions

- None

Additional Information

- Workload Event data must include information required for Decision Support System (DSS), Patient Care Encounter (PCE), and Billing Awareness. Once in VistA, existing VistA functionality will handle required reporting.
- The system accumulates and periodically transmits workload information to the VistA Lab workload recording process. The data is transmitted from VBECS to VistA by the VBECS Workload Capture Remote Procedure called by a nightly Lab background process.
- Workload multipliers for all Blood Bank activities in VistA File #64 must be set to one (1) to avoid excessive 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 Laboratory Management Index Program (LMIP) workload information exists. In addition, for certain events that involve patient processing, the patient location, treating specialty, service, etc., are captured to satisfy PCE or DSS reporting requirements.

These steps address the initial recording of these events.

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

Inactivate a Workload Event

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

User Action	VBECS
1. Inactivate a saved record.	Recognizes the activity performed as an inactivation of an existing Workload Event record. **NOTES** See Appendix B: Workload Process Mapping to Application Option Table.
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.	

Released Technical Bulletins (one-time execution required)

Updating the Printer Driver on Existing VBECS Servers (BB10-01)

Audience

All test sites that installed VBECS 1.0.0.0.

Purpose

To instruct VBECS system administrators to install the Universal Printer Driver on the VBECS servers.

Action

The VBECS server administrator must execute the instructions in this technical bulletin immediately to update the printer driver.

Compliance

This bulletin requires mandatory compliance with these instructions. Failure to update the printer driver will result in errors when printing certain reports.

Prerequisites

Before starting, ensure you have the following:

1) Names or IP addresses of both servers.
2) Administrative access to both servers.

Note: Executing this technical bulletin does not require system downtime. The activities described in this technical bulletin can be performed during normal business hours.

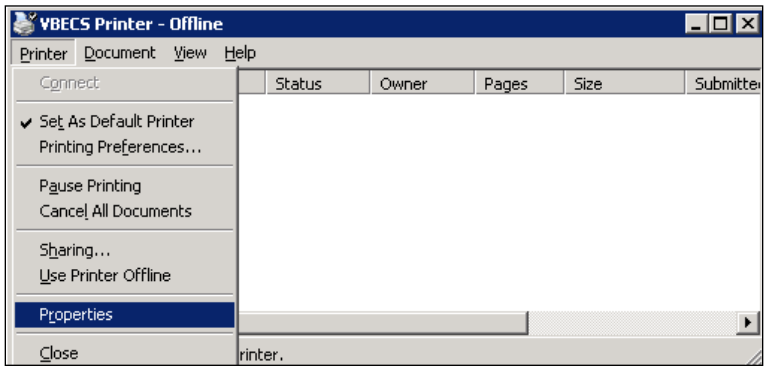
Update the printer driver

Cluster Node 1: VBECS

1) Open a remote desktop connection: click **Start, All Programs, Accessories, Communication, Remote Desktop Connection**. Enter the name of cluster node 1 in the Computer field. Click **Connect.** Log into cluster node 1 with a valid server administrator name and password.
2) Click **Start, Control Panel, Printer and Faxes, VBECS Printer** (note: if your site is multi-divisional, your printers will have the division name appended to the printer name).

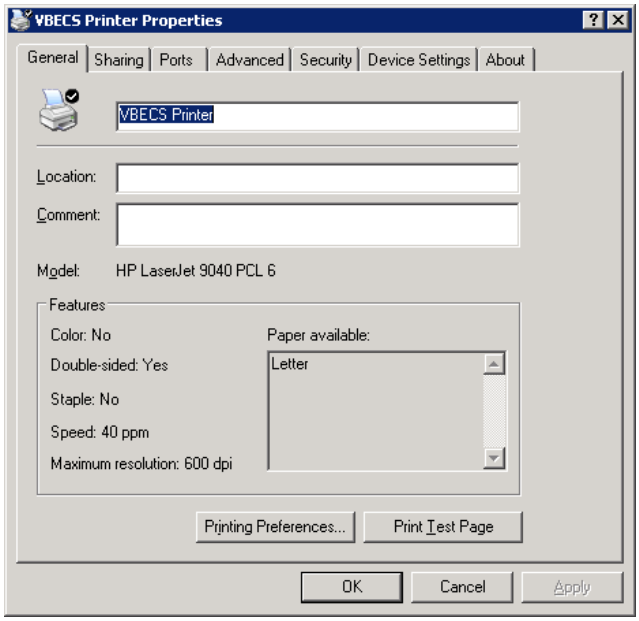
3) Click **Printer, Properties** (Figure 95).

Figure 95: Example of VBECS Printer



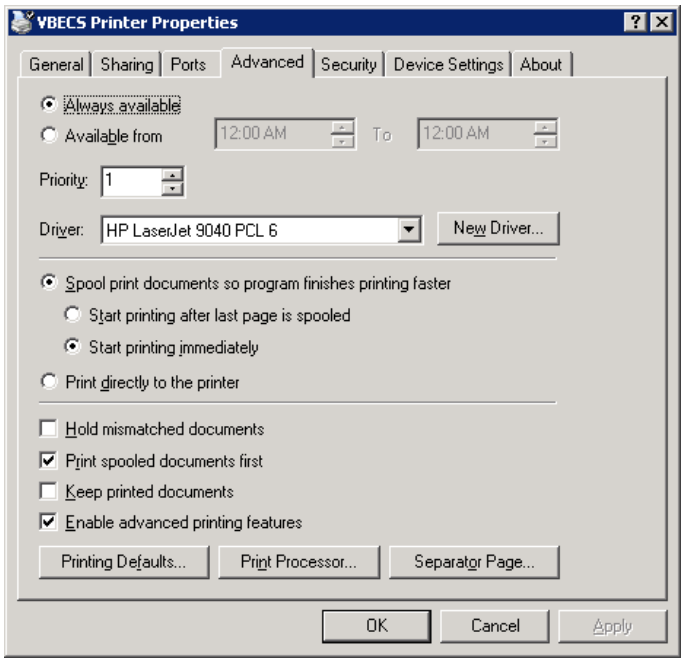
4) Click the **Advanced** tab (Figure 96).

Figure 96: Example of Printer Properties



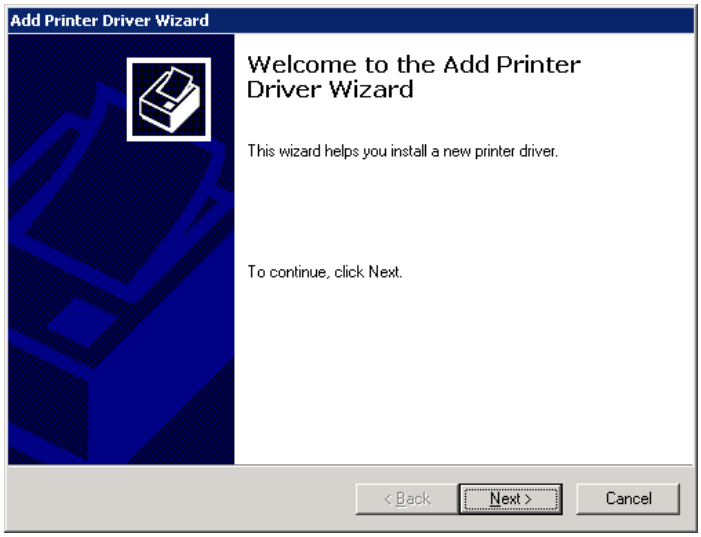
5) Click **New Driver** (Figure 97).

Figure 97: Example of Printer Properties



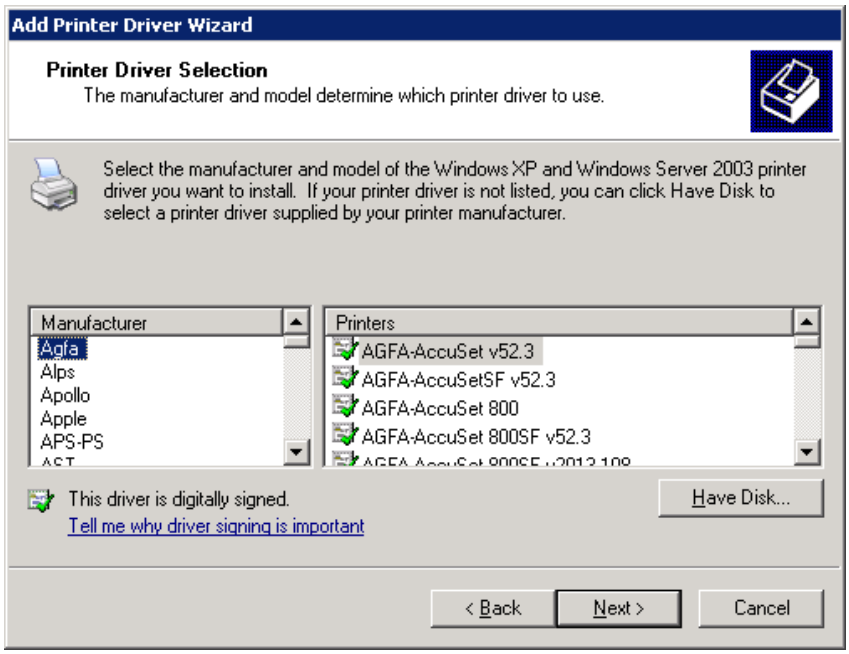
6) Click **Next** (Figure 98).

Figure 98: Example of Printer Driver



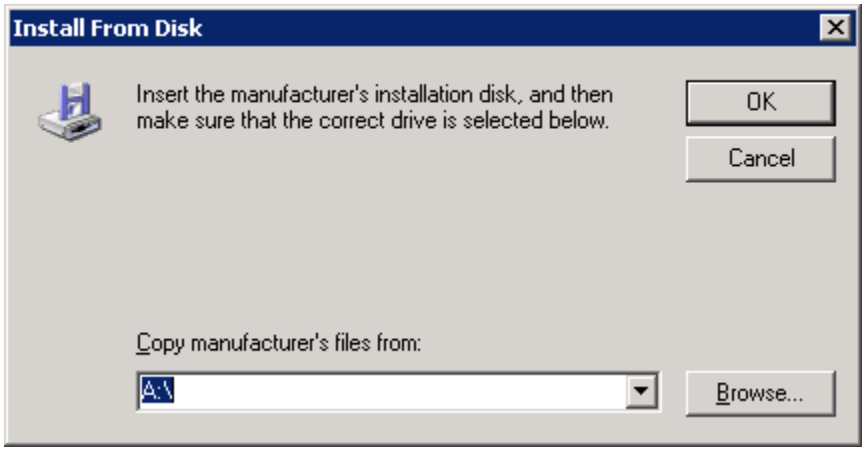
7) Click **Have Disk** (Figure 99).

Figure 99: Example of Printer Driver



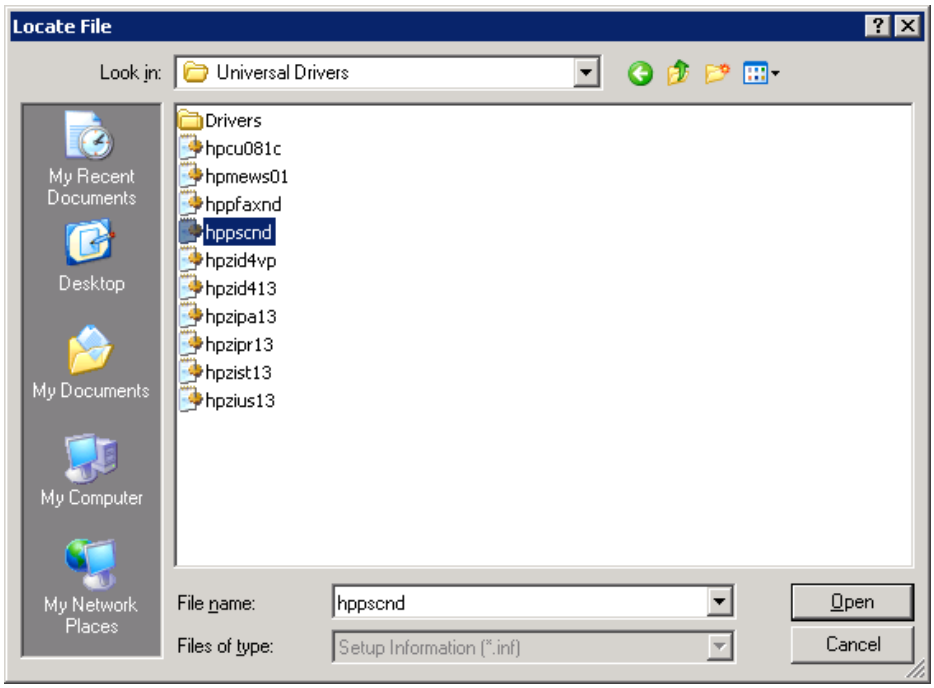
8) Click **Browse** (Figure 100).

Figure 100: Example of Select Driver Location



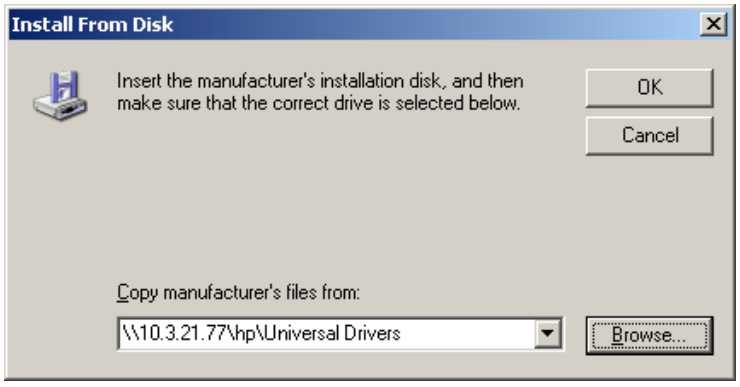
9) Navigate to **\\10.3.9.165\Universal**. Select **hppscnd** and click **Open** (Figure 101).

Figure 101: Example of Locate File



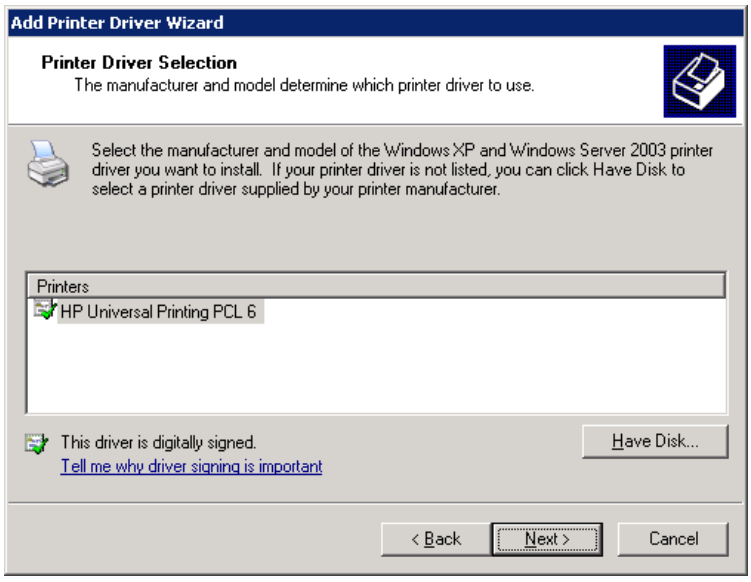
10) Click **OK** (Figure 102).

Figure 102: Example of Click OK



11) Click **Next** (Figure 103).

Figure 103: Example of Driver



12) Click **Finish** (Figure 104).

Figure 104: Finished!

13) If your site is multi-divisional, you will have multiple printers installed on the server. Repeat Steps 2 through 12 for the other printers installed on the server.
14) Repeat Steps 1 through 13 on the other server.

Securing Simple Network Management Protocol (SNMP) on VBECS Servers (BB10-05)

Audience

All VBECS Lab sites.

Purpose

To instruct local hardware support personnel to secure Simple Network Management Protocol (SNMP) on the VBECS servers.

Action

Technical support personnel must execute the instructions in this technical bulletin to properly remedy SNMP vulnerabilities.

Compliance

This bulletin requires mandatory compliance.

Prerequisites

Before starting, ensure that you have the following:

- server administrative privileges on the VBECS servers

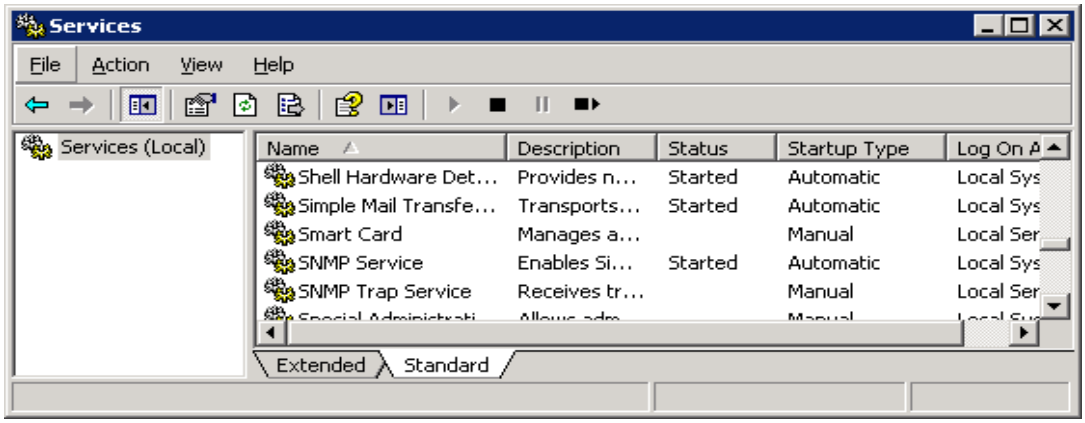
*If a Zebra **Z4M Plus**™ label printer requires a SNMP update you are instructed to file a Remedy ticket for national support.*

Updating the VBECS Servers

To update SNMP on the VBECS servers:

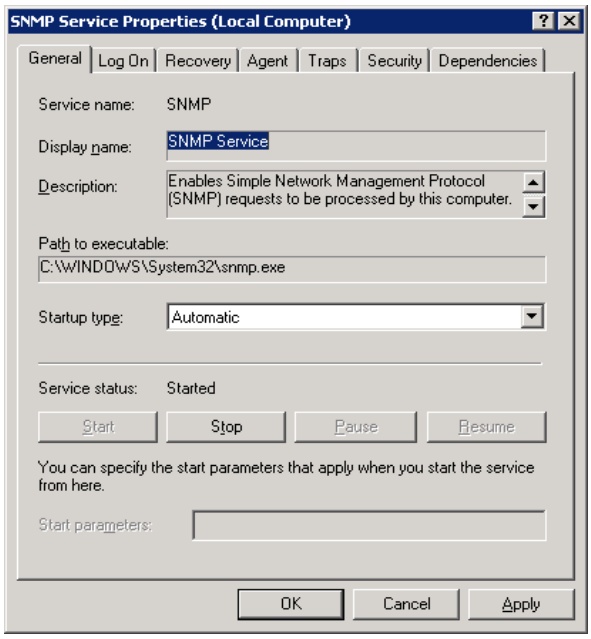
- Log into the server with server administrative privileges.
- Click **Start, Control Panel, Administrative Tools, Services** (Figure 105).

Figure 105: Example of Example of Services



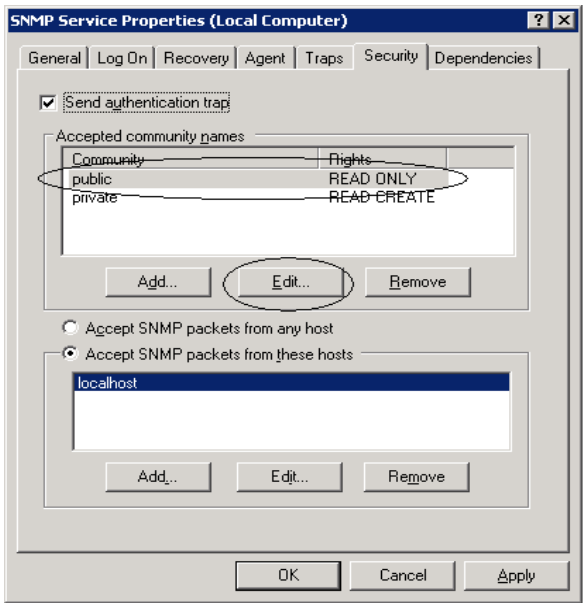
- Right-click on **SNMP Service** and choose **Properties**. Click on the **Security** tab (Figure 106).

Figure 106: Example of SNMP Properties



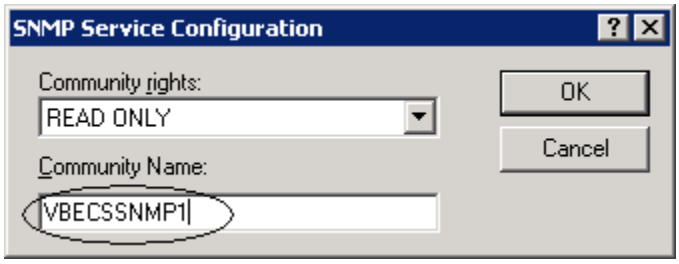
- Select **public** in the Accepted community names box to highlight and click **Edit** (Figure 107).

Figure 107: Example of Public SNMP community name



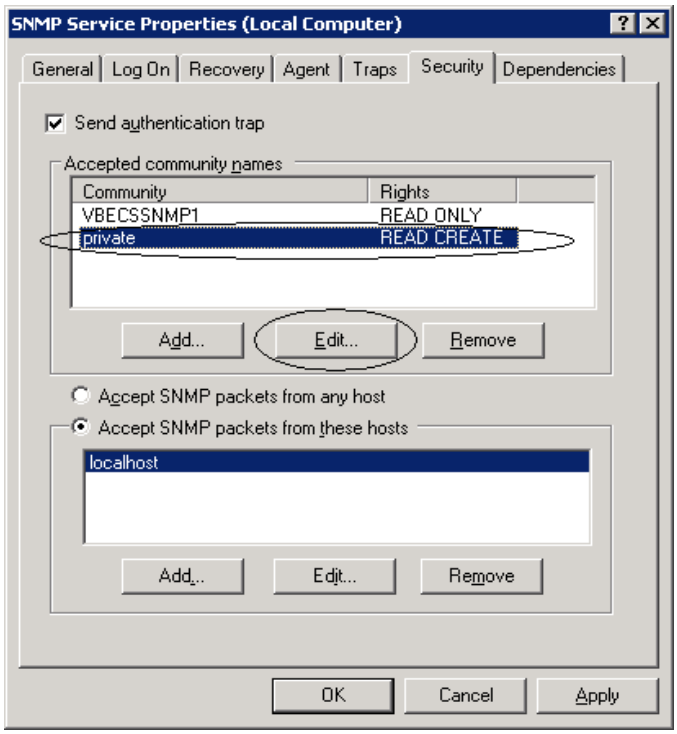
- Change the Community Name to "**VBECSSNMP1**" (Figure 108) and click **OK**.

Figure 108: Example of Changing the Public Community Name



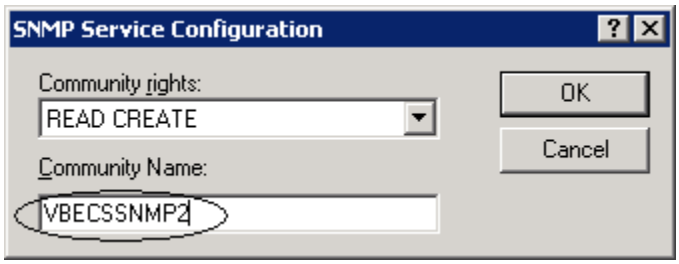
- Select **private** and click **Edit** (Figure 109).

Figure 109: Example of Private SNMP community name



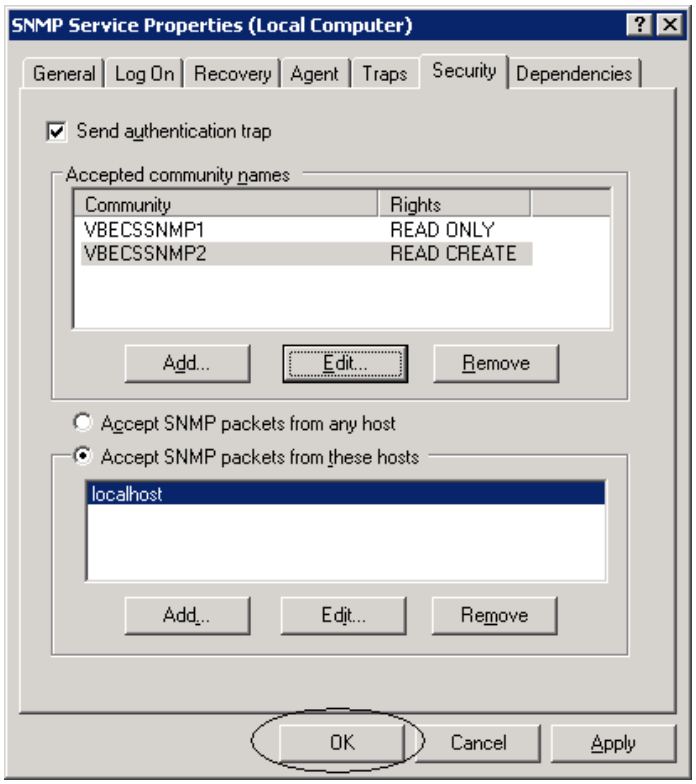
- Change the Community Name to "**VBECSSNMP2**" (Figure 110) and click **OK**.

Figure 110: Example of Community Name



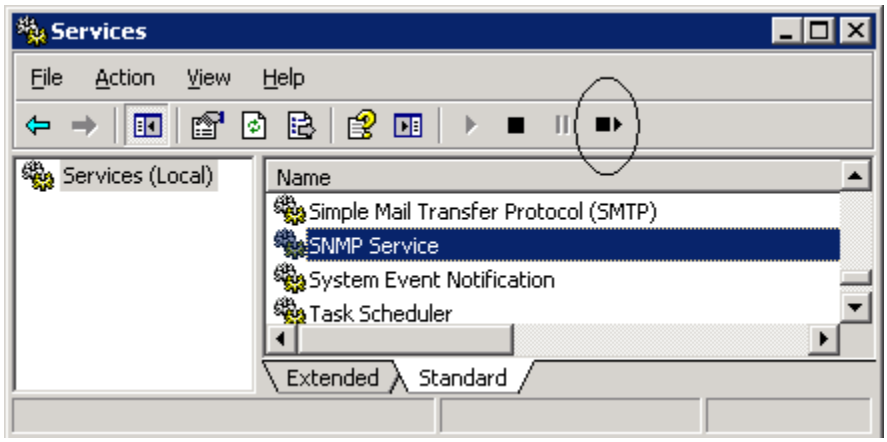
- Click **OK** on the SNMP Service Properties window (Figure 111) to save and close.

Figure 111: Example of SNMP community names



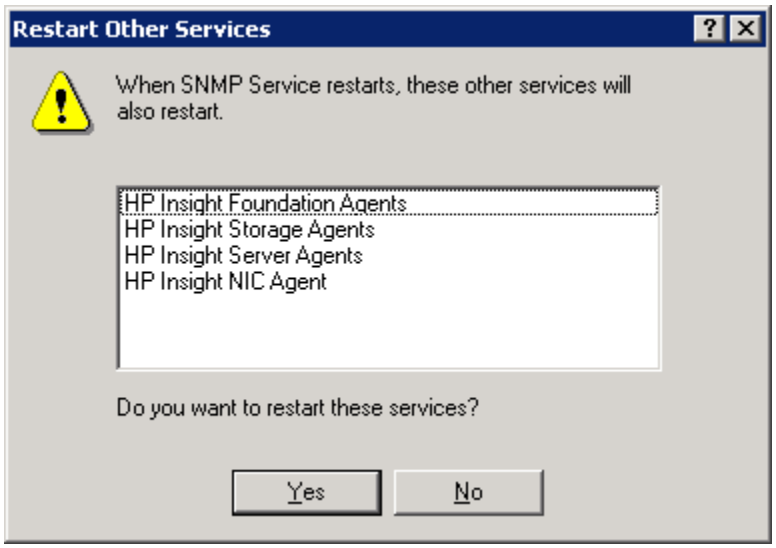
- In the Services window (Figure 112), select the **SNMP Service** and click the **Restart Service** button (circled).

Figure 112: Example of Services



- You will be prompted to restart HP services (Figure 113). Click **Yes**. The services will then stop and restart. After they are done, close the Services console and log off the server.

Figure 113: Example of Restart Other Services



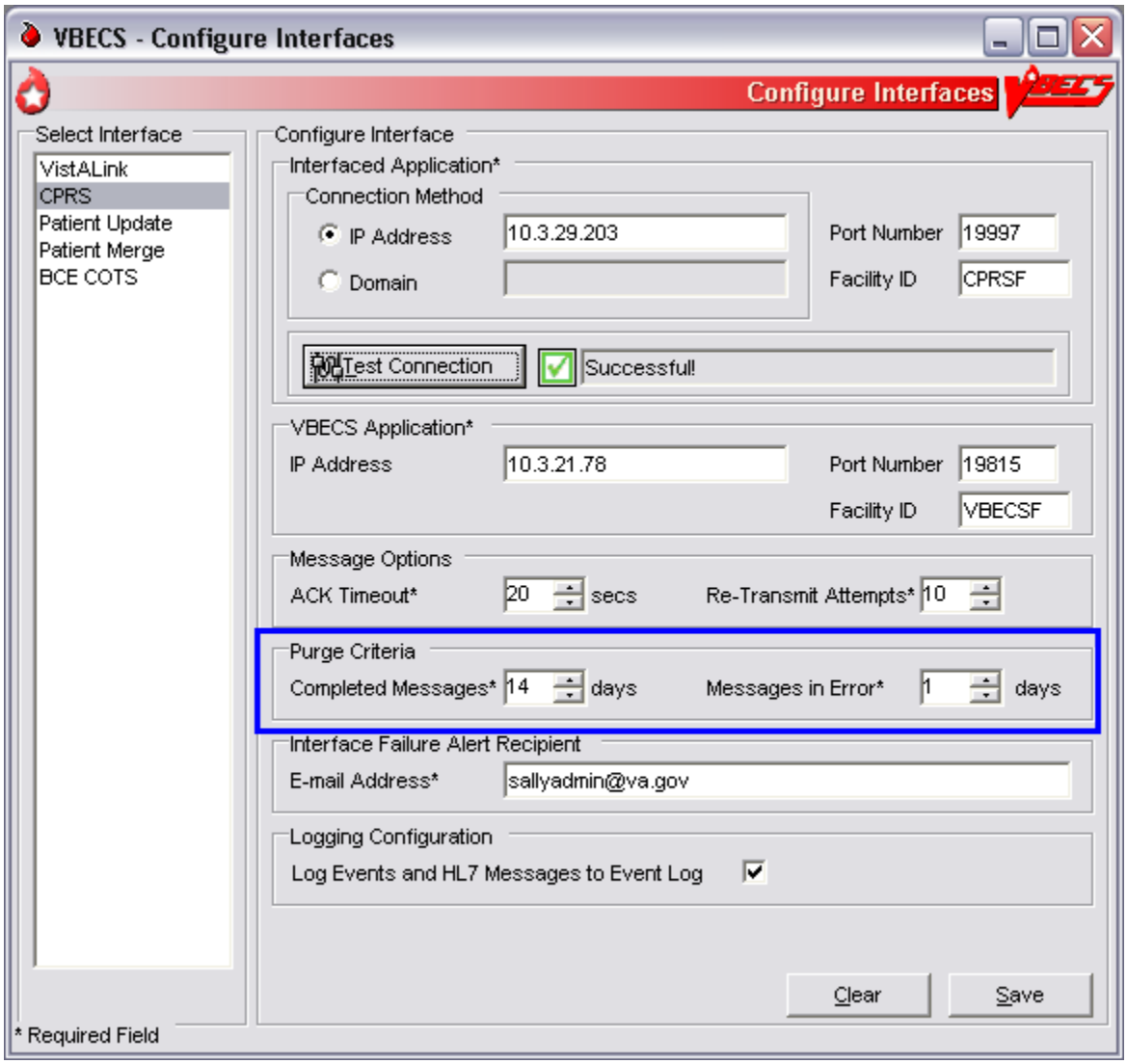
- Repeat Steps 1 through 10 on the other server in your cluster.

External Interfaces

Purging the HL7 Message Log

The purge criteria for HL7 messages stored in the MessageLog table in VBECS can be set in VBECS Administrator (Figure 114). There are values for completed messages and error messages. When a user logs into VBECS, the current messages in the table are checked against the current criteria and any matching messages are deleted.

Figure 114: Example of VBECS Configure Interfaces HL7 Message Log Purge



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 VAISS located in the VistA M environment through RPCs. This data exchange is controlled through 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 RPC XML 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 7: Remote Procedure Calls

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

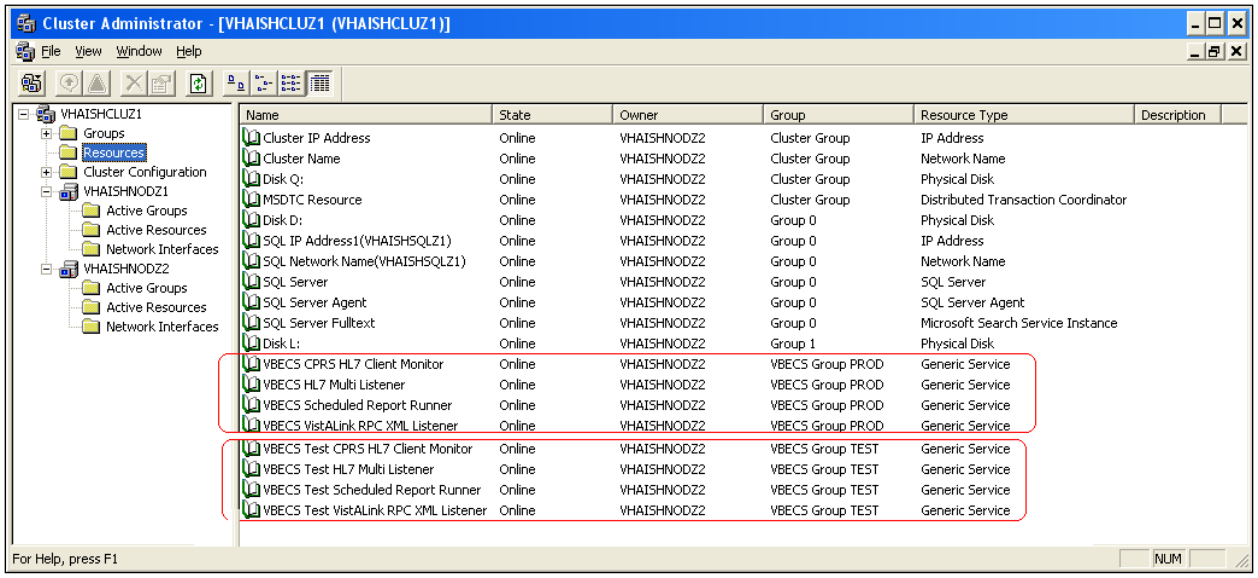
RPC Name	Database Integration Agreement (DBIA)	This RPC:
Lookup		blood components in VBECS.
VBECS Lab Test Results Lookup	4612	Returns a list of VistA Laboratory test results for a patient.
VBECS Medication Profile Lookup	4613	Returns a list of medications for a patient from the VistA Pharmacy package.
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.

VBECS Windows Services

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

VBECS uses Microsoft Windows Services (services) to provide minimal downtime and minimal user interaction. These services are installed on each physical server of the VBECS cluster server group. The Cluster Administrator controls the state and operation of the VBECS services. See Figure 115 for a complete listing of VBECS services. The Install VBECS Services and the VBECS Application section of the VistA Blood Establishment Computer Software (VBECS) Installation Guide describe how these services are installed. For details on stopping and starting VBECS services see the Restarting VBECS Services section.

Figure 115: Example of VBECS Services in Cluster Administrator



Reconfiguring the VBECS HL7 Multi Listener and VistALink Services

VBECS HL7 Multi Listener Service

If changes need to be made to the configuration of the VBECS HL7 Multi Listener service due to a change in IP address or port number, first take the VBECS HL7 Multi Listener resources offline. Navigate to the C:\Program Files\VistA\VBECS\WinServices\VBECS HL7 Multi Listener, and locate the file named VbecsHL7ListenerService.exe.config. The file contents will look similar to the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="BceTransfusionCommentSeparator" value=";" />
    <add key="BceTransfusionReactionMarker" value="*" />
    <add key="PrimaryDbConnectionString" value="Connection Timeout=90;Data
Source=VHAXXXSQLZ1;Initial Catalog=VBECS_V1_PROD;persist security
info=False;packet size=8192;integrated security=SSPI;Application Name=VBECS HL7 Multi
Listener" />
    <add key="serviceName" value="VBECS HL7 Multi Listener" />
    <add key="allowPing" value="true" />
    <add key="listenerIpAddress" value="XX.XX.XX.XX" />
    <add key="listenerPortNumber" value="5000" />
    <add key="monitorService" value="true" />
    <add key="monitorInterval" value="5000" />
    <add key="monitorMaxRetries" value="3" />
    <add key="monitorServiceStartTimeout" value="5" />
```

```
    <add key="BuildNumber" value="1.0.6.2" />
    <add key="PatientFirstNameMaximumLength" value="30" />
    <add key="PatientLastNameMaximumLength" value="30" />
    <add key="PatientMiddleNameMaximumLength" value="30" />
    <add key="PatientFullNameMaximumLength" value="30" />
  </appSettings>
</configuration>
```

Modify the value for the key named listenerIpAddress and the value for the key named listenerPortNumber. Save the file, close it and bring the VBECS HL7 Multi Listener resource online. Repeat the update of the configuration file on the other server. There is no need to bring any more resources online; the Cluster Administrator handles both nodes at the same time.

Test account: The test account listener (VBECS Test HL7 Multi Listener) is changed in the same manner. It is located at C:\Program Files\VistA\VBECS Test\WinServices\VBECS Test HL7 Multi Listener.

VBECS VistALink RPC XML Listener Service

If changes need to be made to the configuration of the VBECS VistALink RPC XML Listener service due to a change in IP address or port number, first stop the VBECS VistALink RPC XML Listener service. Navigate to the c:\Program Files\VistA\VBECS\WinServices\VBECS VistALink RPC XML Listener, and locate the file named VistALink.Listener.WinService.exe.config. The file contents will look similar to the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <sectionGroup name="VistALink">
      <section name="RpcList"
type="gov.va.med.vbecs.DAL.VistALink.Listener.Core.RpcListConfigSectionHandler,VistALin
k.Listener.Core" />
    </sectionGroup>
  </configSections>
  <appSettings>
    <add key="PrimaryDbConnectionString" value="Connection Timeout=90;Data
Source=VHAXXXSQLZ1;Initial Catalog=VBECS_V1_PROD;persist security
info=False;packet size=8192;integrated security=SSPI;Application Name=VBECS VistALink
RPC XML Listener" />
    <add key="serviceName" value="VBECS VistALink RPC XML Listener" />
    <add key="serverName" value="VHAXXXSQLZ1" />
    <add key="databaseName" value="VBECS_V1_PROD" />
    <add key="listenerPortNumber" value="8000" />
    <add key="allowPing" value="true" />
    <add key="listenerIpAddress" value="XX.XX.XX.XX" />
```

```
    <add key="monitorService" value="true" />
    <add key="monitorInterval" value="3000" />
    <add key="monitorMaxRetries" value="3" />
    <add key="monitorServiceStartTimeout" value="5" />
    <add key="BuildNumber" value="1.0.6.2" />
    <add key="PatientFirstNameMaximumLength" value="30" />
    <add key="PatientLastNameMaximumLength" value="30" />
    <add key="PatientMiddleNameMaximumLength" value="30" />
    <add key="PatientFullNameMaximumLength" value="30" />
  </appSettings>
  <VistALink>
```

Modify the value for the key named listenerIpAddress and the value for the key named listenerPortNumber. Save the file, close it and restart the VBECS VistALink RPC XML Listener service.

Test account: The test listener (VBECS Test VistALink RPC XML Listener) is changed in the same manner. It is located at C:\Program Files\VistA\VBECS Test\WinServices\VBECS Test VistALink RPC XML Listener.

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.

Table 8: Windows Service Manager

Windows Service Name	This Service:
VBECS CPRS HL7 Client Monitor	The startup type is set to manual. The cluster administrator will manage the starting of this service. It polls the VBECS Production database for HL7 messages to be sent to CPRS or BCE in the VistA Production account. If the BCE interface is disabled through our VBECS Admin, no BCE messages will be sent or received from BCE. When the BCE interface is enabled you will still not receive any BCE messages until you stop and start this service.
VBECS HL7 Multi Listener	The startup type is set to manual. The cluster administrator will manage the starting of this service. This is the default HL7 listener service for all Production HL7 interfaces.
VBECS Scheduled Report Runner	The startup type is set to manual. The cluster administrator will manage the starting of this service. It runs scheduled VBECS reports for the Production database.
VBECS VistALink RPC XML Listener	The startup type is set to manual. The cluster administrator will manage the starting of this service. 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 CPRS HL7 Client Monitor	The startup type is set to manual. The cluster administrator will manage the starting of this service. It polls the VBECS Test database for HL7 messages to be sent to CPRS or BCE in the VistA Test account. If the BCE interface is disabled through our VBECS Admin, no BCE messages will be sent or received from BCE. When the BCE interface is enabled you will still not receive any BCE messages until you stop and start this service.
VBECS Test HL7 Multi Listener	The startup type is set to manual. The cluster administrator will

Windows Service Name	This Service:
	manage the starting of this service. This is the default HL7 listener service for all Test HL7 interfaces.
VBECS Test Scheduled Report Runner	The startup type is set to manual. The cluster administrator will manage the starting of this service. It runs scheduled VBECS reports for the Test database.
VBECS Test VistALink RPC XML Listener	The startup type is set to manual. The cluster administrator will manage the starting of this service. 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.

This page intentionally left blank.

Troubleshooting

Hardware support on SharePoint

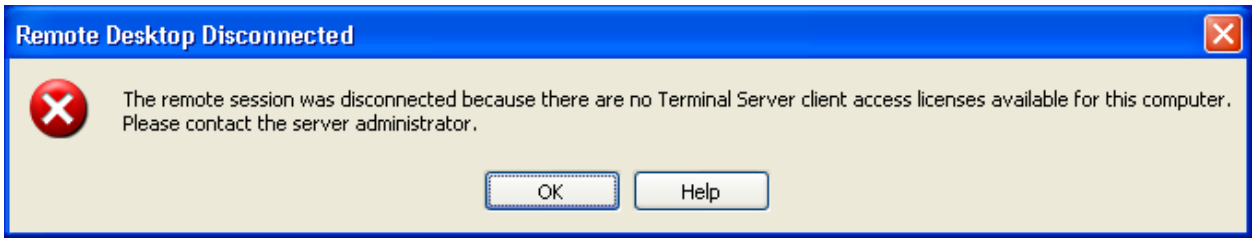
On the VBECS SharePoint site, we have a hardware page. This page contains the following links:

- **Hardware Manuals**: Go here to find manufacturer documentation for server, shared storage, backup device, printers and scanners.
- **Warranty Information**: When calling HP for service (800.633.3600), they will request the SAID. Find the SAID in this spreadsheet.

Remote Desktop Licensing Issues

In order to connect to VBECS, a workstation must have a valid license from an active Terminal 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 116). Deleting the Terminal 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 116: Example of Expired Terminal Services License

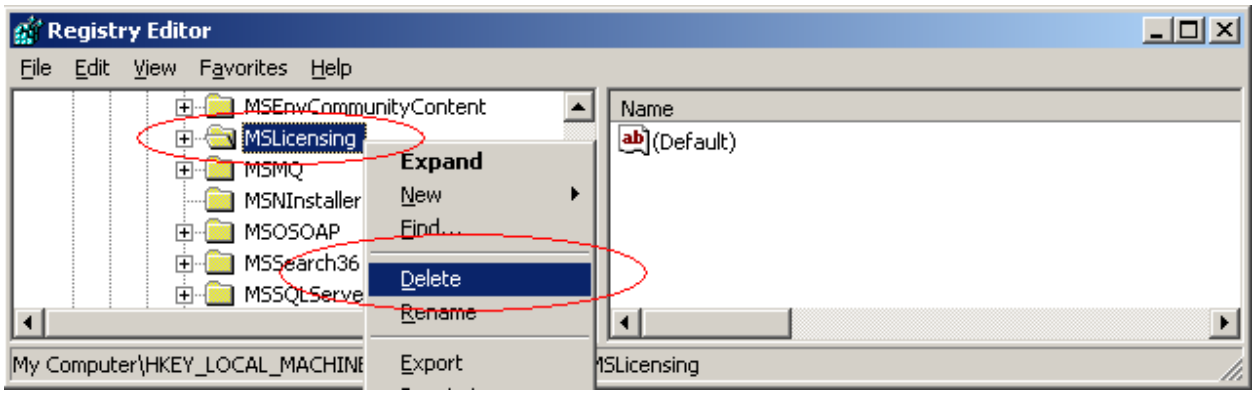


Deleting the Terminal Services Licensing Information on a VBECS Workstation

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

1) Log into the workstation that is receiving the error (Figure 116) and click **Start, Run…**
2) In the Run window, type **regedit** and click **OK**.
3) In the Registry Editor window, expand the folders to the following location: **My Computer, HKEY_LOCAL_MACHINE, SOFTWARE, Microsoft.**
4) Locate and right click the **MSLicensing** folder, select **Delete** (Figure 117).

Figure 117: Deleting the MSLicensing Registry Key



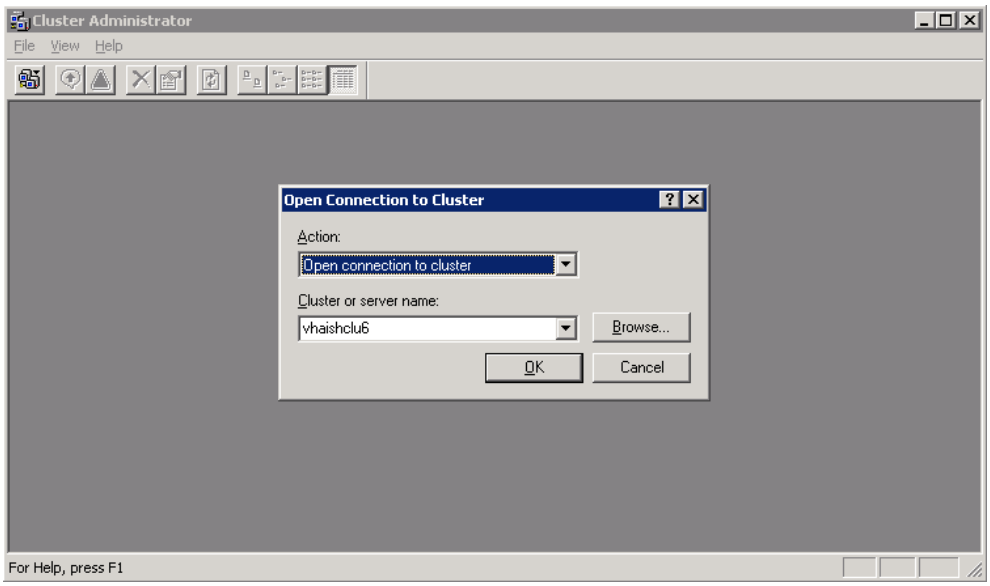
5) Make sure you are at the correct path and click **Yes** to confirm the deletion.
6) Close the Registry Editor.

Stopping and Starting VBECS Services

Stopping VBECS Services

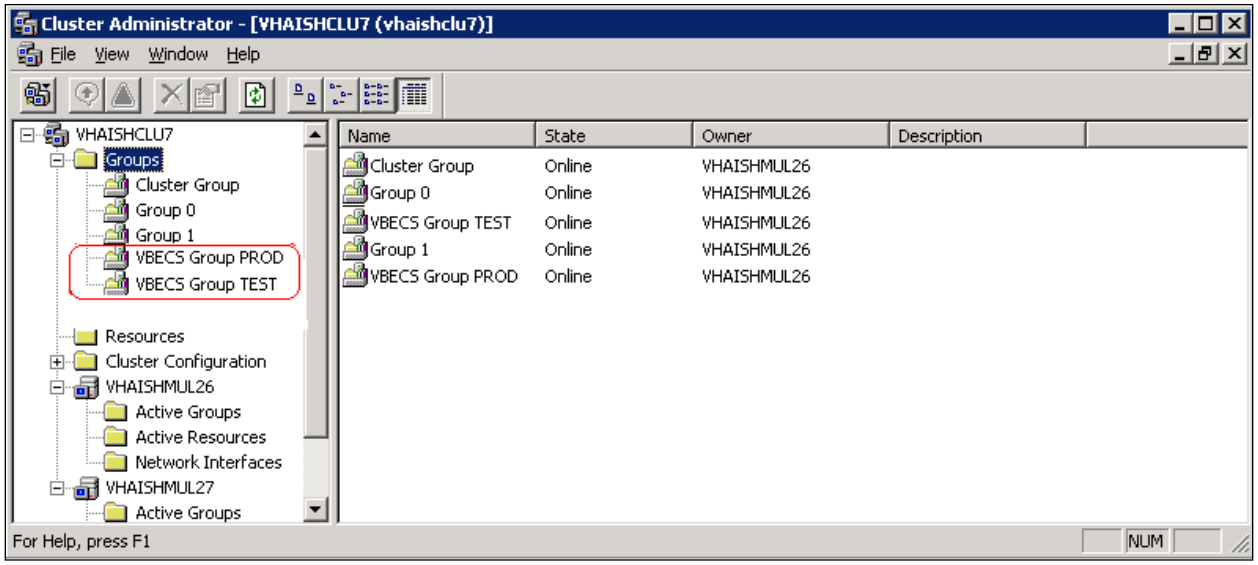
1) Click **Start, Administrative Tools, Cluster Administrator**.
2) If Open Connection to Cluster window does not appear, click **File**, **Open Connection**.
3) Type <***CLUSTER_NAME***> in the **Cluster or server name** field and click **OK** (Figure 118).

Figure 118: Example of Open Connection to Cluster



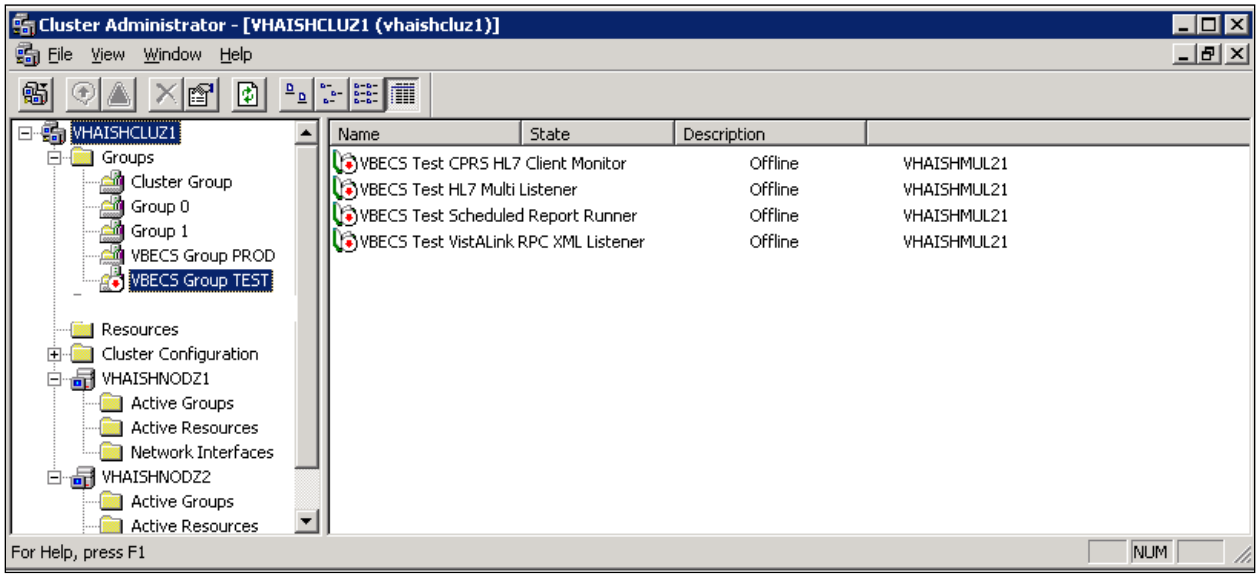
4) The Cluster Administrator window populates. Expand the Groups folder, and verify that **VBECS Group PROD** and **VBECS Group TEST** exist as shown in (Figure 119).

Figure 119: Example of All VBECS Groups Services Online



5) Right-click on a **VBECS Group** and select **Take Offline** (Figure 120).

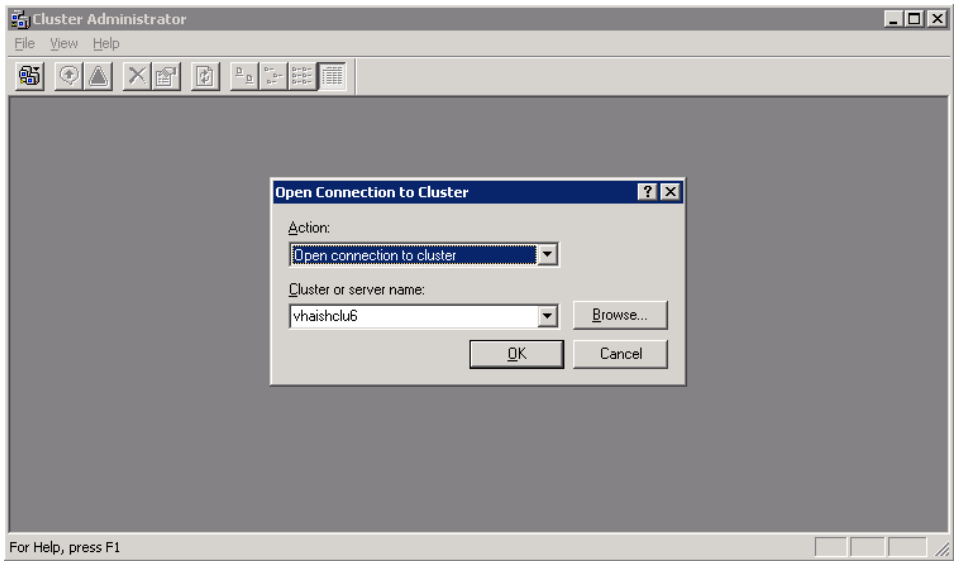
Figure 120: Example of VBECS Group Services Offline



Starting VBECS Services

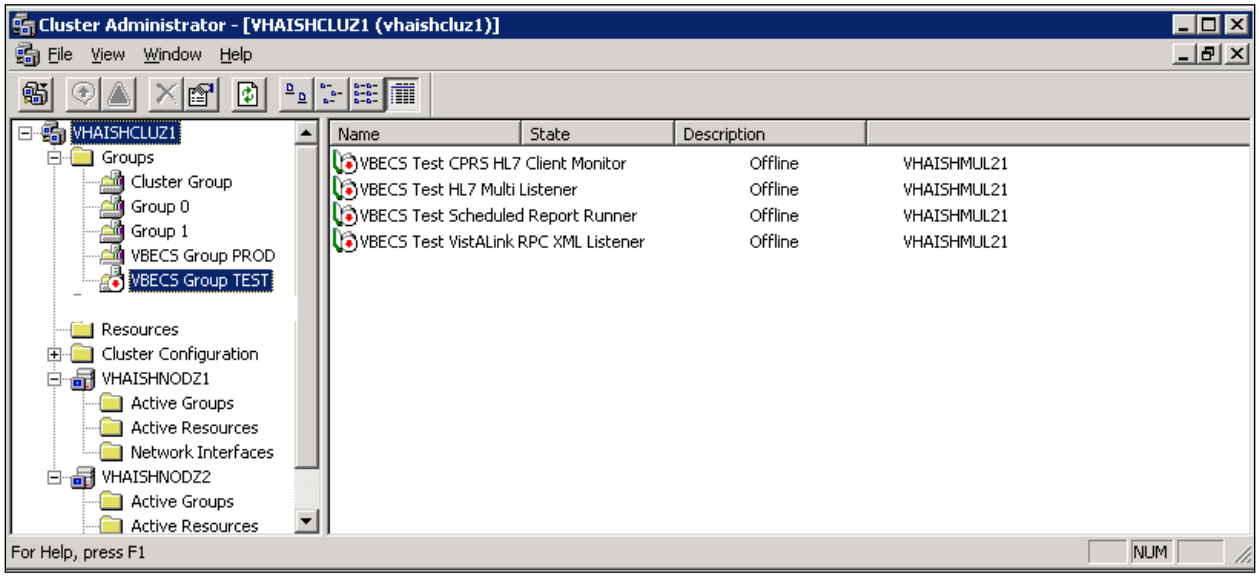
1) Click **Start, Administrative Tools, Cluster Administrator**.
2) If Open Connection to Cluster window does not appear, click **File**, **Open Connection**.
3) Type <***CLUSTER_NAME***> in the **Cluster or server name** field and click **OK** (Figure 121).

Figure 121: Example of Open Connection to Cluster



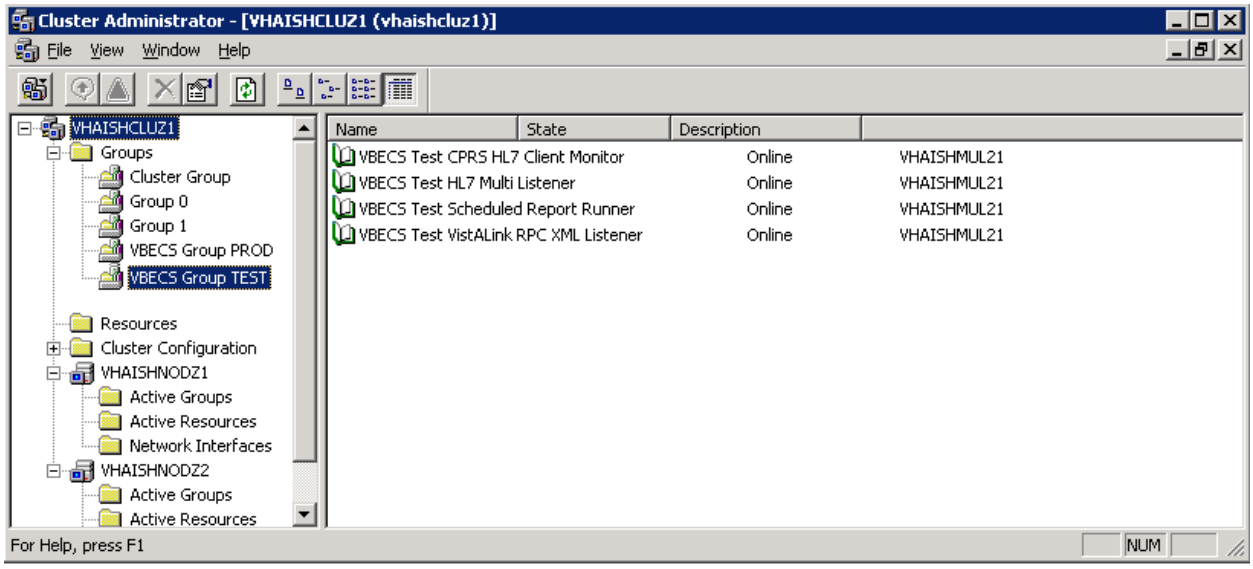
4) The Cluster Administrator window populates. Expand the Groups folder, and verify that **VBECS Group PROD** and **VBECS Group TEST** exist as shown in Figure 122.

Figure 122: Example of VBECS Group Services Offline



5) Right-click on a **VBECS Group** and select **Bring Online** (Figure 123).

Figure 123: Example of VBECS Group Services Online

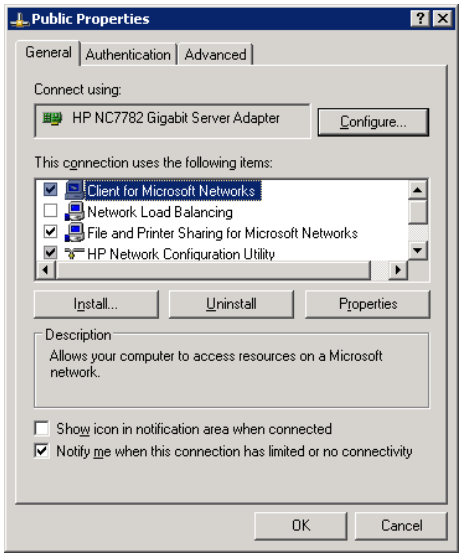


Verify NIC Card Configuration

If the VBECS application experiences network latency issues, such as problems when scanning barcodes, check the NIC card configuration settings.

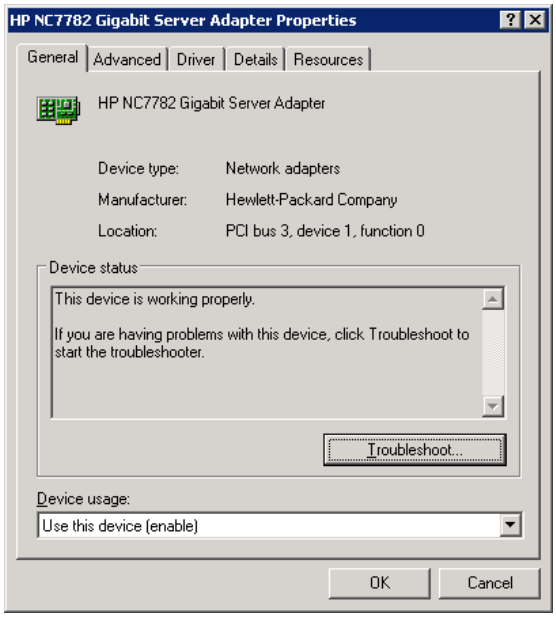
1) Using remote desktop connection, log into cluster node 1.
2) Click **Start, Control Panel, Network Connections, Public**. Click **Properties**.
3) Click **Configure** (Figure 124).

Figure 124: Example of Public Properties



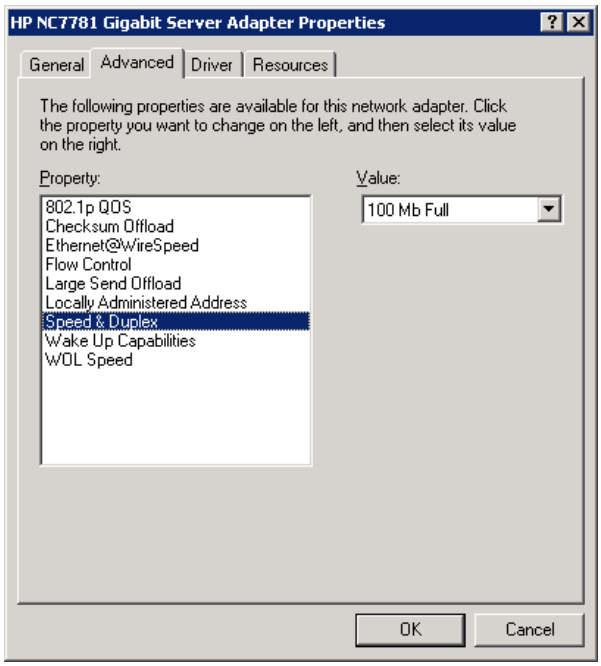
4) Click on the **Advanced** tab (Figure 125).

Figure 125: Example of NIC Properties



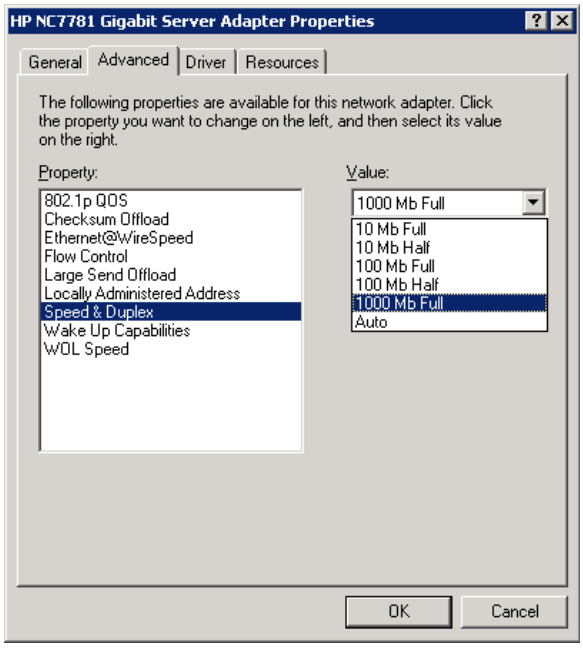
5) Click **Speed and Duplex** (Figure 126) (e.g., 100Mb Full).

Figure 126: Example of HP NC7782 Gigabit Server Adapter Properties



6) Verify that the value stated matches the Switch Port Speed. Contact the Network Administrator of the servers for the Switch Port Speed.
7) If both values are the same, click **Cancel** and continue to Step 11 for cluster node 2.
8) If the values are different, make the values match (Figure 127).

Figure 127: Example of Updated HP NC7782 Gigabit Server Adapter Properties

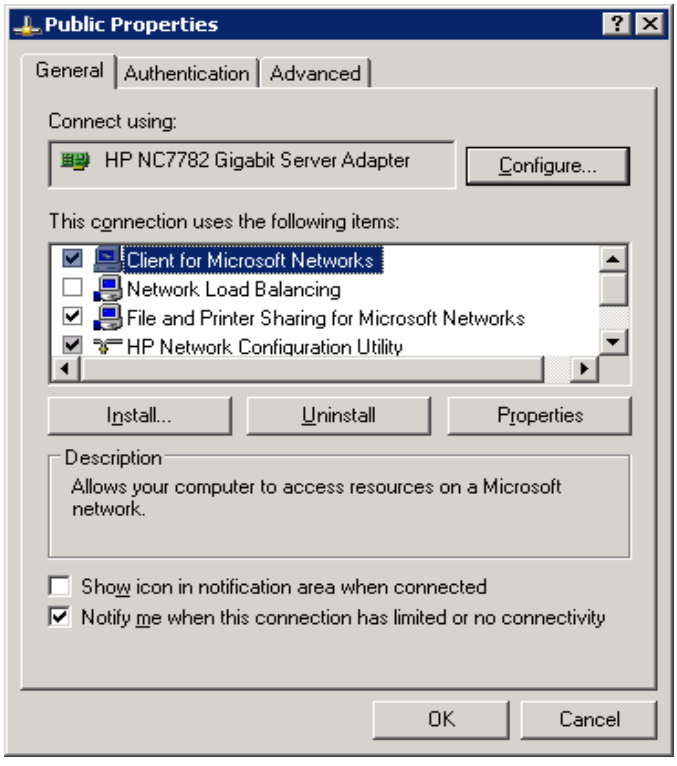


9) Click **OK**.
10) The remote desktop reconnection message popup will be received (Figure 128).

Figure 128: Example of Reconnecting Message

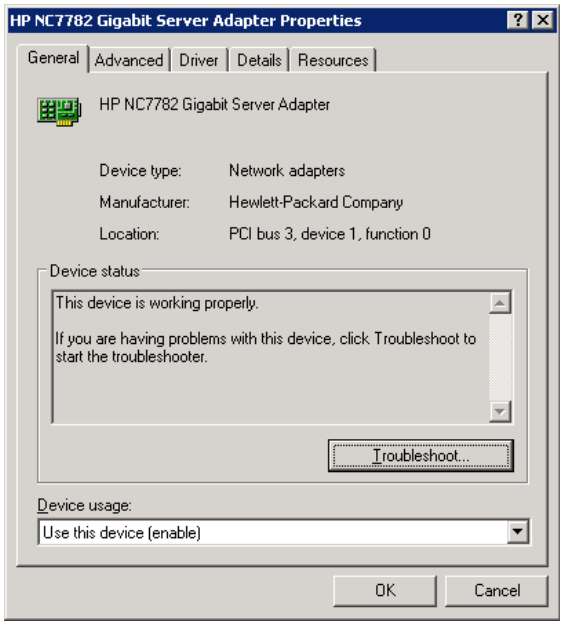
11) Log off cluster node 1 when the remote session is restored. **Log into cluster node 2.**
12) Click **Start, Control Panel, Network Connections, Public**. Click **Properties**.
13) Click **Configure** (Figure 129).

Figure 129: Example of Public Properties



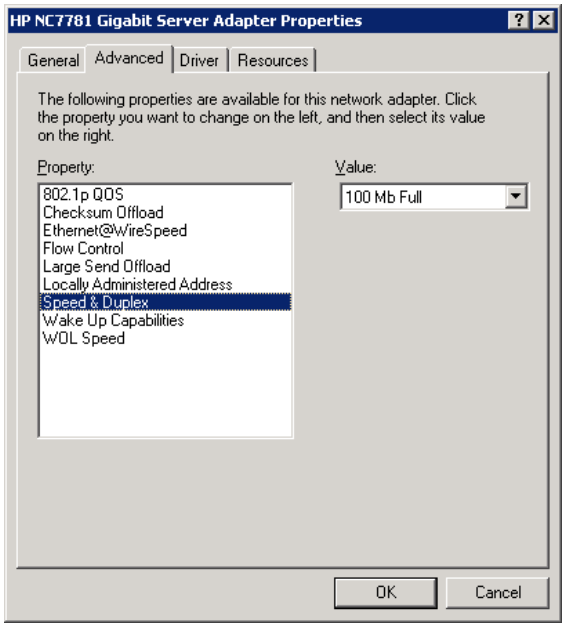
14) Click on the **Advanced** tab (Figure 130).

Figure 130: Example of NIC properties



15) Click **Speed and Duplex** (Figure 131) (e.g., 100Mb Full).

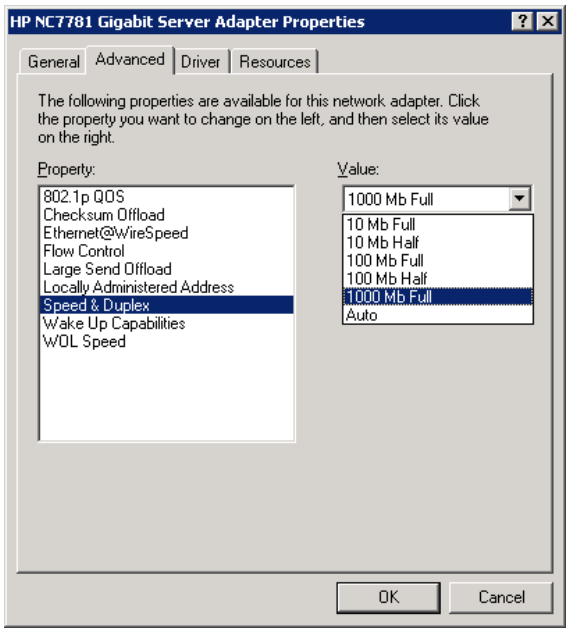
Figure 131: Example of HP NC7782 Gigabit Server Adapter Properties



16) Verify that the value stated matches the Switch Port Speed. Contact the Network Administrator of the servers for the Switch Port Speed.
17) If both values are the same, click **Cancel** and do not proceed with these remaining steps.

18) If the values are different, make the values match (Figure 132).

Figure 132: Example of Update HP NC7782 Gigabit Server Adapter Properties



19) Click **OK**.

20) The remote desktop reconnection message popup will be received (Figure 133).

Figure 133: Example of Reconnecting Message

21) After the remote session is restored, click **Start**, **Administrative Tools**, **Cluster Administrator** (It may take several minutes for the Cluster Administrator utility to completely load).

22) If the Passive cluster node 2 has an inactive icon (Figure 134) wait until the node comes back online (Figure 135).

Figure 134: Example of Passive Cluster Node Offline

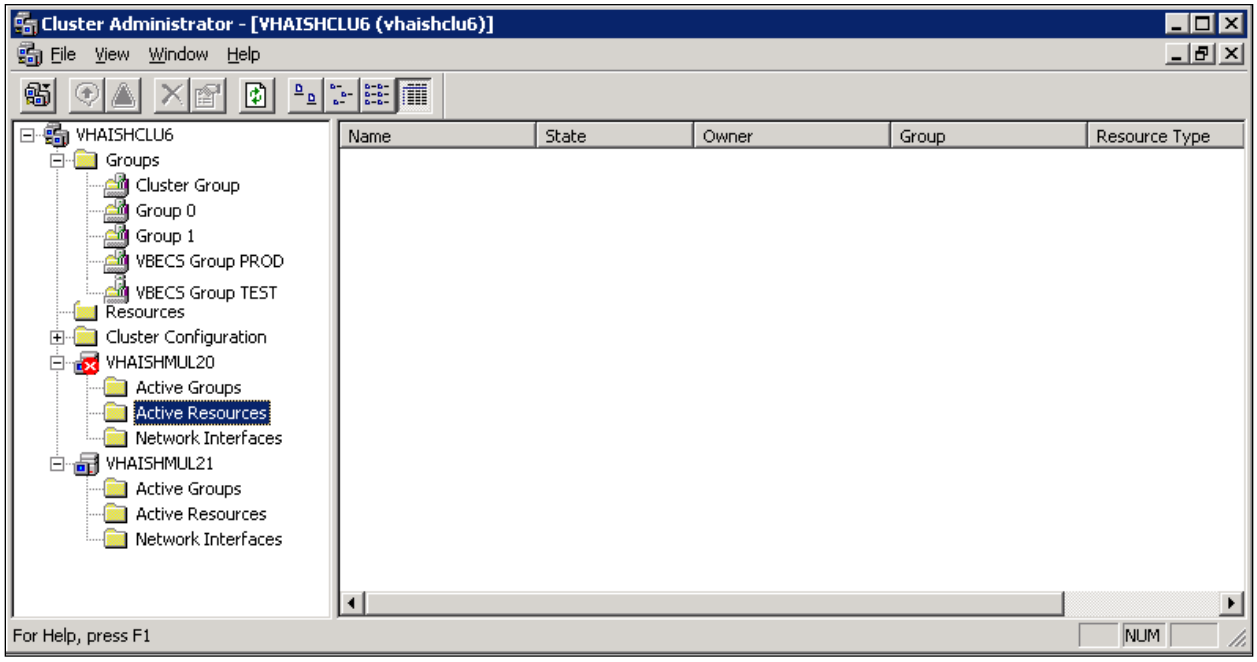
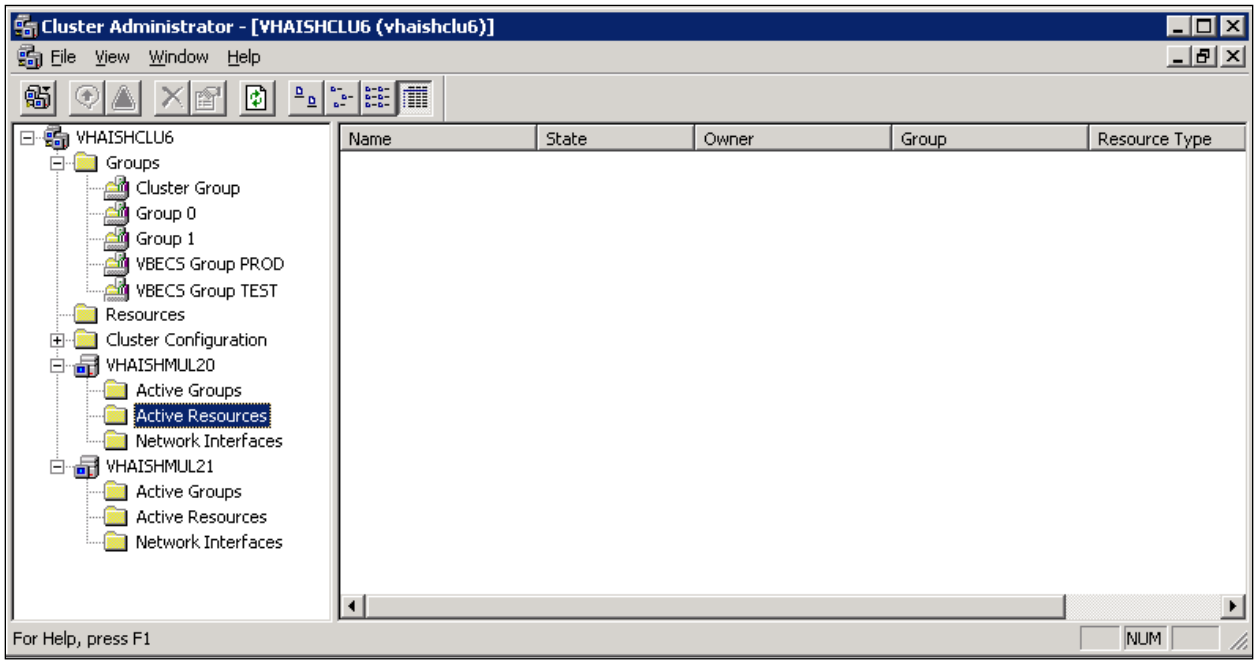


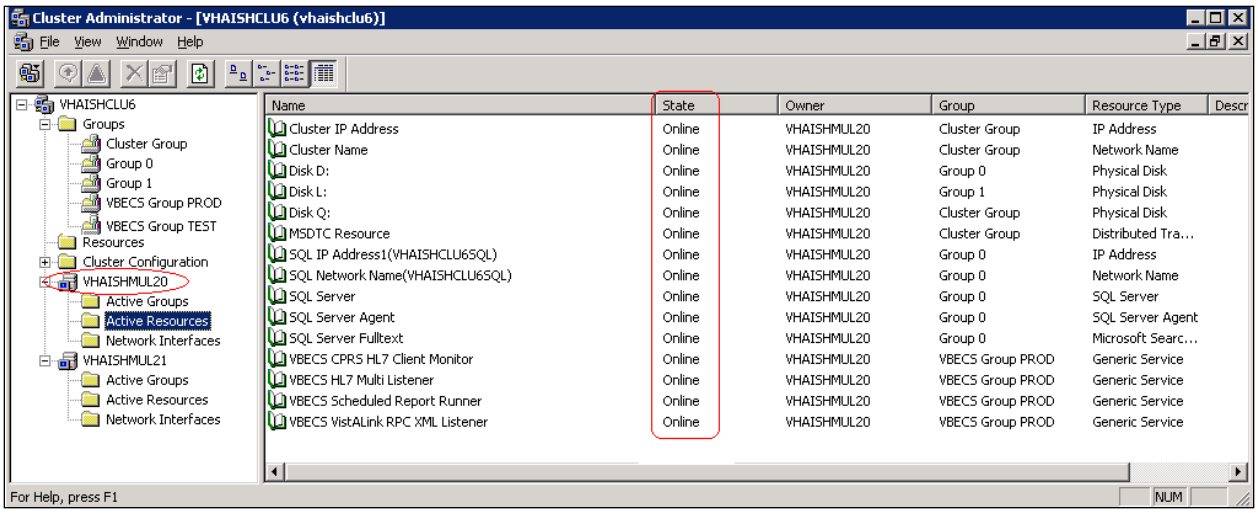
Figure 135: Example of Passive Cluster Node Online



23) Log off the Remote Desktop Connection.
24) Restart (reboot) the active node (cluster node 1).

25) After cluster node 1 has been restarted, restart (reboot) cluster node 2.
26) Open a remote desktop connection to the cluster; click **Start, Administrative Tools, Cluster Administrator.**
27) If **Open Connection to Cluster** window does not appear, click **File, Open Connection**.
28) Type <***CLUSTER_NAME***> in the **Cluster or server name** field and click **OK**.
29) Verify that all Active Resources of the active node (cluster node 1) have State marked Online (Figure 136).

Figure 136: Example of Active Cluster Node Resources Online



If resource(s) state remains offline, please file a Remedy ticket immediately.

VBECS Exception Logging

VBECS logs all errors that occur in the system in the application event viewer on the cluster. A user defined as an administrator on the cluster can connect to the cluster through Remote Desktop Connection to view these errors.

1) Click **Start**, **Control Panel, Administrative Tools**.
2) Open the Event Viewer and select the Application log to view the errors that VBECS logs.
3) Double-click the application icon on the right side of the screen list view.
4) In the list view on the right side of the screen, click the date column header to sort the errors by date.
5) Evaluate "Error" and warning errors and submit a Remedy ticket if the error was logged at the same time a VBECS user reported an error. Ignore informational messages. The VBECS development and maintenance team will investigate the ticket.

VBECS Exception Workarounds

When an exception occurs in VBECS, click **Copy to Clipboard**. Paste all details of the exception in a Remedy ticket. A common exception that occurs within VBECS was traced to a Microsoft .NET 2003 problem that will not be resolved until VBECS is upgraded with the implementation of Microsoft .NET 2010. The exception shows in the details:

1) Exception Information

****

Exception Type: System.NullReferenceException

Message: Object reference not set to an instance of an object.

TargetSite: IntPtr CallWindowProc(IntPtr, IntPtr, Int32, IntPtr, IntPtr)

HelpLink: NULL

Source: System.Windows.Forms

StackTrace Information

****

at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr wndProc, IntPtr hWnd, Int32 msg, IntPtr wParam, IntPtr lParam)

at System.Windows.Forms.NativeWindow.DefWndProc(Message& m)

at System.Windows.Forms.Control.DefWndProc(Message& m)

at System.Windows.Forms.Control.WmUpdateUIState(Message& m)

at System.Windows.Forms.Control.WndProc(Message& m)

at System.Windows.Forms.ScrollableControl.WndProc(Message& m)

at System.Windows.Forms.ContainerControl.WndProc(Message& m)

at System.Windows.Forms.ParkingWindow.WndProc(Message& m)

at System.Windows.Forms.ControlNativeWindow.OnMessage(Message& m)

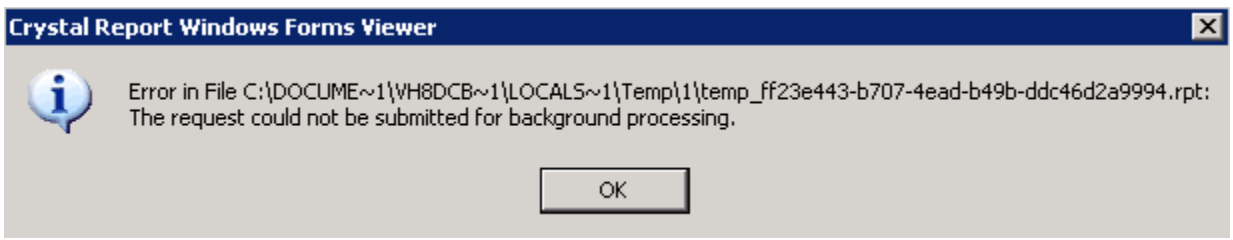
at System.Windows.Forms.ControlNativeWindow.WndProc(Message& m)

at System.Windows.Forms.NativeWindow.Callback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)

This exception occurs randomly when a screen is loading. When this occurs, the user must click **Shut down** on the exception message and try the option again.

When the user prints a report that accepts a given date range, a Crystal Report Windows Forms Viewer window may appear (Figure 137).

Figure 137: Example of Crystal Reports Message



The user may change the date range given (alter the start or end date by plus or minus one day) to resolve this problem. (This documented Crystal problem will be fixed in a future version of VBECS).

VBECS Application Interfaces

Table 9: 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 HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server.	Start or restart the VBECS HL7 Multi Listener Windows Service.
		Network connectivity issue	Contact local system support.
		The HL7 message is missing patient last or first name or one or more name components length(s) exceed(s) the VBECS maximum supported value.	VBECS responds to the new order request with an application reject (AR) acknowledgement message indicating Patient Name(s) not found in HL7 Message or Patient's Name(s) field size(s) exceed(s) VBECS maximum supported value. Rejected patient order messages due to invalid patient name message content are recorded on the Windows Event Log and an email message containing the MSH segment of the rejected HL7 message.
VBECS Admin: Configure Division	New orders are not showing up in VBECS.	Order mappings to institutions within a division's configuration were changed.	Stop and restart the VBECS HL7 Multi Listener Service.
VBECS: Patient Update Alerts	VistA patient updates are not showing up in VBECS.	The patient being updated in VistA is not in the VBECS Patient table and is, therefore, not a Blood Bank patient.	No action is required.
		The fields that were updated in VistA are not stored in VBECS, therefore, no data will be updated.	No action is required.
		The Taskman scheduled option VAFC BATCH UPDATE is not scheduled to run or has not reached the time limit in the schedule.	Schedule the VAFC BATCH UPDATE option to run at the desired increment or use the option "One-time Option Queue" in the Taskman Management Options to start the task.
		The VBECSPTU Logical Link is not running on the VistA system.	Start the VBECSPTU Logical Link.

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

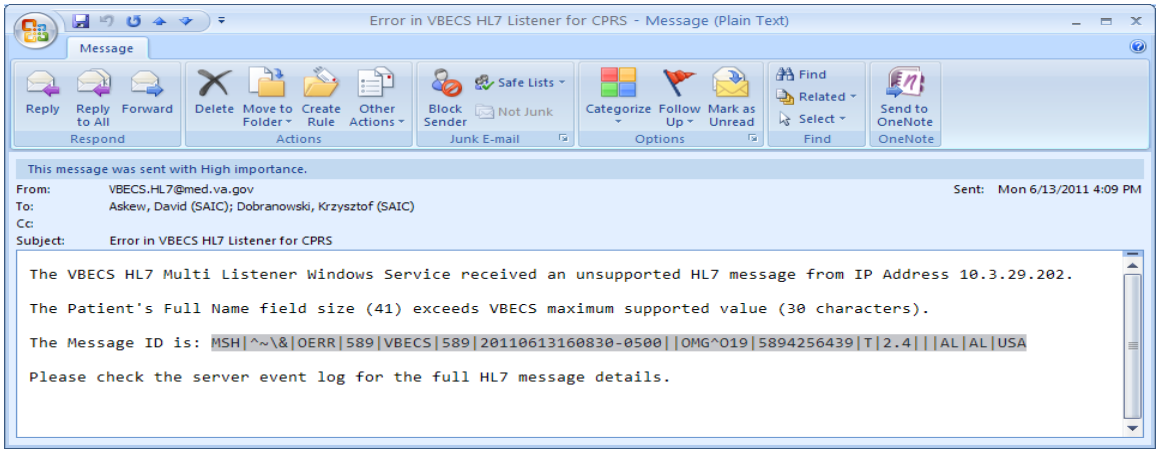
Source	Description of Problem	Possible Cause	Solution
	for the OERR-VBECS Logical Link and is hung in an "Open" state.	Network connectivity issue	Contact local system support.
	The VistA HL7 System Link Monitor shows more MESSAGES TO SEND than MESSAGES SENT for the VBECSPTU Logical Link and is hung in an "Open" state.	The VBECS HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server.	Start or restart the VBECS HL7 Multi 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 HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server.	Start or restart the VBECS HL7 Multi 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 CPRS Client Monitor Windows Service is not running or is locked on the VBECS Cluster server.	Start or restart the VBECS CPRS Client Monitor Windows Service.
		The VBECS-OERR Logical Link is not running.	Start the VBECS-OERR Logical Link in Background mode.
		Network connectivity issue	Contact local system support.
CPRS: Blood Bank Order Dialog	CPRS displays "Not able to open port" message in Patient Information screen in Blood Bank Order Dialog.	The VBECS VistALink XML RPC Listener Service is not running or is locked on the VBECS Cluster server.	Start or restart the VBECS VistALink XML RPC Listener Service.
		Network connectivity issue	Contact local system support.
CPRS: Reports Tab, Blood Bank Report	CPRS displays "`----BLOOD BANK REPORT IS UNAVAILABLE----`"	The VBECS VistALink XML RPC Listener Service is not running or is locked on the VBECS Cluster server.	Start or restart the VBECS VistALink XML RPC Listener Service.
		Network connectivity issue.	Contact local system support.
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 HL7 Multi Listener Windows Service, which caused a failure to respond to CPRS with acceptance.	Log onto the VBECS Cluster Server and review the System Application Event Log for error details.
		Network connectivity issue.	Contact local system support.
VBECS Cluster 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 HL7 Multi 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.

Source	Description of Problem	Possible Cause	Solution
	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 Cluster 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 HL7 Multi 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 Cluster Server Application Event Log: Source is CPRS HL7 Parser	An HL7 message sent from CPRS to VBECS was rejected. The description in the Event Log is "Exception message: Division [*division]* is not supported by this instance of VBECS."	An invalid or unsupported division associated with the Patient Location was selected in CPRS when the order was created.	The order must be created in CPRS again with a valid Patient Location associated with a VBECS-supported division.
	An HL7 message sent from CPRS to VBECS was rejected. The description in the Event Log is "Exception message: Unable to find valid Associated Institutions information. Please check configuration in VBECS Admin."	Clinician logs into VistA with a division that is not mapped to VBECS.	The order must be created in CPRS again with a division that is mapped to VBECS.

Finding Application Log Entries from Email Alerts

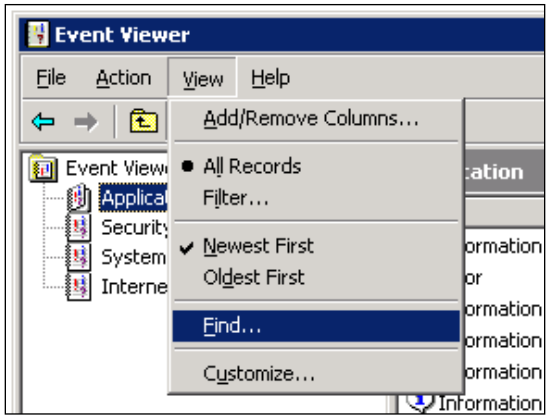
1) When HL7 message patient last or first name components length(s) exceed(s) the VBECS maximum supported value of 30, an email will be received (Figure 138).

Figure 138: Example of Error in VBECS HL7 Listener for CPRS



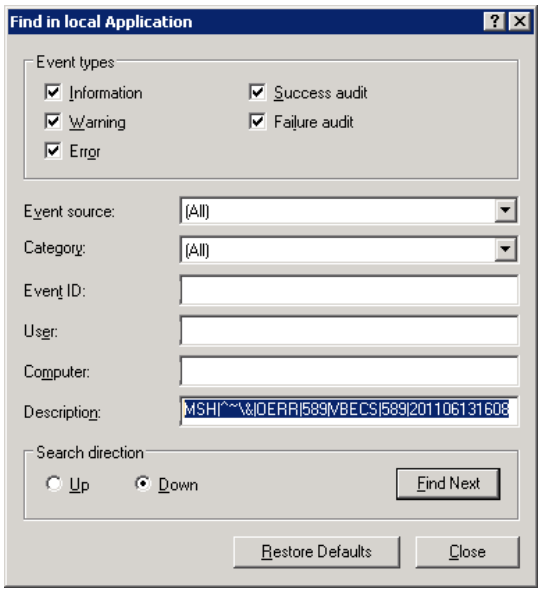
2) Click **Start, Administrative Tools, Event Viewer**.
3) Select **Application Log**, **View**, **Find** (Figure 139).

Figure 139: Example of Event Viewer



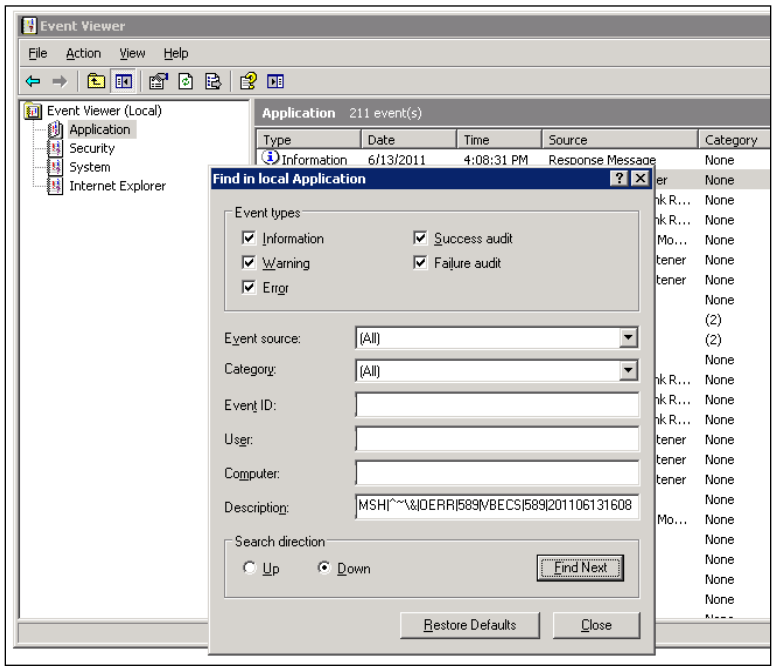
4) Enter the **MessageID** highlighted in the email received (Figure150) in the **Description** field. Click **Find Next** (Figure 140).

Figure 140: Example of Find in Local Application



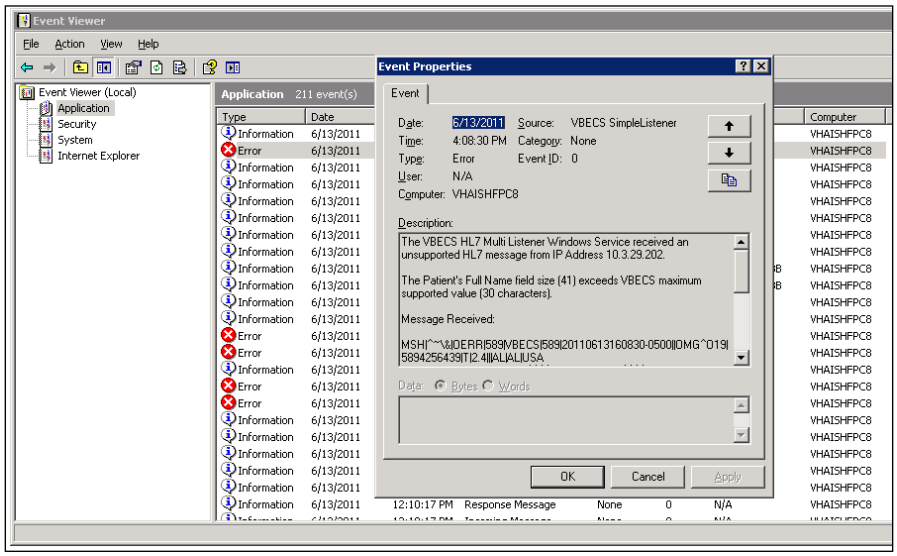
5) When the event record has been found, the row will be highlighted. Click **Close** to close the Find utility (Figure 141).

Figure 141: Example of Find in Local Application Description



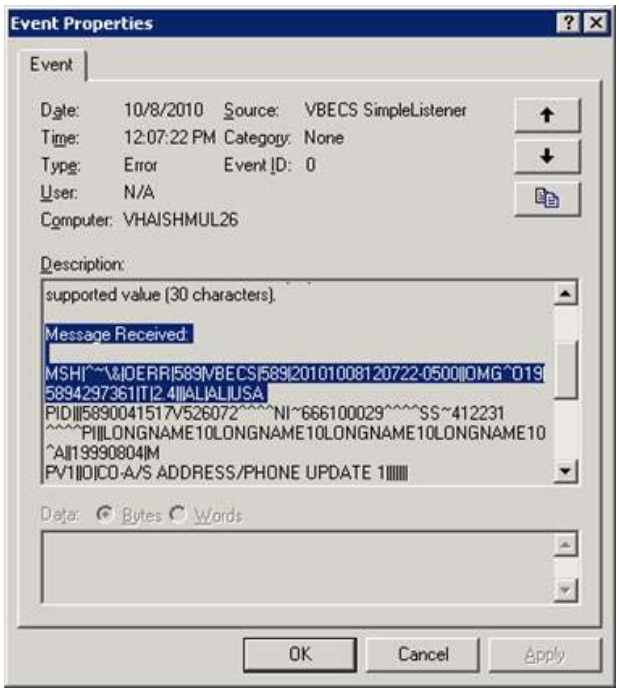
6) Double-click on the highlighted row (Figure 142).

Figure 142: Example of Event Properties



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 143).

Figure 143: Example of Analyzing Event Properties



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.

Cluster Connectivity Lost

Problem: Connections to the cluster are lost. The cluster is not pingable by name or IP address, but individual nodes are still up.

Probable Cause: A network outage that affects both nodes simultaneously will cause the cluster to fail.

Solution:

1) Log into one of the cluster nodes and restart. Wait 5 minutes.
2) Restart the other cluster node.
3) After the node in Step1 has finished rebooting, verify that the cluster is back up.
4) When both nodes have restarted, stop and start services per the instructions in the previous section.

Printing Fails to Report Printer

Problem: The printer fails to print.

Probable Cause: A printer name is not consistent with what is configured in VBECS or a driver is incorrect.

Solution:

Verify Printer Name

1) Log into VBECS Administrator and note the default printer in Configure Division.
2) Verify that the printer name on the server is consistent with the name noted in step 1.
3) If still broken, verify printer drivers are consistent.

Verify Printer Drivers

1) Log into one of the servers with administrator rights.
2) Open **Control Panel**, **Printers and Faxes**.
3) Double-click the printer noted in step 1 under **Verify Printer Name**.
4) Select **Printer**, **Properties** and click the **Advanced** tab.
5) Note the driver name in the **Driver** field.
6) Repeat Steps 1 through 5 on the other server. If drivers are inconsistent, update the server that is not working with the correct driver.

Zebra Printer Problems

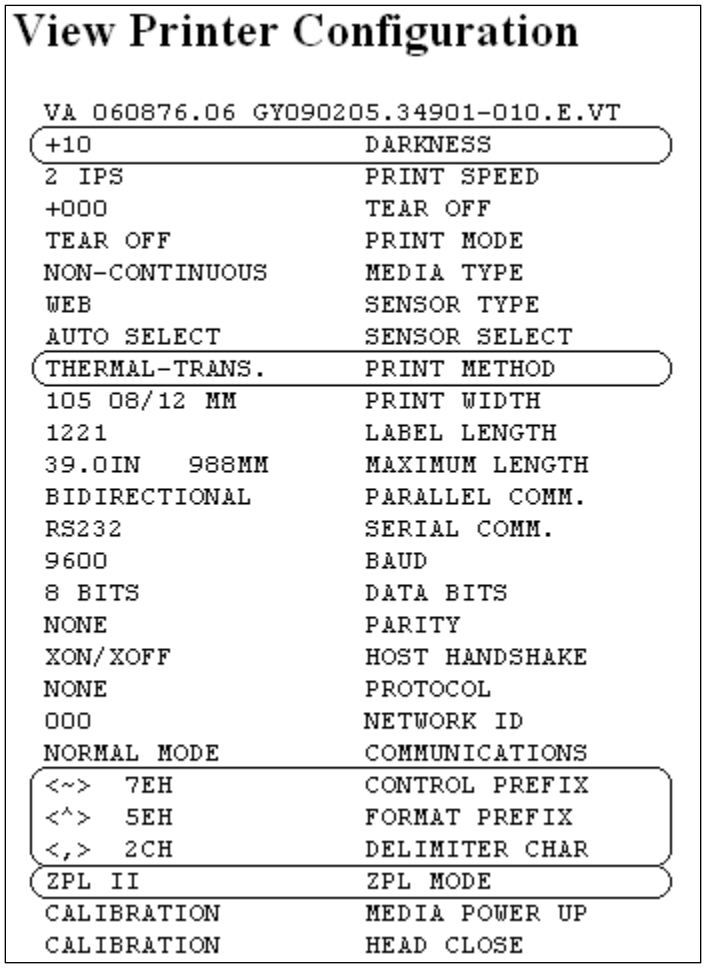
Printer IP address must be added to the Access Control List (ACL).

Problem: The printer prints, but there is not 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 144).

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

Figure 144: Example Zebra Printer Settings

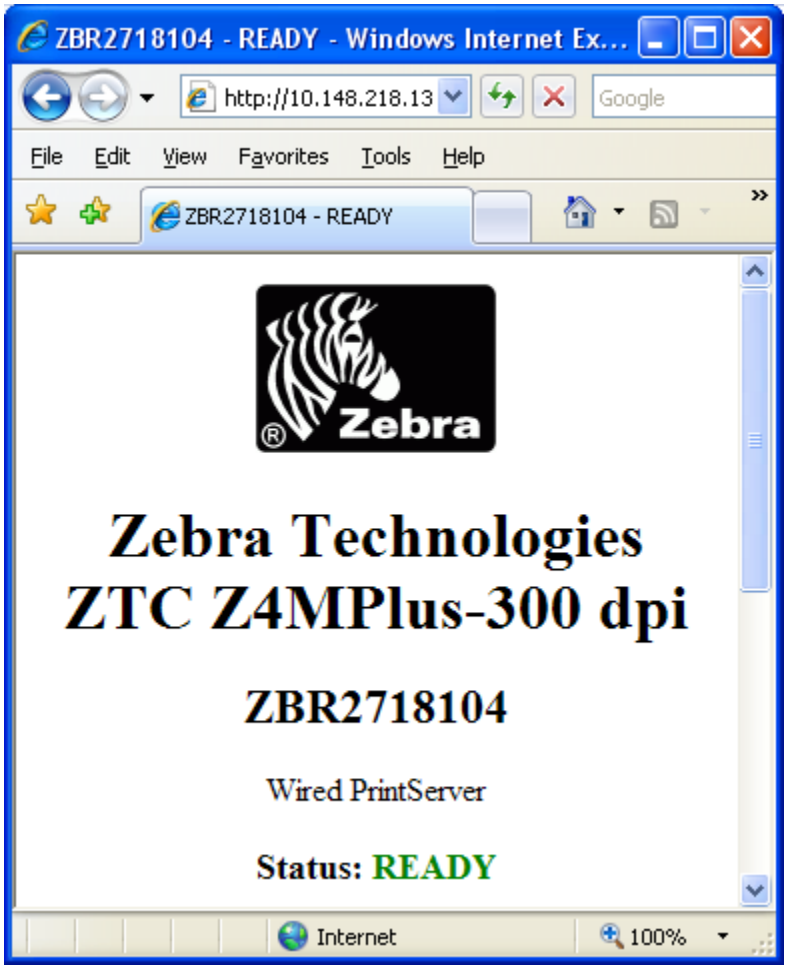


Problem: The printer doesn't print. It also cannot be pinged or be seen in a web browser (Figure 145).

Probable Cause: Network settings are not correct on the printer

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

Figure 145: Example of Zebra Printer Web Console



Problem: The printer doesn't 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 144.

Scanner Problems

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 compter** (Figure 146). 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 147 through Figure 154 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.

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.

Figure 146: On the local computer

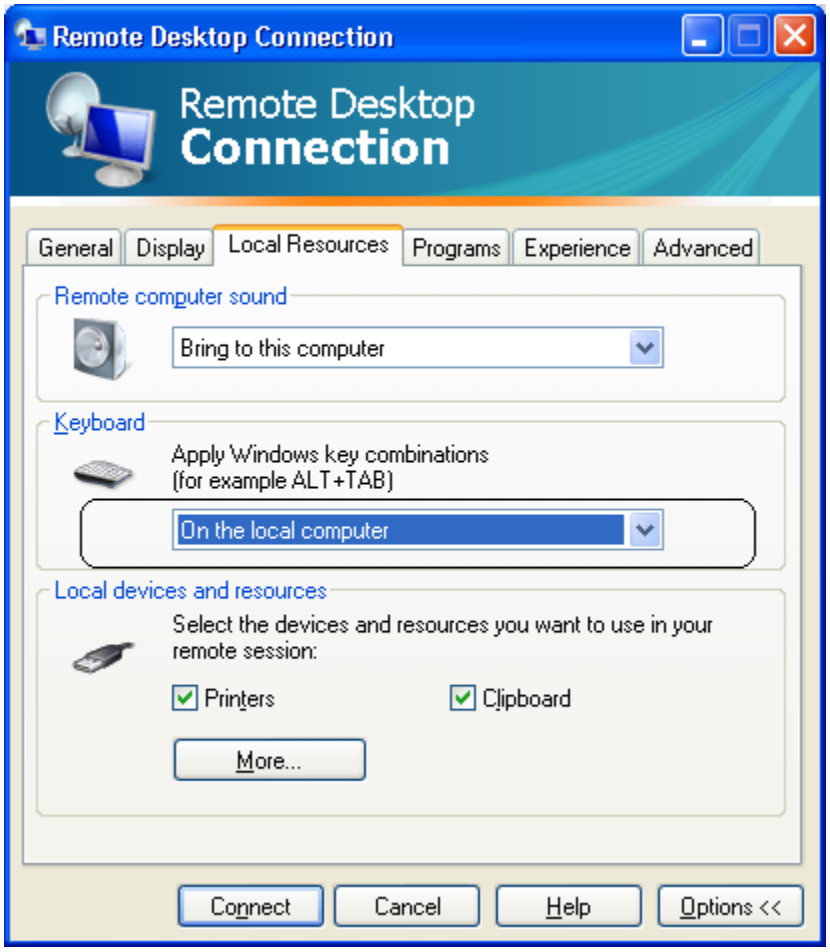


Figure 147: 10 milliseconds

Figure 148: 20 milliseconds

Figure 149: 30 milliseconds

Figure 150: 40 milliseconds

Figure 151: 50 milliseconds

Figure 152: 60 milliseconds

Figure 153: 70 milliseconds

Figure 154: 80 milliseconds

VBECS FTP Download Issues

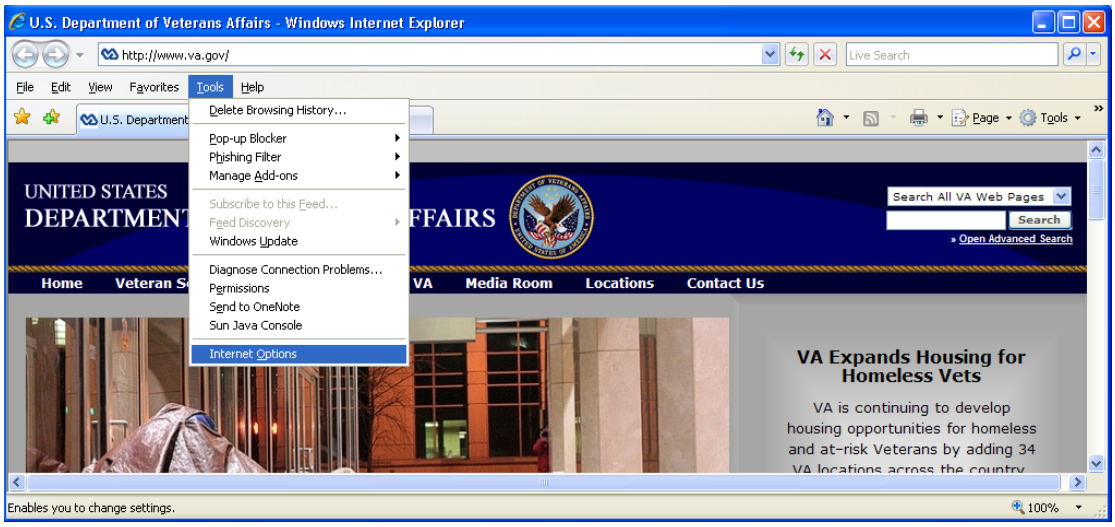
Problem: VBECS FTP Download Security Alert with message 'Your current settings do not allow you do download files from this location'

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

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

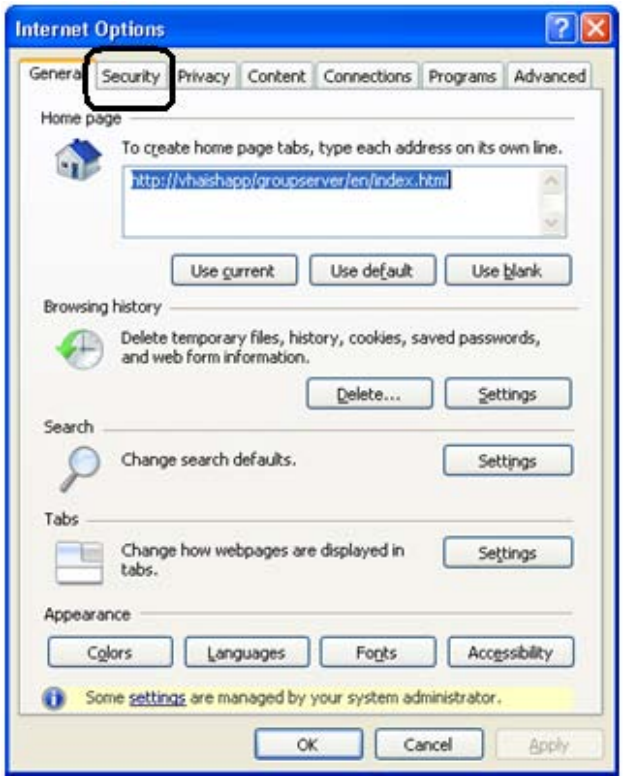
1) Open a remote desktop connection to cluster node 1.
2) Open Internet Explorer and select **Tools, Internet Options** (Figure 155).

Figure 155: Example of Internet Explorer Window



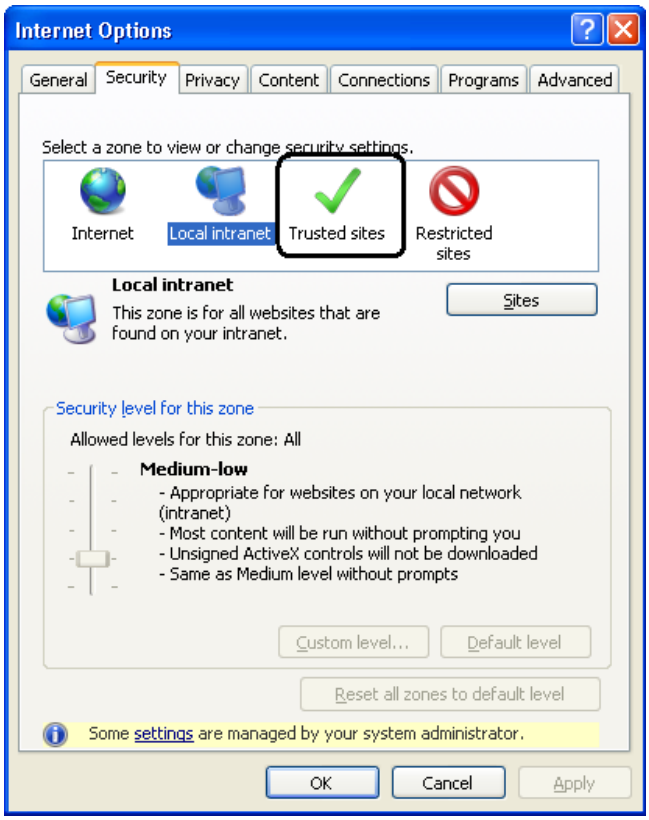
3) Select the **Security** tab (Figure 156).

Figure 156: Example of Internet Explorer Internet Options Security tab



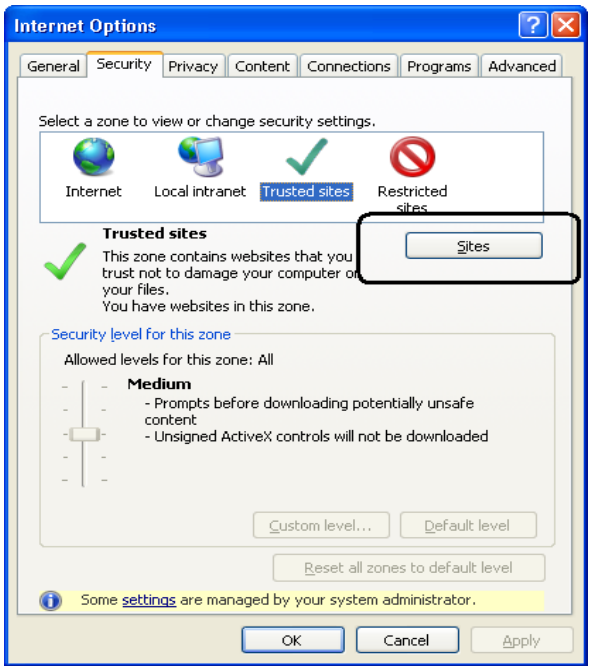
4) Select **Trusted sites** (Figure 157).

Figure 157: Example of Internet Options Trusted Sites



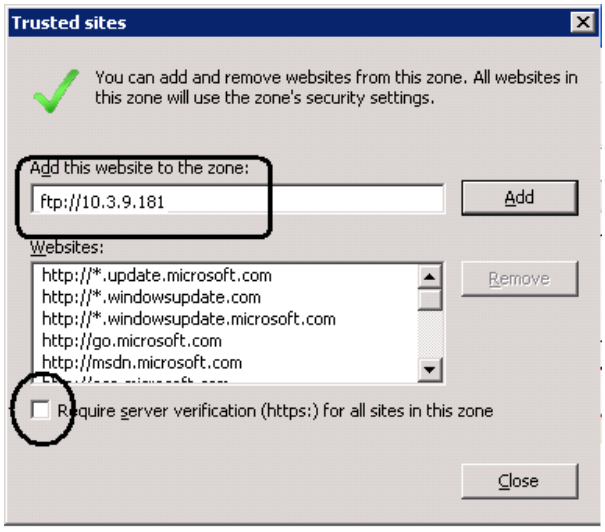
5) Click **Sites** (Figure 158).

Figure 158: Example of Select a Zone to View or Change Security Settings



6) Make sure **Require server verification**… is unchecked. Enter **ftp://10.3.9.181** and click the **Add** button (Figure 159).

Figure 159: Example of Adding the VBECS FTP to the Trusted Sites



7) Close all windows.
8) Log off cluster node 1.
9) Repeat Steps 1 through 8 for cluster node 2.

This page intentionally left blank.

Archiving and Recovery

The VBECS database will be backed up once daily at an established time to a tape drive. If a disaster occurs, the data in VBECS can be recovered from the backup media.

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

- Only the VBECS data is backed up. The operating system is not backed up. In the event of a disaster, the operating system will have to be reinstalled and configured.

Additional Information

- None

VBECS Backup

If your servers are maintained at a data center, ignore this section since data center personnel will perform this task.

To preserve VBECS data in case of database corruption or destruction of hardware, the VBECS databases are copied over to shared storage via a scheduled job configured with the VBECS installation. VBECS is comprised of the following SQL databases: VBECS_V1_PROD and VBECS_V1_PROD_MIRROR (production) VBECS_V1_TEST and VBECS_V1_TEST_MIRROR (test VBECS account). Both production and test share the use of the msdb and master SQL databases. It is critical that every VBECS database is backed up nightly to tape. Remove the tape and take it to another location in accordance with local policy. For more technical details on backups, see *VistA Blood Establishment Computer Software (VBECS) Installation Guide*. For details on tape storage and backup frequency, refer to local policy.

VBECS Recovery

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 regulation.

If your servers are maintained at a data center, ignore this section since data center personnel will perform this task.

File a Remedy ticket in the event of a disaster that destroys or damages the VBECS system. The VBECS team and VA Product Support will work to recover or rebuild the system.

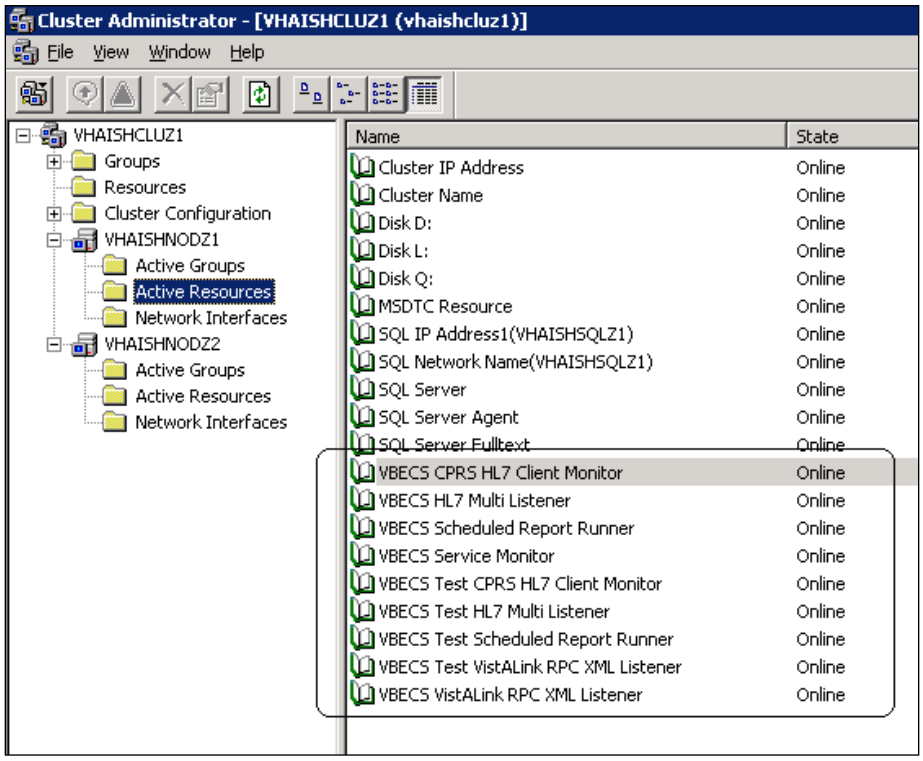
Reinstall the System

If your servers are maintained at a data center, ignore this section since data center personnel will perform this task.

This section should not be followed once application data has been entered. Following these steps will cause all VBECS application data to be lost.

1) Install the image on the server hard drive.
2) Reinstall VBECS using *VistA Blood Establishment Computer Software (VBECS) Installation Guide*.
3) Make sure all VBECS Services are stopped on both servers. All VBECS service names begin with "VBECS" (Figure 160). To stop a service, open Cluster Administrator and take all VBECS Services offline.

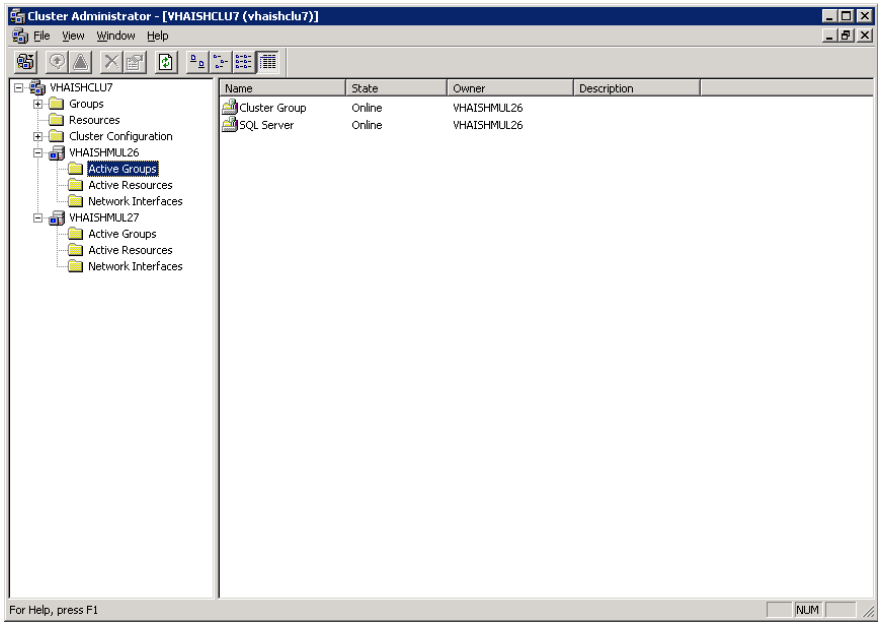
Figure 160: Example of VBECS Services



4) Log onto the server that is connected to the tape drive and has Backup Exec installed on it. Log in as an Administrator.

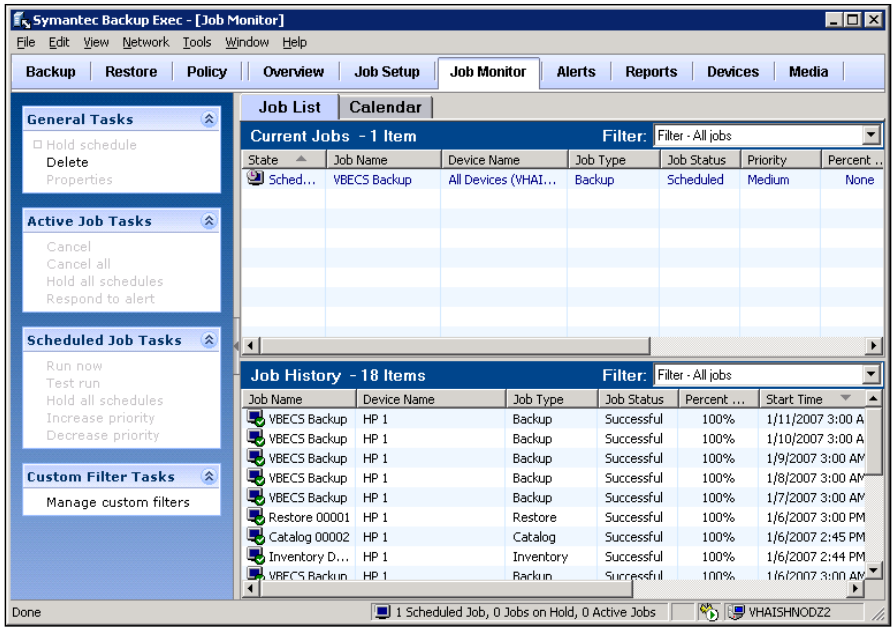
5) In Cluster Administrator (Figure 161), make sure this node is the active node in the cluster. If not, drag Cluster Group and SQL Server to the Active Groups folder of this node to make it the active node.

Figure 161: Example of Cluster Administrator



6) Click **Start**, **All Programs**, Symantec **Backup Exec 10d for Windows Servers**. The main Backup Exec console is displayed (Figure 162).

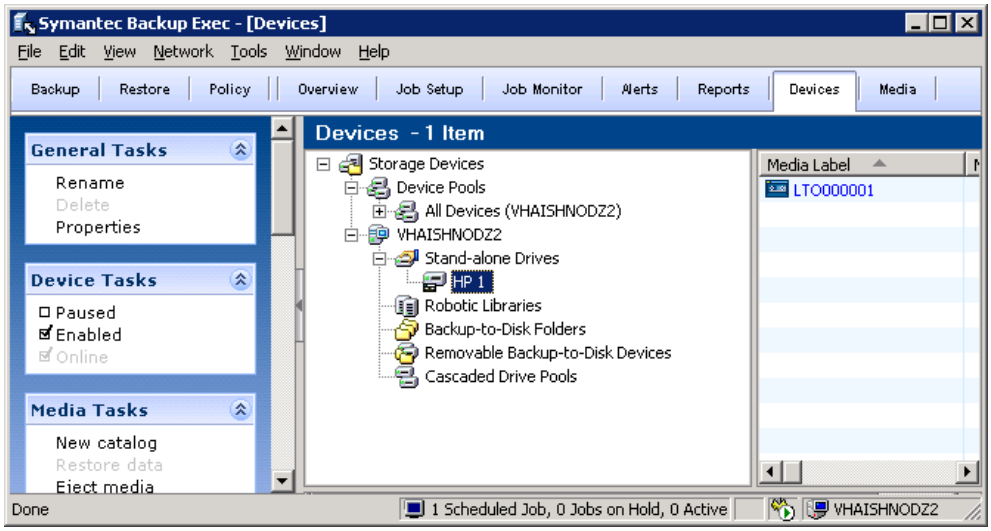
Figure 162: Example of Backup Exec Console



Inventory the Tape

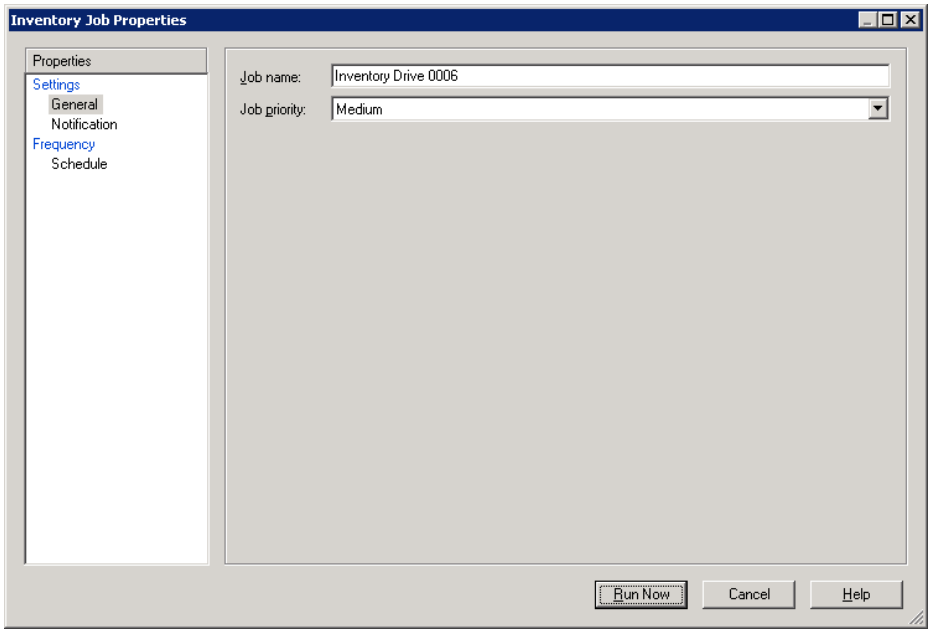
1) Place the tape that reflects the most recent system backup in the tape drive.
2) Click the **Devices** button (Figure 163).
3) Right-click **HP 1** under the cluster node (not the drive pool).
4) Select **Inventory**. The Inventory Job Properties window appears (Figure 164).

Figure 163: Example of Devices



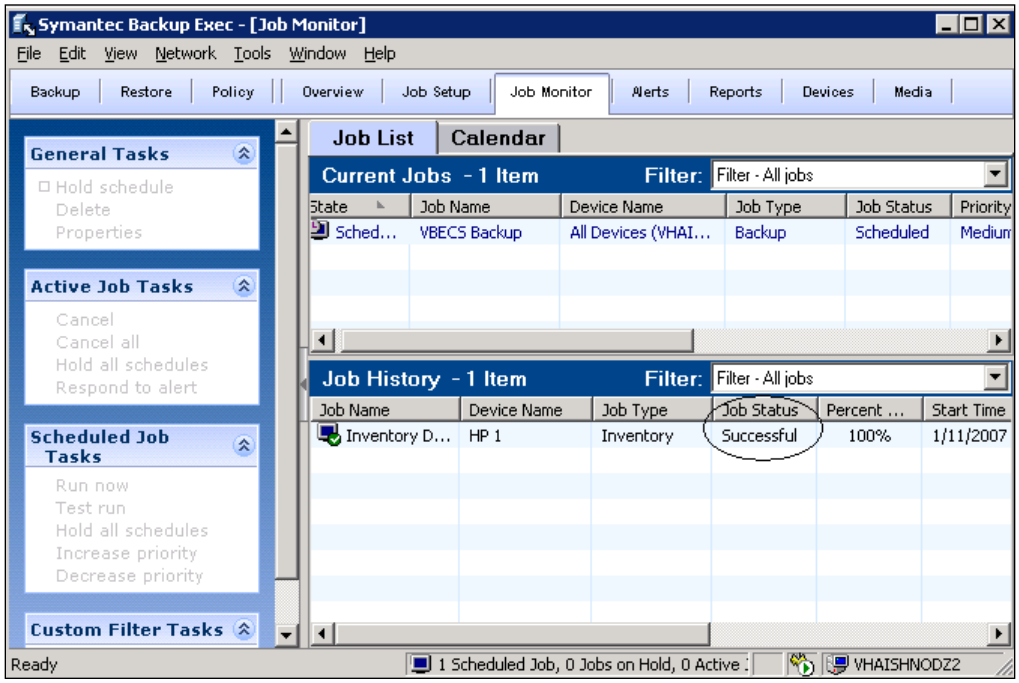
5) Click **Run Now**. Click **OK** to close information messages that appear.

Figure 164: Example of Inventory



6) Click **Job Monitor** (Figure 165) and make sure the job completed successfully.

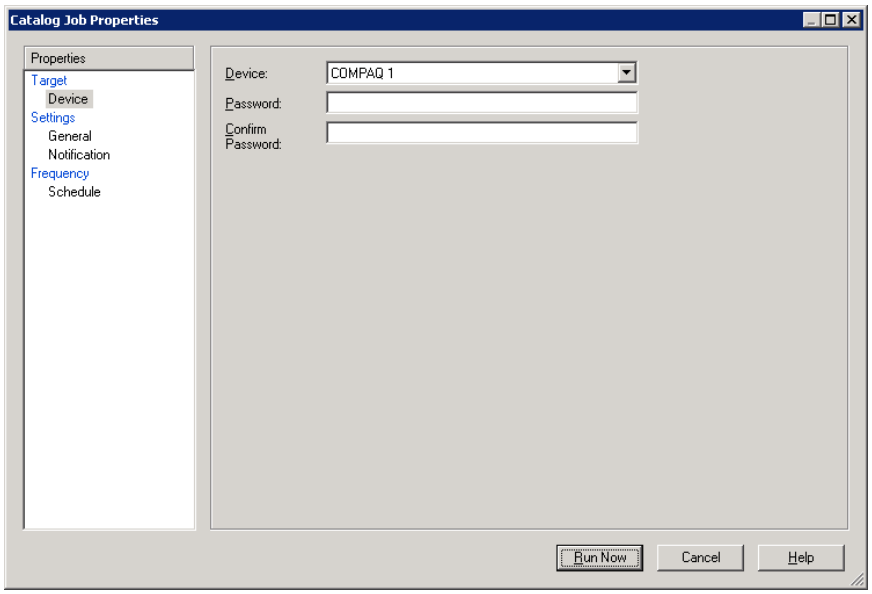
Figure 165: Example of Successful Inventory



Catalog the Tape

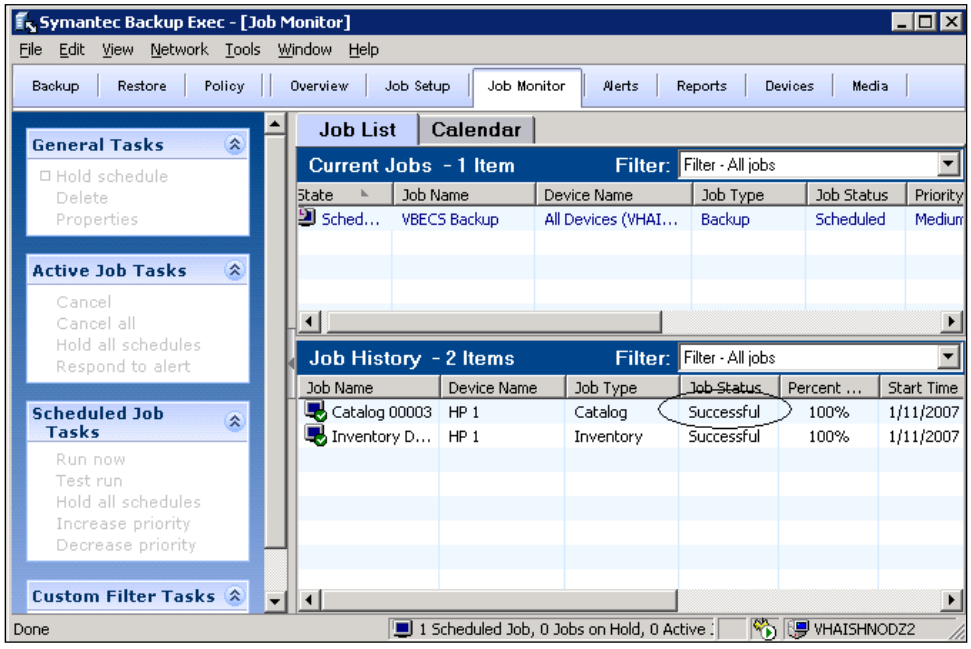
1) Click **Devices** again. Right-click **HP 1** under the cluster node.
2) Select **Catalog**. The Catalog Job Properties window appears (Figure 166). Click **Run Now**. Click **OK** to close information messages that appear.

Figure 166: Example of Catalog



3) Click **Job Monitor** (Figure 167) and make sure the job completed successfully.

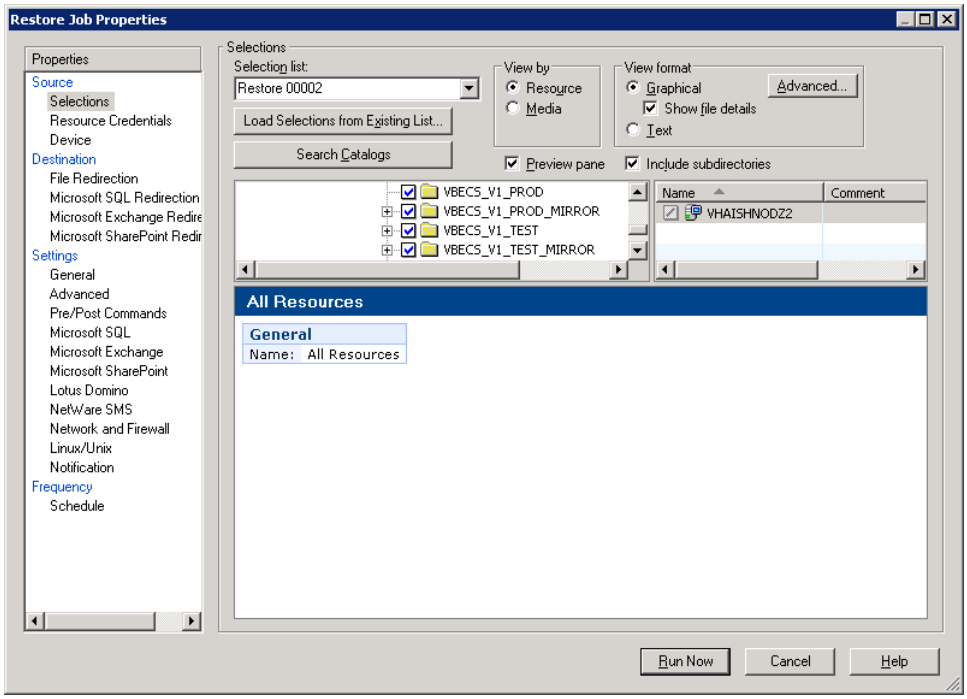
Figure 167: Example of Successful Catalog



Restore Files

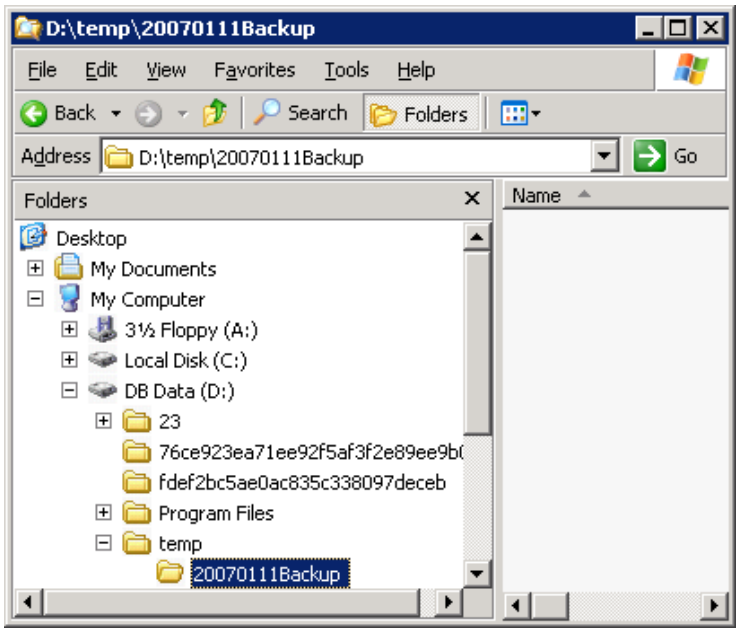
1) Click **Restore**.
2) Select all four folders under temp\Backup (Figure 168).

Figure 168: Example of Restore Properties



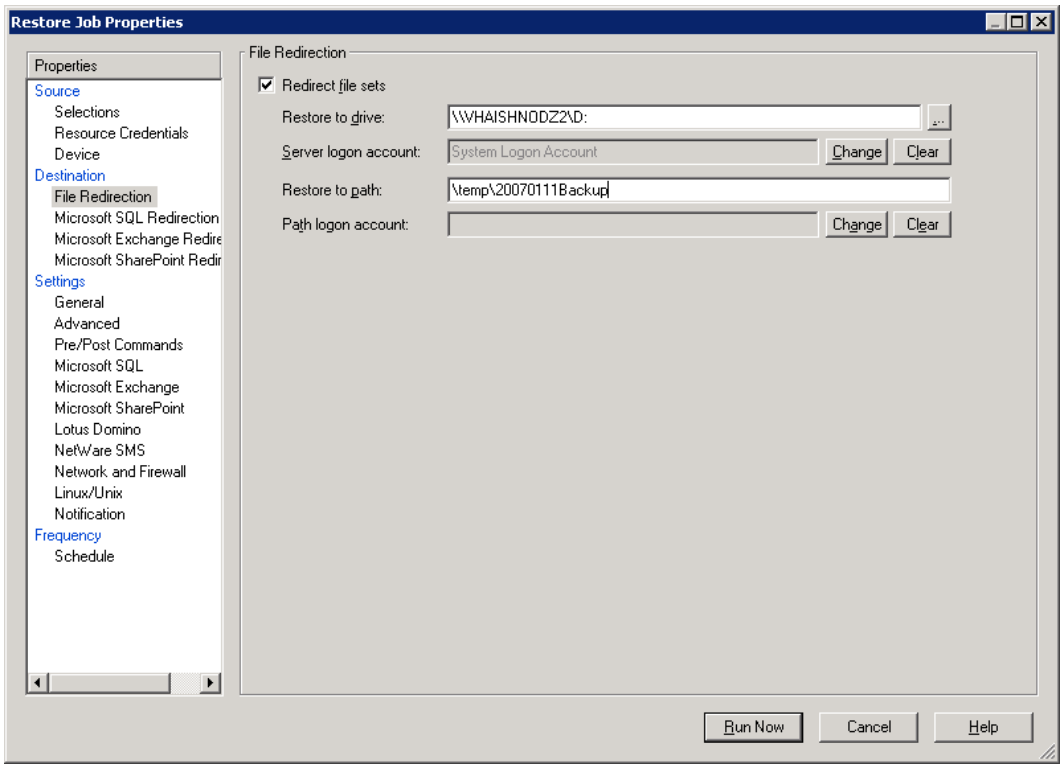
3) Create the "**temp\yyyymmddBackup**" directory on the D: drive (Figure 169).

Figure 169: Example of Backup Directory



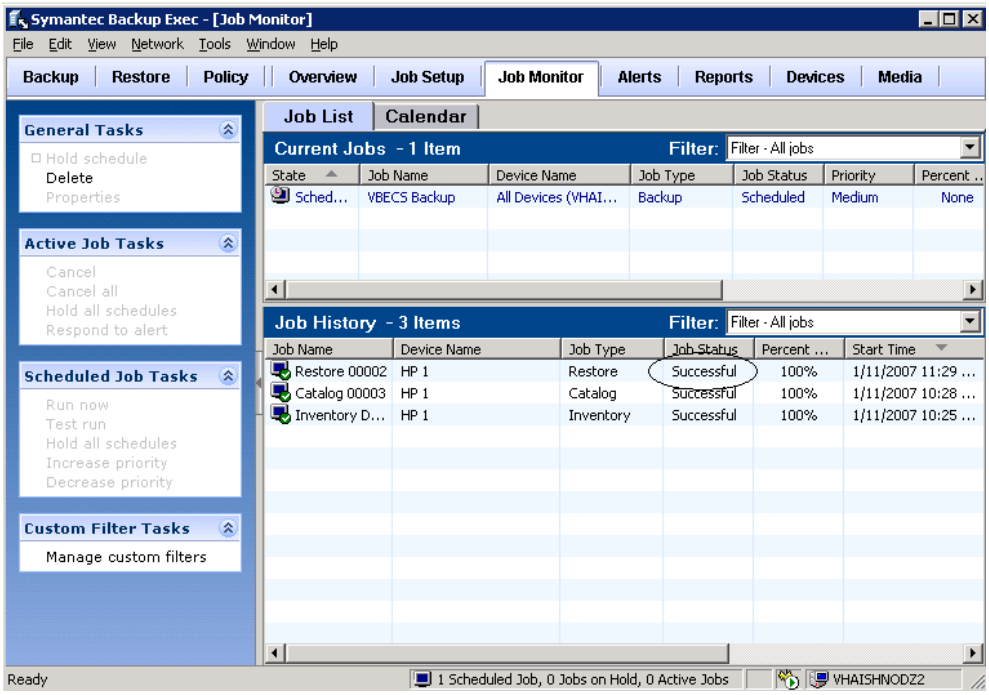
4) Click **File Redirection** on the left (Figure 170). Click the **Redirect file** sets check box.
5) In the Restore to drive field, enter **D:** (Backup Exec automatically populates the field with the server name).
6) In the Restore to path field, enter **D:\temp\yyyymmddBackup**\ (yyyymmdd represents the current date).
7) Click **Run Now**.
8) Click **OK** on information messages that appear.

Figure 170: Example of Restore Properties



9) Click **Job Monitor** (Figure 171) and make sure the job completed successfully.

Figure 171: Example of Successful Restore



Restore the Databases

If you find the need to perform a database restore, contact customer support to have qualified personnel assist you with the database restore.

VA Service Desk Primary Contact

For Information Technology (IT) support, call the VA Service Desk (VASD), 888-596-HELP (4357) toll free, 24 hours per day, 7 days per week. [Users with access to the VASD-supported request tool (e.g., Remedy) may file a ticket in lieu of calling the VASD.]

VA Service Desk Alternate Contacts

- During business hours: As an alternate to the toll-free number, call 205-554-4710 (or 205-554-4711 through 205-554-4725), Monday through Friday (excluding holidays), 8:00 a.m. to 7:30 p.m. (Eastern Time).
- Outside business hours: Call 205-554-3459 through 3462 or 3464, 3465, 3475, 3476, or 3482 through 3484 or 708-547-4671 through 4674.
- Web site: http://vaww.itsupportservices.va.gov/vasd_home.asp (VHA Enterprise Management Center).
- Email: vhacionhd@va.gov

This page intentionally left blank.

Failover

VBECS does not have a seamless failover mechanism. If one 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. It may take 30 to 60 seconds for the Windows cluster and SQL Server running on it to fail over, which will open on the secondary server (without the user being aware of it). 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:

- A server can fail in the VBECS cluster 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 fails over 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.
- VBECS can fail because of a power outage. The UPS device will sound an alarm to alert the staff that the power is out. The IRM staff will inform the VBECS users to save their work and exit the system before the battery runs out.
- A server may fail because of a subcomponent failure such as a network interface card failure. SCOM will monitor the servers for subcomponent failures. If a failure occurs, SCOM will alert the IRM.

If only one node in a cluster is damaged, failover will occur. The IRM must check the SCOM alerts for notification that the act occurred and fix the other node immediately to restore it to operation. When only one node is operating, no further failover can occur.

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.

If a server fails due to a hardware issue, such as a network interface card failure, a Remedy ticket must be entered. If this failure occurs on only one node, users may continue to use the software after the system successfully fails over. The failover process will occur in 90 seconds. If both nodes in the cluster fail, file a Remedy ticket and refer VBECS users to Downtime Forms and Instructions in the *VistA Blood Establishment Computer Software (VBECS) User Guide*.

This page intentionally left blank.

Performance

VBECS may delay a critical function such as patient transfusion if the network suffers latency issues. File a Remedy ticket when latency issues arise.

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

Locking

VBECS is designed with pessimistic locking controlled within the application code: if one user selects a record for edit, the record is locked by that user. If another user tries to edit that record, a message will tell him that the record is locked and who has the record. The second user is not granted access to the record.

Locks have a timeout period defined in the configure division portion of the VBECS Administrator application. When a lock times out or is released by a user completing his edit, another user can edit that record.

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

This page intentionally left blank.

Security

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

Active Directory

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

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

Group Policy

Group policy controls the user experience (what the user sees and has access to on the VBECS server). To configure this correctly, the recommendations in "Locking Down Windows Server 2003 Terminal Server Sessions" and "Windows Server 2003 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.

Virtual Local Area Network

As a medical device, VBECS must exist in a segregated part of the LAN [Virtual Local Area Network (VLAN)]. The VLAN is configured to only allow necessary communication in and out of the VBECS system. Unneeded ports are blocked.

System Center Operations Manager

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 installation process. SCOM will monitor these high-level categories:

- Windows Server 2003 Operating System
- CPU health and usage
- Network interface cards
- SQL Server
- Clustering
- Memory usage
- Hard disk health and usage
- VBECS executables and services
- Windows Services

Note: SCOM is the replacement for Microsoft Operations Manager (MOM.). Your site may still be using MOM, but will be automatically upgraded in the first half of 2012. These changes will be transparent to the site.

Application-Wide Exceptions

Table 10 explains system exceptions to aid VA Product Support in determining the cause and resolving system issues.

Table 10: 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.

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.
ABS	Antibody screen, antibody screen test.
Access Code	A field in the VistA New Person file used to uniquely identify a user on the VistA system.
ACL	Access Control List
Active Directory	A hierarchical directory service built on the Internet's Domain Naming System (DNS).
API	Application Programmer Interface.
CPRS	Computerized Patient Record System.
DBIA	Database Integration Agreement.
DSS	Decision Support System.
HCPCS	Healthcare Common Procedure Coding System.
HL7	Health Level Seven.
ICN	Integration Control Number.
LLP	Lower Layer Protocol.
LMIP	Laboratory Management Index Program.
MLLP	Minimal Lower Layer Protocol.
MOM	Microsoft Operations Manager.
OSI	Open Systems Interconnect.
OU	Organizational Unit.
PCE	Patient Care Encounter.
RDP	Remote Desktop Protocol.
RPC	Remote Procedure Call.
SCOM	System Center Operations Manager.
TCP/IP	Transmission Control Protocol/Internet Protocol.
UPS	Uninterruptible power source.
VAISS	VBECS Application Interfacing Support Software.
VBECS	VistA Blood Establishment Computer Software.
VDL	VA Software Document Library.
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.
VLAN	Virtual Local Area Network.
XML	Extensible Markup Language.

This page intentionally left blank.

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:

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

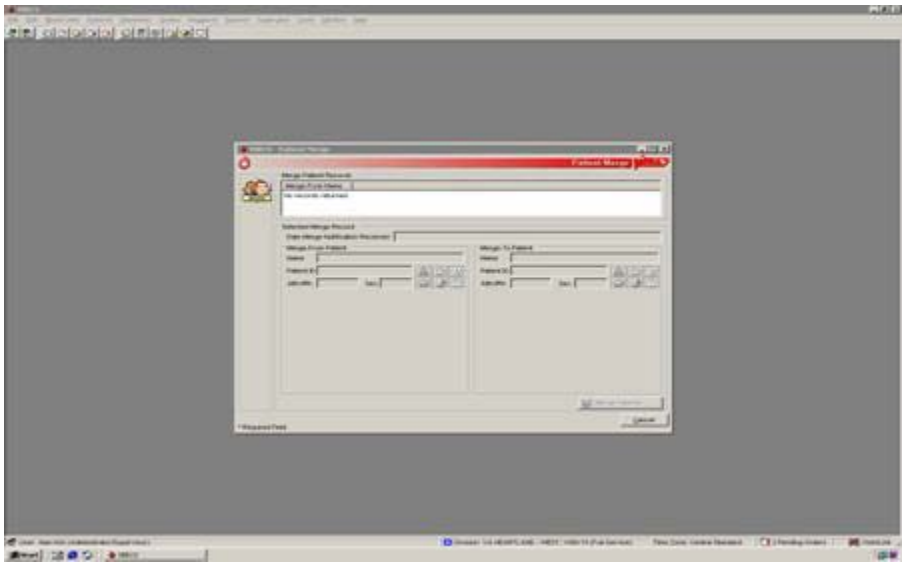
> *If you wish to place a document on both servers for ease of copying and pasting, assign file names similar to "mmyydd Technical-Security Validation Record Server1" and "mmyydd Technical-Security Validation Record Server2."*

2) When the screen you wish to capture is displayed, press the **Print Screen key**.
3) In the Technical-Security Validation Record document, place the cursor where you want to insert the picture.
4) Click  (the paste icon) or select **Edit**, **Paste (**Figure 172**)**.

Figure 172: Paste

5) Label the screen shot within the document with the technical manual-security guide step, page number, and server on which the picture was taken (Figure 173).

Figure 173: Example of Screen Shot



Appendix B: Workload Process Mapping to Application Option Table

Table 11 associates record saves with workload processes. The data fields identified for transmission at the completion of a Workload Event are based on current VistA workload-related files and fields. VBECS will transmit information to a new flat file. There are no donor workload types in VBECS.

Table 11: Workload Process Mapping to Application Option

Record Save Option	VBECS Process	Transaction Type [P (Patient), U (Unit), M (Miscellaneous)]	Explanation
Record a Transfusion Reaction Workup	ABO Forward and reverse typing (patient)	P	An ABO/Rh test for "pre" or "post" is enabled and a valid interpretation other than Not Tested is selected. A workload event is accrued separately for "Pre" and "Post" entries.
Record Patient ABO/Rh		P	Accrue workload when a CPRS-ordered ABO/Rh test is performed.
Invalidate Patient Test Results*		P	Accrue workload when a completed ABO/Rh test is invalidated.
Record Patient ABO/Rh	ABO Forward and reverse typing (patient) Repeat Test	M	Accrue workload when a reflex or repeat ABO/Rh test is performed, completed, and saved.
Invalidate Patient Test Results*		M	Accrue workload when a reflex or repeat ABO/Rh test is invalidated.
ABO/Rh Confirmation	ABO forward typing (unit)	U	An ABO confirmation test is performed. When multiple units are selected in a batch, each unit in the batch accrues a workload event. Note: Workload generated during Anti-D testing is not included in the unit's confirmation test. Workload is not accrued when an ABO or Rh discrepancy override is processed and VBECS releases all patient assignments. Workload is not accrued when VBECS quarantines the unit due to a discrepancy. There is no special handling for workload collection for additional confirmation tests on a unit.
Edit Unit Information*		U	Accrue workload when an ABO confirmation test is invalidated.
ABO/Rh Confirmation	ABO/Rh forward typing (unit)	U	An ABO/Rh confirmation test is performed. When multiple units are selected in a batch, each unit in the batch accrues a workload event. Note: Workload generated during Anti-D is part of the unit's confirmation test. Workload is not accrued when an ABO or Rh discrepancy override is processed and VBECS releases all patient assignments. Workload is not accrued when VBECS quarantines the unit due to a discrepancy. Any unit successfully confirmed accrues workload. For split modifications: workload is not inherited by split units. A split unit that requires confirmation accrues confirmation workload at the time of testing. There is no special handling for workload collection for additional confirmation tests on a unit.
Edit Unit Information*		U	Accrue workload when an ABO/Rh confirmation test is invalidated.
Accept Order	Accept Order	M	Accrue workload when an order is accepted. When a multiple orders are selected, each order accrues workload.

Enter Antibody Identification Results	Antibody identification Work-Up	P	User enters additional workload associated with the individual reflex-ordered ABID. The selected VBECS multiplier will multiply against the VistA multiplier and display the (multiplication) product on the Division Workload Report.
Invalidate Patient Test Results*		P	Accrue workload when the ABID is invalidated.
Record a Transfusion Reaction Workup	Antibody Screen (patient)	P	An ABS test for “pre” or “post” is enabled and a valid interpretation other than Not Tested is selected. A workload event is accrued separately for “Pre” and “Post” entries.
Record Patient Antibody Screen		P	Accrue workload when an ordered ABS test is performed.
Invalidate Patient Test Results*		P	Accrue workload when a completed ABS test is invalidated.
Record Patient Antibody Screen	Antibody Screen (patient) Repeat Test	M	Accrue workload when a reflex or repeat ABS test is performed, completed, and saved.
Invalidate Patient Test Results*		M	Accrue workload when a reflex or repeat ABS test is invalidated.
Unit Antigen Typing / Patient Antigen Typing	Antigen phenotyping, Single Test phase (QC)	M	Accrue workload when Antiserum QC in Unit or Patient Antigen Typing includes the testing of both the positive and negative control cells, per specificity by lot number, when only one phase of reactivity is chosen for the test grid (IS or AHG). One workload event is collected per completed tab for regular or repeat antigen tests.
Unit Antigen Typing / Patient Antigen Typing	Antigen phenotyping, Multiple Test phases (QC)	M	Accrue workload when Antiserum QC in Unit or Patient Antigen Typing includes the testing of both the positive and negative control cells, per specificity by lot number, when only multiple phases of reactivity are chosen for the test grid, IS/RT, RT/37, or weak D. One workload event is collected per completed tab for regular or repeat antigen tests. When weak D is the selected test, QC may not be accrued for the rack selection. QC is accrued when positive and negative cells must be tested for the lot number.
Cancel Pending Order	Cancel Order	M	Accrue workload when an order on the pending order list is canceled. When multiple orders are canceled, each order accrues workload.
Cancel Active Order	Cancel Order	M	Accrue workload when an order on the pending task list is canceled. When multiple orders are canceled, each order accrues workload.
Select Units for Crossmatch	Crossmatch unit, electronic	P	This process is invoked when an individual unit is selected for patient assignment and the unit is electronically crossmatched. When multiple units are selected, each unit accrues workload.
Enter Crossmatch Results	Crossmatch unit, serologic immediate spin	P	Accrue workload when an individual unit crossmatch is selected to include only the IS phase, is completed, and is saved. When multiple units are selected, each unit accrues workload.
Invalidate Patient Test Results*		P	Accrue workload when a completed crossmatch test is invalidated. This applies to the workload originally saved with the serologic immediate spin test.

Record a Transfusion Reaction Workup	Crossmatch unit, serological Coombs	P	A crossmatch test for “pre” or “post” is enabled and a valid interpretation other than Not Tested is selected. A workload event is accrued separately for “Pre” and “Post” entries. When multiple units are selected, each unit accrues workload.
Enter Crossmatch Results		P	Accrue workload when an individual unit crossmatch is selected to include all phases or only the AHG phase, is completed, and is saved. When multiple units are selected, each unit accrues workload.
Invalidate Patient Test Results*		P	Accrue workload when a completed crossmatch test is invalidated. This applies to the workload originally saved with the test, serological Coombs.
Enter Crossmatch Results	Crossmatch, Repeat Test	M	Accrue workload when an individual unit crossmatch is selected to include all phases or IS or only the AHG phase, is completed, and is saved. When multiple units are selected, each unit accrues workload.
Invalidate Patient Test Results*		M	Accrue workload when an individual unit crossmatch is invalidated.
Enter Daily QC Results	Daily Rack Quality Control (QC)	M	Accrue workload when Daily QC rack completed for one individual rack includes all rows in configured QC. When multiple racks are tested, each completed and saved tab accrues a workload event.
Record Patient Direct Antiglobulin Test	DAT (QC)	M	Accrue workload when Reagent QC completed in Patient DAT testing includes the testing of both the positive and negative control cells, per specificity per lot number, when only one phase of reactivity is chosen for the test grid (IS or AHG). One workload event is collected per completed tab for regular or repeat antiglobulin tests (PS, IgG, Comp).
Record a Transfusion Reaction Workup	Direct Antiglobulin Test (DAT)	P	A DAT test for “pre” or “post” is enabled and a valid interpretation other than Not Tested is selected. A workload event is accrued separately for “Pre” and “Post “entries.
Record Patient Direct Antiglobulin Test		P	Accrue workload when a DAT is completed and saved. This count is used for all antiglobulin tests (PS, IgG, Comp) when ordered from CPRS or Reflex testing.
Invalidate Patient Test Results*		P	Accrue workload when a completed DAT, PS, IgG, or Comp is invalidated.
Record Patient Direct Antiglobulin Test	Direct Antiglobulin Test (DAT) Repeat test	M	Accrue workload when a reflex or repeat DAT test is performed, completed, and saved. This applies to all repeat antiglobulin tests (PS, IgG, Comp).
Invalidate Patient Test Results*		M	Accrue workload when a completed Repeat DAT, PS, IgG, or Comp is invalidated.
Modify Units	Deglycerolize unit	U	Accrue workload when an individual blood unit is processed by the Deglycerolize modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	An individual blood unit’s status is invalidated when the original modification process was “Deglycerolize.”

Discard or Quarantine Unit	Discard unit	U	Accrue workload when an individual blood unit's status is invalidated. When a batch of units is selected, each unit accrues workload.
Remove Final Status*		U	Accrue workload when a unit is discarded for waste or credit. When a batch of units is selected, each unit accrues workload.
Modify Units	Freeze unit	U	Accrue workload when an individual blood unit is processed by the Freeze modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	An individual blood unit's status is invalidated when the original modification process was "Freeze."
Modify Units	Irradiate unit	U	Accrue workload when an individual blood unit is processed by the Irradiate modification type. When a batch of units is irradiated, each unit accrues workload. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	An individual blood unit's status is invalidated when the original modification process was "Irradiate."
Modify Units	Leukoreduce unit	U	Accrue workload when an individual blood unit is processed by the Leukoreduce modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	An individual blood unit's status is invalidated when the original modification process was "Leukoreduce."
Split a Unit	Split unit	U	Accrue workload when a unit modification of Split and a single workload event is recorded regardless of the number of units created by the modification. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	A Split Unit has its unit status invalidated. A single workload event is recorded regardless of the number of units originally created by the modification.
Modify Units	Rejuvenate unit	U	Accrue workload when an individual blood unit is processed by the Rejuvenate modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	An individual blood unit's status is invalidated when the original modification process was "Rejuvenate. "

Modify Units	Thaw	U	Accrue workload when an individual blood unit is processed by the Thaw modification type. When a batch of units is thawed, each unit accrues workload. This applies to Thaw FFP and Thaw Cryo. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	An individual blood unit's status is invalidated when the original modification process was "Thaw." This modification type is applicable to Thaw FFP and Thaw Cryo.
Modify Units	Wash unit	U	Accrue workload when an individual blood unit is processed by the Wash modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	An individual blood unit's status is invalidated when the original modification process was "Wash."
Modify Units	Volume Reduce	U	Accrue workload when an individual blood unit is processed by the Volume Reduce modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Remove Final Status*		U	An individual blood unit's status is invalidated when the original modification process was Volume Reduce.
Issue Blood Components	Issue unit	P	Accrue workload when a unit is issued to a patient. When a batch of units is processed, each unit invokes one workload process.
Justify Patient ABO/Rh Change	Justification	M	Workload is accrued when a patient's ABO or Rh typing is justified. One workload event is accrued per patient justification.
Login Equipment	Login Equipment	M	Accrue workload when a lot number of any type of equipment is logged into the system. When multiple lot numbers are processed in a batch, each lot number's workload is counted.
Login Reagent	Login Reagent	M	Accrue workload when a lot number of any type of reagent is logged into the system. When multiple lot numbers are processed in a batch, each lot number's workload is counted.
Login Supply	Login Supply	M	Accrue workload when a lot number of any type of supply is logged into the system. When multiple lot numbers are processed in a batch, each lot number's workload is counted.
Maintain Specimen	Maintain Specimen	M	Accrue workload when a specimen is maintained during order acceptance and is required for acceptance of the order. Note: This is collected in addition to the accept order workload accrued by accepting an order. Marking a specimen unacceptable does not create a negative workload event.

Patient antigen phenotype	Patient antigen phenotype (multiple phases)	P	Accrue workload when a patient antigen phenotype test with IS/RT or IS/37 phases is completed and saved. One workload event is collected per completed tab for repeat or regular antigen tests.
Invalidate Patient Test Results*		P	Accrue workload when a patient antigen phenotype test as defined by the antiserum specificity tested with any phases is invalidated.
Patient antigen phenotype	Patient antigen phenotype (single phase)	P	Accrue workload when a patient antigen phenotype test with AHG or IS phase is completed and saved. One workload event is collected per completed tab for repeat or regular antigen tests.
Invalidate Patient Test Results*		P	Accrue workload when a patient antigen phenotype test as defined by the antiserum specificity tested with a single phases is invalidated.
Pool Units	Pool unit	U	Accrue workload when a pooled unit is created and a single workload event is recorded regardless of the number of units included in the pooled unit. This applies to the Pool modification type. Add/Remove unit from a pool does not accrue any workload. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Edit Unit Information*		U	Accrue workload when a unit is inactivated if the pooled unit was created in VBECS.
Remove Final Status		N/A	No effect on workload accrual when a unit is removed from a modified status that was included in a pool.
Discard or Quarantine Unit	Quarantine unit	U	Accrue workload when a unit is marked for quarantine. When a batch of units is selected, each unit accrues workload.
Free Directed Unit For Crossover	Release directed unit	U	Accrue workload when an individual blood unit with the restriction type of “directed” is released for use as an allogeneic unit.
Release Unit from Patient Assignment	Release unit from patient back to inventory	U	Accrue workload when an individual unit is released from patient assignment. When multiple units are selected, each unit accrues workload.
Discard or Quarantine Unit	Release unit from Quarantine	U	Accrue workload when a unit is released from quarantine. When a batch of units is selected, each unit accrues workload.
Return Issued Unit	Return Issued unit	U	Accrue workload when a unit is returned from issue status.
Modify Units	Thaw/pool Cryo	U	Accrue workload when an individual unit has a modification of Thaw/Pool Cryo. A single workload event is recorded regardless of the number of units included in the pooled unit. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit.
Edit Unit Information*		U	Accrue workload when a unit is inactivated (unit record inactivated) when the pooled unit was created in VBECS.
Remove Final Status		N/A	There is no effect on workload accrual when a unit is removed from a modified status that was included in a Thaw/pool Cryo pool.

Enter Post-Transfusion Details	Transfuse Unit	U	Accrue workload when an individual blood unit's status is updated to "transfused."
Remove Final Status*		U	An individual blood unit's status is invalidated when the unit was in a status of "transfused."
Record a Transfusion Reaction Workup	Transfusion Reaction Investigation	P	Accrue workload when a transfusion reaction investigation is saved. This does not include workload accrued by the optional TRW serologic testing.
Invalidate Patient Test Results*		P	Accrue workload when a transfusion reaction investigation previously saved is invalidated.
Unit Antigen Typing	Unit Antigen phenotyping, Multiple Test phases	U	Accrue workload when a unit antigen phenotype test with IS/RT or IS/37 phases is selected and completed for an individual blood unit. There is no special handling for workload collection for additional repeat antigen typing tests on a unit.
Edit Unit Information*		U	Accrue workload when a unit antigen phenotype test with Multiple Test phases is invalidated for an individual blood unit.
Unit Antigen Typing	Unit Antigen phenotyping, Single Test phase	U	A unit antigen phenotype test with AHG or IS phase is selected and completed for an individual blood unit. There is no special handling for workload collection for additional repeat antigen typing tests on a unit.
Edit Unit Information*		U	Accrue workload when a unit antigen phenotype test with Single Test phase is invalidated for an individual blood unit.
Incoming Shipment	Unit login	U	An individual unit record is activated as "saved" to an incoming shipment invoice. When multiple units are entered, each unit added to the database accrues workload.
Edit Unit Information*		U	Accrue workload when a unit is inactivated and logged in through incoming shipment or is a pooled unit created in VBECS. When the unit was created by split modification, no workload is invalidated in this option.
Outgoing Shipment	Unit logout	U	An individual unit's status is updated to "transferred" on a confirmed outgoing shipment invoice. When multiple units are selected, each unit accrues workload. Accrue workload on confirmation of the invoice, not the addition of a unit to a temporary outgoing shipment invoice: an invoice may be confirmed only once.
Remove Final Status*		U	An individual unit status is invalidated when the unit had a previous unit status of "transferred."
Update Equipment Record	Update Equipment Record	M	Accrue workload when a lot number of any type of equipment is updated in the system.
Update Reagent Inventory	Update Reagent Inventory	M	Accrue workload when a lot number of any type of reagent is updated in the system. When multiple lot numbers are processed in a batch, each lot number's workload is counted.
Update Supply Inventory	Update Supply Inventory	M	Accrue workload when a lot number of any type of supply is updated in the system. When multiple lot numbers are processed in a batch, each lot number's workload is counted.

*Accumulates negative workload when it is associated with inactivation of a unit or removal of a final status.

Appendix C: Known Defects and Anomalies

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

This page intentionally left blank.

Appendix D: Active Directory Request Form

Fill out this form and email or fax it to your data center contact to have users added or deleted from the VBECS Active Directory groups. Email or fax it to your data center contact for action. Contact the Implementation Team to verify your data center contact, if necessary. The data center administrator facilitating this request will return this form to you when the changes are completed.

Blood bank information

Site Name:	
Site identifier:	VISN number:
Contact name:	Phone number:
Email:	Fax Number:

Data Center information

Technician name:	Phone number:
Email:	Fax number:

VBECS Users (users of normal VBECS): RnnxxxVbecsUsers group (nn is data center identifier and xxx is site identifier)

Specify the action, name and Windows ID of each technician requiring a change in access. The data center administrator will fill in his/her initials in the last column to confirm the change.

Row	Action	Last name, first name	Windows ID	Initials (for data center administrator only)
1	Add ☐ Delete ☐			
2	Add ☐ Delete ☐			
3	Add ☐ Delete ☐			
4	Add ☐ Delete ☐			
5	Add ☐ Delete ☐			
6	Add ☐ Delete ☐			
7	Add ☐ Delete ☐			
8	Add ☐ Delete ☐			
9	Add ☐ Delete ☐			
10	Add ☐ Delete ☐			
11	Add ☐ Delete ☐			
12	Add ☐ Delete ☐			
13	Add ☐ Delete ☐			
14	Add ☐ Delete ☐			
15	Add ☐ Delete ☐			
16	Add ☐ Delete ☐			
17	Add ☐ Delete ☐			
18	Add ☐ Delete ☐			
19	Add ☐ Delete ☐			
20	Add ☐ Delete ☐			

VBECS Administrators (users of administrative unit of VBECS): RnnxxxVbecsAdministrators group (nn is data center identifier and xxx is site identifier)

Specify the action, name and Windows ID of each technician requiring a change in access. The data center administrator will fill in his/her initials in the last column to confirm the change.

Row	Action	Last name, first name	Windows ID	Initials (for data center administrator only)
1	Add ☐ Delete ☐			
2	Add ☐ Delete ☐			
3	Add ☐ Delete ☐			
4	Add ☐ Delete ☐			
5	Add ☐ Delete ☐			
6	Add ☐ Delete ☐			
7	Add ☐ Delete ☐			
8	Add ☐ Delete ☐			
9	Add ☐ Delete ☐			
10	Add ☐ Delete ☐			

Appendix E: Data Center Instructions

Purpose

This appendix describes the tasks that must be completed by the data center for a successful VBECS installation, and is divided into 3 main sections depending on when the activities take place:

- Initial Setup Tasks: These tasks must be completed prior to installation of any VBECS systems.
- Ongoing Tasks: These are continual maintenance tasks.
- Installation Time Tasks: These tasks are to be completed at the time of a VBECS installation.

Initial Setup Tasks

Execute these tasks once, prior to setting up the VBECS systems in the data center.

Active Directory

VBECS User and Server Administrator Requirements

VBECS depends on Active Directory for remote server access for both VBECS and administration.

Set up two groups set up in Active Directory. The groups must have a "Universal" scope and a "Security" type.

- R*nnxxx*VbecsUsers (replace *nn* with your two-digit region number and *xxx* with the site location code): These are normal users of the VBECS system. Members of this group will have access to the server and are allowed to launch the VBECS application.
- R*nnxxx*VbecsAdministrators (replace *nn* with your two-digit region number and *xxx* with the site location code): These are users who must access the administrative component of VBECS. Members of this group will have access to the server and are allowed to launch the VBECS Administrator application.

Create a server administrator group to be shared across servers. This group must have a "Universal" scope and a "Security" type. This group will have administrative access to the VBECS servers at installation:

- R*xx*VbecsServerAdmins (replace *xx* with your two-digit region number): These are traditional server administrators who need full administrative privileges to the system. For SCOM support, add the VA IT Engineering CIS Monitoring Team group to this administrator group.

VBECS Server Requirements

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.

Group Policy

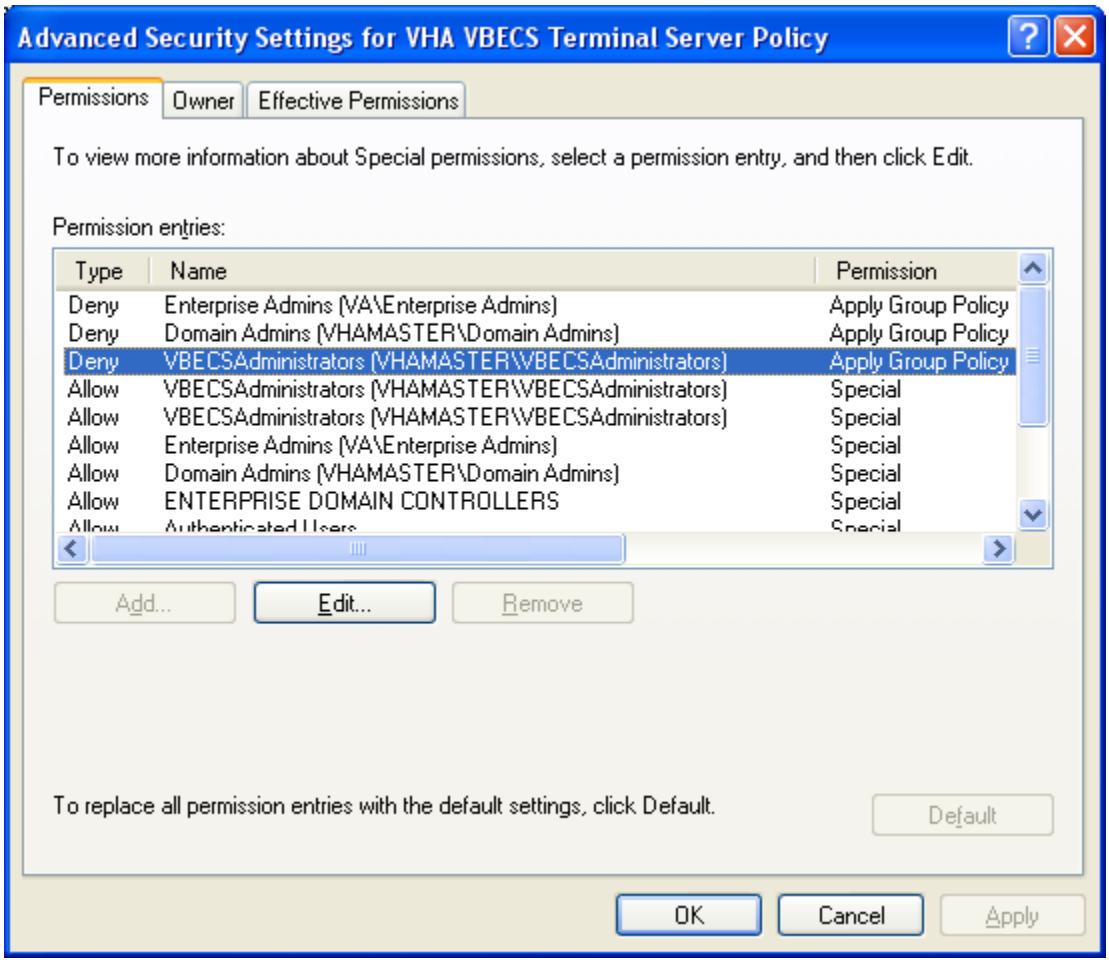
Import the VHA VBECS Terminal Server Policy from the VHAMASTER domain. If the VBECS development team changes the policy, import it again.

When importing the policy, clear the VBECS Windows Software Update Services settings (see Computer Configuration/Administrative Templates/Windows Components/Windows Update).

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 174.

Figure 174: Example of a Group Policy Not Applied to VBECSAdministrators Group



Service Accounts

VBECS requires dedicated service accounts for Microsoft Cluster and Microsoft SQL Server. Add these accounts to your R*xx*VbecsServerAdmins group. Define these service accounts once to be shared across VBECS servers (*xx* represents the two-digit region number):

- Microsoft Cluster: R*xx*VBESVCCLU01
- Microsoft SQL Server: R*xx*VBESVCSQL01

At installation, give the passwords for these accounts to the installer.

Terminal Server License Server

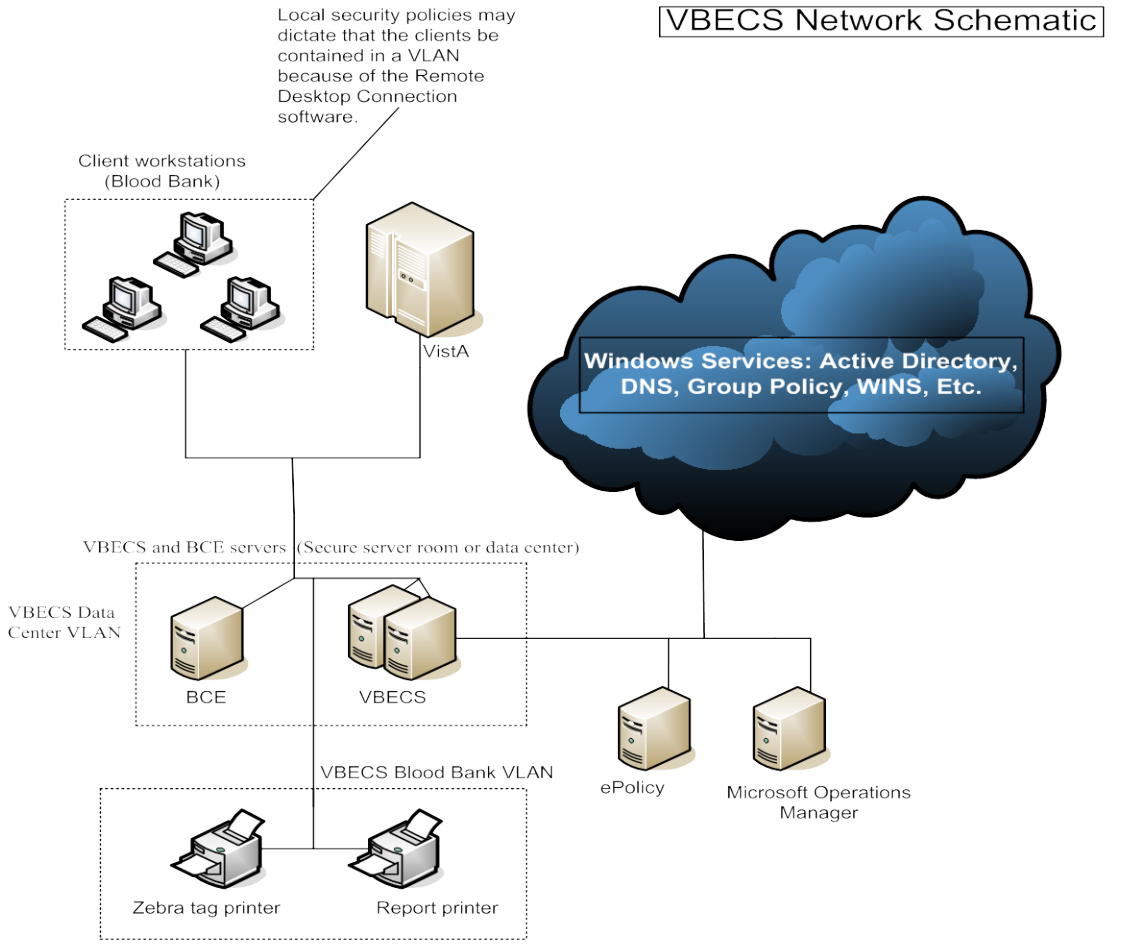
VBECS is a Terminal Server application and requires a license. Ensure that there is at least one Terminal Server License server set up for your domain.

VLAN

Since VBECS is a medical device, VBECS servers and printers must reside in a VLAN. Do not turn on the VLAN until installation is complete. Since this is a data center installation, the servers will reside on a VLAN separate from that of the printers, which reside at the blood bank.

Appendix H: Complete VLAN Requirements details the communication requirements for the VLAN. Figure 175 depicts how VBECS resides in the network.

Figure 175: VLAN Schematic



VBECS best fits into the domain limited model described in Medical Device Isolation Architecure Guide. The system will have to communicate with Microsoft resources as well as centralized resources such as ePolicy, Microsoft Operations Manager, VistA and Windows Software Update Services.

VBECS is written in C# .NET and uses an SQL Server database. Clients access VBECS through Remote Desktop Connections.

Ongoing Tasks

Execute the tasks in this section continually.

Back Up the VBECS Database

Back up the VBECS database nightly:

- Back up all folders and files in the \\<cluster name>\d$\Program Files\Microsoft SQL Server\MSSQL\BACKUP directory.
- Maintain backups for at least seven days.

VBECS Updates

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

Windows Updates

The VBECS development team must test every Microsoft Windows update. Once the development team is satisfied that the update causes no adverse effects, a VistA information patch in the VBEC (yes VBEC) namespace will be created. This patch will describe where to obtain the update and how to apply it. The patch will be released to customers by VA Product Support.

Installation of patches needs to be coordinated with the blood bank manager since most updates require a reboot.

Installation Time Tasks

Complete the Checklists and Password List

Complete these checklists and password list in the *VistA Blood Establishment Computer Software (VBECS) Installation Guide* prior to installation:

- Appendix B: Blood Bank Hardware Checklist: This checklist helps ensure that the correct server hardware is on-site.
- Appendix E: Server Configuration Checklist: This checklist contains server details such as names and IP addresses.
- Appendix H: Password List: This list includes passwords for the cluster and SQL server user IDs.

Update the VBECS Server Administrators Group

Refer to the appendices in the *VistA Blood Establishment Computer Software (VBECS) Installation Guide* to complete the installation of VBECS:

- Add the installers to the VBECS Server Administrators (R*xx*VbecsServerAdmins) group. See the Windows IDs of VBECS Installers cell in the Contact Information table of the Server Configuration Checklist (Appendix E). Upon successful completion, delete the installers from the group.
- Add the executor of the VBECS data conversion to the VBECS Server Administrators group. See the Data Conversion section of the Blood Bank Configuration Checklist (appendix).

Appendix F: Services Allowed to run on VBECS Servers

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

The following services are permitted to run on VBECS servers.

- Application Experience Lookup Service
- Automatic Updates
- Cluster Service
- COM+ Event System
- Computer Browser
- Cryptographic Services
- DCOM Server Process Launcher
- DHCP Client
- Distributed Link Tracking Client
- Distributed Transaction Coordinator
- DNS Client
- Error Reporting Service
- Event Log
- FTP Publishing Service
- HID Input Service
- HP Insight Notifier
- HP Insight Foundation Agents
- HP Insight NIC Agents
- HP Insight Server Agents
- HP Insight Storage Agents
- HP ProLiant Remote Monitor Service
- HP Smart Array SAS/SATA Event Notification Service
- HP System Management Homepage
- HP Version Control Agent
- HTTP SSL
- IIS Admin Service

- IPSEC Services
- Logical Disk Manager
- McAfee Framework Service
- McAfee McShield
- McAfee Task Manager
- MOM
- MSSQLSERVER
- Net Logon
- Network Connections
- Network Location Awareness (NLA)
- NT LM Security Support Provider
- Plug and Play
- Pml Driver HPZ12
- Print Spooler
- Protected Storage
- Remote Access Connection Manager
- Remote Procedure Call (RPC)
- Remote Registry
- SCOM
- Secondary Logon
- Security Accounts Manager
- Server
- Shell Hardware Detection
- Simple Mail Transfer Protocol (SMTP)
- SQLSERVERAGENT
- System Event Notification
- Task Scheduler
- TCP/IP NetBIOS Helper
- Terminal Services
- VBECS CPRS HL7 Client Monitor
- VBECS CPRS HL7 Listener

- VBECS HL7 Multi Listener
- VBECS Patient Merge HL7 Listener
- VBECS Patient Update HL7 Listener
- VBECS Scheduled Report Runner
- VBECS Service Monitor
- VBECS VistALink RPC XML Listener
- VBECS Test CPRS HL7 Client Monitor
- VBECS Test CPRS HL7 Listener
- VBECS Test HL7 Multi Listener
- VBECS Test Patient Merge HL7 Listener
- VBECS Test Patient Update HL7 Listener
- VBECS Test Scheduled Report Runner
- VBECS VistALink RPC XML Listener
- Windows Management Instrumentation
- Windows Time
- Workstation
- World Wide Web Publishing Service

This page intentionally left blank.

Appendix G: Auditing on VBECS Servers

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

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

This page intentionally left blank.

Appendix H: Complete VLAN Requirements

Please note the following:

- All requirements are TCP and UDP unless specified otherwise.
- **Inbound** is traffic from the server back to the LAN.
- **Outbound** is traffic from the LAN to the server.
- The ACL needs to be open to all servers in the system (2 nodes, cluster and SQL Server).
- Data centers: Please see Table 12 for additional guidance if your servers do not reside in the VHAMASTER (vha.med.va.gov) domain.

These settings are meant to serve as a starting point for your ACL. To ensure all resources are accounted for, please review firewall logs.

Table 12: VBECS Communication Requirements

Servers, Workstations, Printers	IP Address	Notes
Data center domain controllers (all), WINS, DNS	See data center network administrator	
Data center WSUS	See data center network administrator	

Table 13: VLAN Requirements

Servers	IP Address	Port(s)	Direction	Notes
vha.med.va.gov WINS servers	10.3.29.33 10.3.29.34 10.39.129.200 10.142.16.150	42 135-139 1512	inbound/ outbound	Check the network settings on your VBECS servers to confirm which ones you are using.
Local WINS servers	Consult network personnel.	42 135-139 1512	inbound/ outbound	
va.gov domain controllers	10.3.21.193 10.3.21.197 10.3.21.199 10.3.30.1 10.204.1.10 10.222.161.29	53 88 123 (UDP) 135 through 139 389 445 (TCP) 636 1512 3268 3269 3289 Echo, Echo-reply, Traceroute, (ICMP)	inbound/ outbound	Due to round robin DNS, all va.gov domain controllers must be accessible.
med.va.gov domain controllers	10.3.21.194 10.3.21.216 10.3.30.2 10.4.229.41 10.186.130.147	53 88 123 (UDP) 135 through 139	inbound/ outbound	Due to round robin DNS, all med.va.gov domain controllers must be accessible.

Servers	IP Address	Port(s)	Direction	Notes
	10.222.161.25	389		
		445 (TCP)		
		636		
		1512		
		3268		
		3269		
		3289		
		Echo, Echo-reply, Traceroute, (ICMP)		
vha.med.va.gov domain controllers	10.1.21.192 10.2.21.192 10.3.21.192 10.3.21.215 10.3.27.14 10.3.27.33 10.3.30.25 10.4.21.192 10.4.229.2 10.5.21.192 10.6.21.192 10.6.197.13 10.15.32.250 10.52.65.100 10.61.192.139 10.63.196.55 10.124.115.50 10.189.1.1 10.189.37.217 10.189.46.203 10.189.61.5 10.189.77.230 10.189.110.3 10.190.40.20 10.191.10.7 10.191.23.85 10.208.13.14 10.222.186.10 10.222.228.3 10.252.92.7 10.252.93.7 10.252.94.7 10.252.95.7	53	inbound/ outbound	Due to round robin DNS, all vha.med.va.gov domain controllers must be accessible.
		88		
		123 (UDP)		
		135 through 139		
		389		
		445 (TCP)		
		636		
		1512		
		3268		
		3269		
		3289		
		Echo, Echo-reply, Traceroute, (ICMP)		
Local VISN domain controllers	Consult network personnel.	53	inbound/ outbound	Due to round robin DNS, all va.gov domain controllers must be accessible.
		88		
		123 (UDP)		
		135		
		137		
		139		
		389		
		445 (TCP)		
		636		
		1512		
		3268		
		3269		

Servers	IP Address	Port(s)	Direction	Notes
		3289		
SMTP Support	10.236.10.254 10.237.10.254 10.238.10.254 10.239.10.254	25	inbound	VBECS email alerts
Terminal Services license servers	10.184.161.48 10.186.130.34	135 137 139 445 1024 through 65535	inbound/ outbound	These servers make up tslicense.va.gov
System Center Operations Manager	10.3.36.20 10.3.36.22 10.3.36.24 10.3.36.26	135 137 139 445 1024 through 5000 5723 49152 through 65535	inbound/ outbound	All of these ports must be open to allow SCOM agent installation. After SCOM implementation is complete, a VBECS technical bulletin will be issued to close the majority of SCOM ports and leave port 5723 open.
Microsoft Operations Manager	10.3.31.51 10.3.31.52	1270	inbound/ outbound	Note that this entry will be deleted after SCOM agent is installed. Another technical bulletin will be released after the implementation is complete that will reflect this.
VBECS workstations that require an RDP connection	Consult network personnel	3389	inbound/ outbound	Assign static IPs if necessary.
VBECS printers (label and report)	Consult network personnel	9100	inbound/ outbound	
VBECS VistALink Production Listener	Consult network personnel	21992	inbound/ outbound	Verify IPs with network personnel.
VBECS VistALink Test Listener	Consult network personnel	21991	inbound/ outbound	Verify IPs with network personnel.
HL7 Production Listener	Consult network personnel	21994	inbound/ outbound	Verify IPs with network personnel.
HL7 Test Listener	Consult network personnel	21993	inbound/ outbound	Verify IPs with network personnel.
VBECS-OERR HL7 Listener	Consult network personnel	Consult network personnel	inbound/ outbound	Applicable for data center sites.
VistA VistALink Production Listener	Consult network personnel	Consult network personnel	inbound/ outbound	Verify IPs and ports with network personnel.
VistA VistALink Test Listener	Consult network personnel	Consult network personnel	inbound/ outbound	Verify IPs and ports with network personnel.
ePolicy	10.254.36.41 10.254.36.42 10.254.36.43	8079 8080 8082	inbound/ outbound	This is a central resource used to update virus definition files and configure virus scans.

Servers	IP Address	Port(s)	Direction	Notes
	10.254.36.44 10.254.36.45	8180 8181 8443 8444		
VBECS Development Support and Windows Server Update Services	10.3.9.181 10.3.21.77	20 21 135 through 139 445 1024 through 65535	inbound/ outbound	Tier 3 support.
Backups	Consult network personnel	Consult network personnel	inbound/ outbound	If your site uses a centralized backup solution, you will need to add entries for this.
PIV/eToken authentication	64.18.29.194 64.18.30.12 64.18.20.12 64.18.17.35 64.18.29.195 10.208.14.107 10.235.122.196 10.235.122.195 10.234.122.196 10.3.30.47 10.234.122.195 10.3.30.39 10.105.10.18 10.105.10.19 10.208.14.108 10.184.161.48 10.186.130.34 10.105.8.101 10.184.161.48 10.186.130.34 10.105.8.101	80	inbound/ outbound	
PIV/eToken authentication	64.18.17.34 64.18.29.210 10.184.161.48 10.105.8.101 10.186.130.34	389	inbound/ outbound	

Index

A

B

C

D

E

F

G

H

I

K

L

M

O

P

R

S

T

U

V

W

This is the last page of the *VistA Blood Establishment Computer Software (VBECS) 1.6.0 Technical Manual-Security Guide*.