Voluntary Service System (VSS)

Site Installation Guide

March 2003

Revised August 2006

Department of Veterans Affairs
Health Systems Design & Development (HSD&D)

Revision History

DATE	REVISION	DESCRIPTION	AUTHOR
3/18/03	1.0	Document issued as Part 2 of the VSS Installation Guide, under the title *Site Implementation Guide*. Contained information for local IRMs and Voluntary Services to: • Set up and configure equipment and software required to run the VSS application • Migrate local Voluntary data to the national database at the EMC.	Mike Garvey, Ron DiMiceli, Cathi Graves, Lloyd Hurt, Jim Alexander.
5/2/03	2.0	Material issued as standalone document under the title, *Site Installation Guide*. Incorporated minor changes, especially in the section "Setting Up the Auto-login kiosk"	Jim Alexander, Mike Garvey
5/8/03	2.1	Minor changes to Revision and TOC sections.	Jim Alexander
5/16/03	2.2	Addition to the "IRM Data Transmission Instructions" in the "Data Migration Instructions" section.	Jim Alexander, Ron DiMicelli
5/21/03	2.3	Minor change to "Auto-Login Kiosk Setup Instructions" section.	Jim Alexander, Mike Garvey
8/22/03	2.4	Additional instructions to "Auto-Login Kiosk Setup Instructions" for MS Service Pack 4 installation.	Jim Alexander, Mike Garvey
11/10/04	2.5	Additional instructions to "Auto-Login Kiosk Setup Instructions" for Windows XP.	Mike Garvey
11/15/04	2.6	Manual updated to comply with SOP 192-352 Displaying Sensitive Data.	Corinne Bailey
4/18/06	2.7	Game instructions to Overview portion of "Auto-Login Kiosk Setup Instructions".	Mike Gabriel, Corinne Bailey
8/23/06	2.8	Revised manual to remove references to data migration, update kiosk setup steps, and add instructions for ActiveX Control	Mike Gabriel, John Sistrunk, Corinne Bailey
10/11/06	2.9	Updated url for VistA Documentation Library	Corinne Bailey

Table of Contents

Introduction

AUDIENCE AND SCOPE

This document is for use by IRM and Voluntary Service groups at VHA sites during the implementation of the VSS application. It contains information for setting up equipment required by the VSS application.

CONTENTS

This guide includes the following material.

- Checklists of IRM and Voluntary implementation tasks
- System requirements for Voluntary PCs, auto-login kiosks, meal-ticket printers
- Browser setup instructions
- Kiosk setup instructions

Implementation Steps for IRM and Voluntary

This section lists the steps that the IRM and Voluntary Services need to take to implement the VSS system at a VHA facility. This section should serve as an overview and checklist. Some of the steps listed here refer to other parts of this document where the information is described in much greater detail.

The implementation steps summarized in the text are divided into two sections; one for the IRM, and one for Voluntary. Although IRM and Voluntary Services have different responsibilities during the implementation process, they must coordinate and communicate carefully for the equipment upgrade and kiosk installation to be successful.

It should be stressed that during the Alpha and Beta implementations, the most problematic step was the installation of the auto-login kiosks. It is crucial to the success of site implementation, therefore, to set up, test, troubleshoot, and instruct staff on the use of auto-login kiosks. It is highly recommended that an IRM resource be reserved for two full days to troubleshoot the auto-login/meal-ticket printer.

IRM

Coordinate with Voluntary - Contact Voluntary Services Chief to discuss tasks, schedules, and the Voluntary staff who will support the IRM during implementation.

Equipment List - Examine Voluntary equipment list and determine the following:

- Which currently used equipment does not meet VSS system requirements. (See *System Requirements* section.)
- Which login locations have dumb terminals. You will need to replace these with PCs.
- Remote login locations that will have to be locked down in kiosk mode.

Equipment Upgrade - Replace and upgrade equipment and software as required for staff computers and volunteer auto-login stations.

Internet Access - Ensure that the VSS staff that will be doing administrative work have internet access. They will need:

- Microsoft Internet Explorer 5.5 or higher, with latest service packs (IE 6.0 is highly recommended)
- Internet access
- NT domain and username.

Browser LAN Settings - Assist VSS administrator to change browser LAN settings on computers with Internet access. Ensure that the site has a trust relationship with VHAMASTER. (See *Browser Setup Instructions* section.)

Test Connectivity - Test Internet connectivity for each machine.

Set Up and Test Kiosks - Set up, test, and instruct staff on the use of auto-login kiosks. Reserve two full days of an IRM resource to troubleshoot and practice the auto-login/meal-ticket printer installation. **This step is the most crucial to the success of the VSS implementation.**

Verify the connection types needed for both the PC and the printer. Make sure you have the correct setup for your particular situation.

The IRM is required to test the kiosk prior to going live with VSS. If they encounter any problems, they will log a Remedy Ticket, and if the Help Desk cannot resolve the issue, then the Remedy ticket will have to be referred to a technical resource in HSD&D. (See *Auto-Login Kiosk Setup Instructions* section.)

Message from EMC - Receive message from EMC whether or not data has been received and entered into database. If there is a problem, the EMC will give instructions.

VOLUNTARY

Coordinate with IRM - Contact IRM to discuss tasks, schedules, and the Voluntary staff who will support the IRM during implementation.

Equipment List - A Voluntary service representative should make a list of the equipment and software used by VSS staff and by volunteers at login locations. Make special note of the following:

- Locations where dumb terminals are used (the IRM will need to replace these)
- Remote locations, away from office staff (the IRM will need to lock these down in "Kiosk mode")
- Deliver and discuss the list with an IRM representative.

Security Agreements - Each staff person who will be using the VSS system should sign a security agreement in coordination with both the facility ISO and the designated Voluntary Services VSS Site User Administrator. A typical site will have no more than five or six users needing access.

Browser LAN Settings - Change LAN settings on browsers. (See *Browser Setup Instructions* section.) If the Voluntary administrator does not have administrator access to do this, request it be done by the IRM.

New Volunteer Kiosk Test - Enter a small number of new volunteers into the VTK system prior to implementation, enter hours for them, and print meal tickets using the new auto-login kiosks. These volunteers should be held back after orientation in order to participate in the test. The kiosks will be pointed to the EMC's production database.

System Requirements

WORKSTATION HARDWARE

- Standard PC architecture, with Pentium 150MHz processor or greater
- 64 MB of RAM or greater
- 2 GB hard disk or greater, with a minimum of 60 MB of free space
- VGA or greater display adapter with color monitor
- Microsoft mouse or compatible pointing device
- A network interface card (NIC) with appropriate network transport software. Supported connection method and transport are TCP/IP and HTTP.

WORKSTATION SOFTWARE

- MS Windows XP operating system with latest service packs
- Microsoft Internet Explorer 5.5 with latest service packs (Internet Explorer 6.0 is highly recommended)
- Adobe Acrobat Reader Version 5.0 or higher
- Microsoft Office with all service packs installed (necessary to run reports)
- Network transport software appropriate for the network interface card being used. The supported connection method and transport are TCP/IP and HTTP.

MEAL TICKET PRINTER

- Star Micronics SP200 Dot Matrix Printer
- Serial cable using a D-sub9/MaleD-sub 25 connection

THIN CLIENT

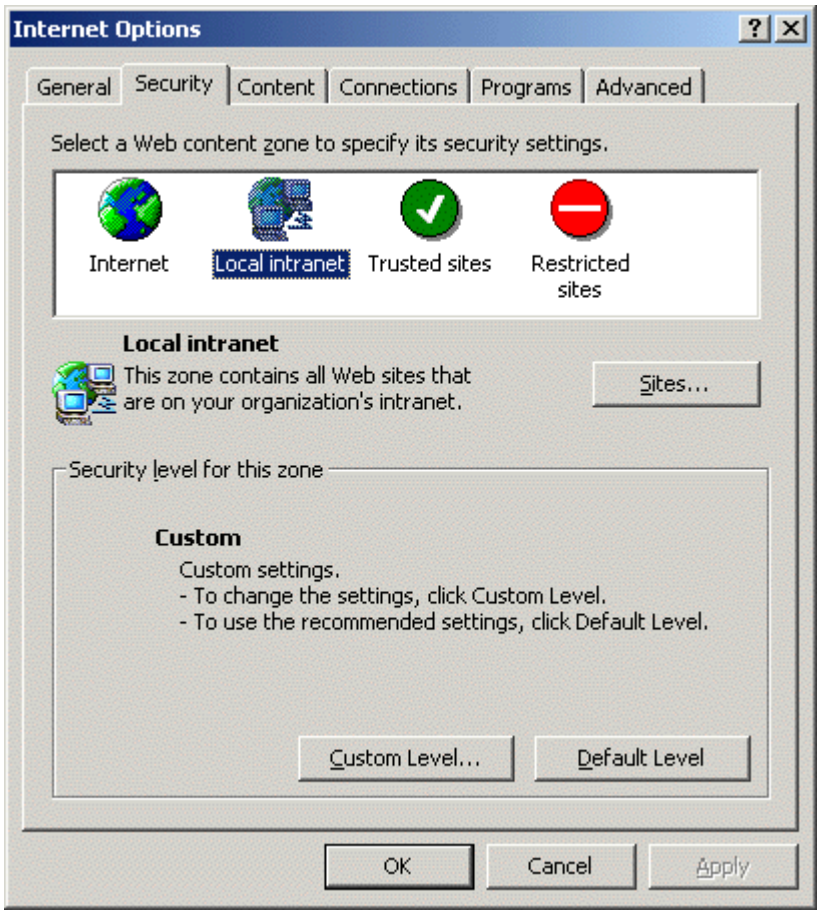
If you want to set VSS up to run with Thin Client, please refer to the VSS web page at http://www.va.gov/vdl/application.asp?appID=135 for instructions.

Browser Setup Instructions

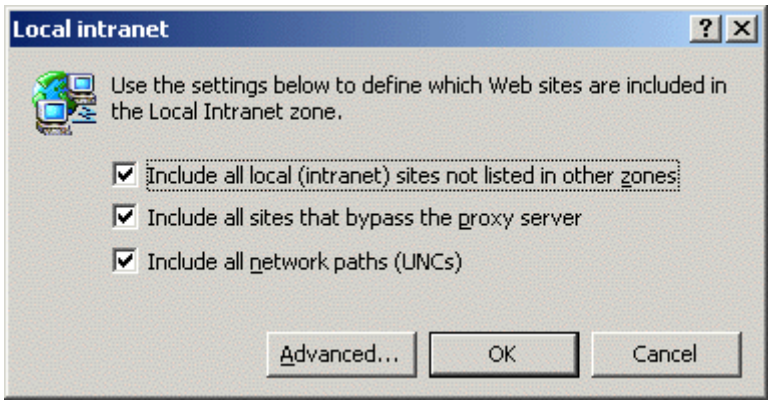
To enable your copy of Internet Explorer (5.5. or 6.0) to identify "Local intranet" sites on the VA network, follow the steps below.

1. In IE, go to the Tools | Internet Options menu.

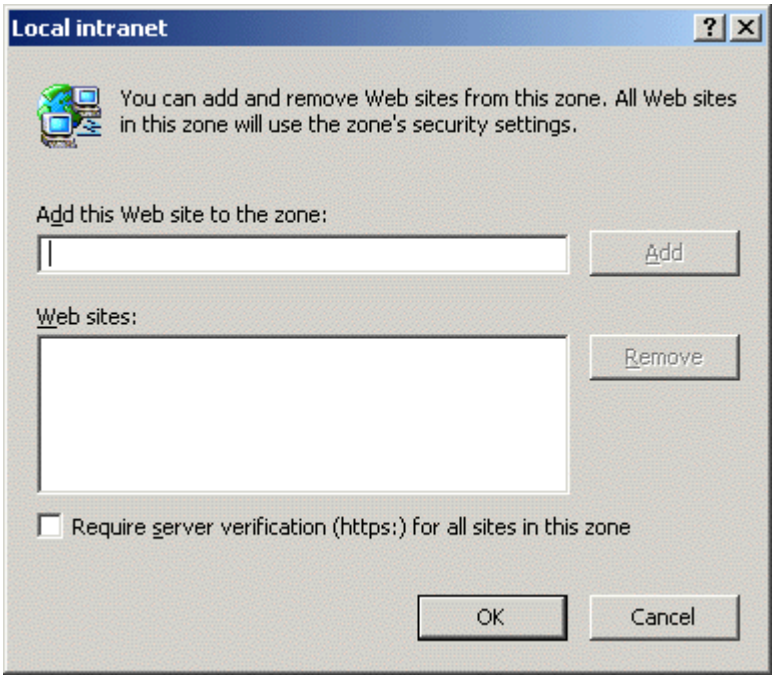
2. Choose the Security Tab.



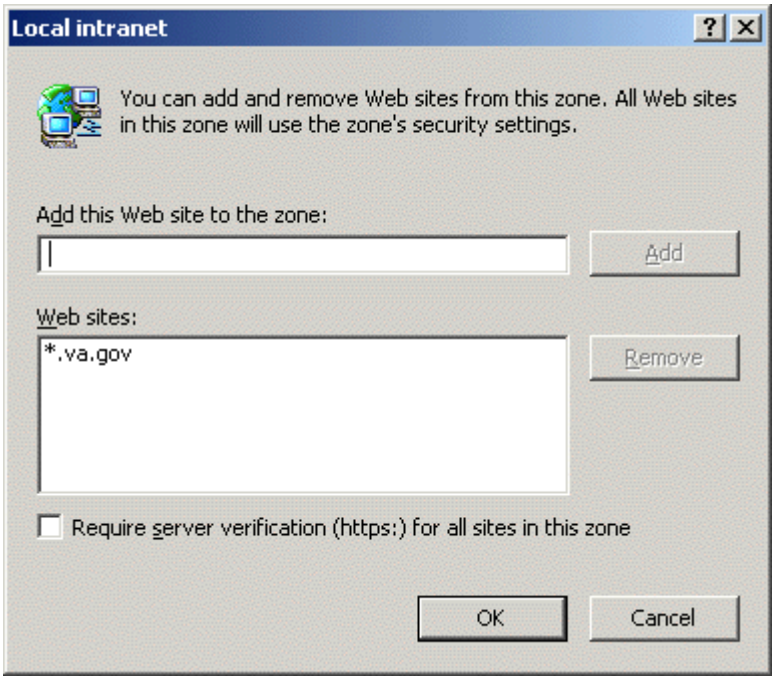
3. In the Security tab, highlight "Local intranet" and click the Sites button. This brings up the “Local intranet” window.



4. Click the Advanced button. (The settings for the three checkboxes in the "Local intranet" window are not important for this test.) This brings up another "Local intranet" window. In this window, you can add web sites to the "Local intranet" zone.

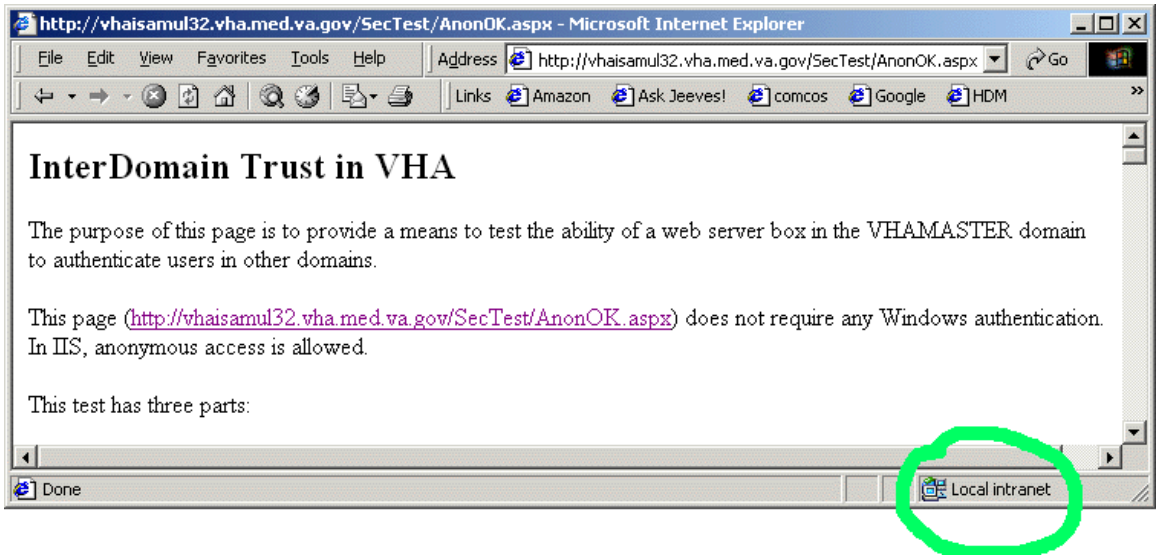


5. In the "Add this Web Site to the Zone" box, enter “*.va.gov” and press the Add button. The dialog box will look like this:



6. Keep clicking OK to save these changes and exit out to your browser window.

7. Check that the Security Zone, located in the lower right-hand portion of Internet Explorer's status bar, now shows "Local intranet" when you access any site ending in "…med.va.gov".



8. If your browser shows "…med.va.gov" pages as "Local intranet" zone, your browser is ready.

Auto-Login Kiosk Setup Instructions

OVERVIEW

The auto-login kiosk allows volunteers to log into the Voluntary Services System, post their time for the day, and print a meal ticket. This section is a detailed instructional guide for the IRM staff to use to properly install an auto-login kiosk station.

For the auto-login system to work properly, Windows XP operating system with latest service packs is required. The NT 4.0 operating system will not allow the left margins to view the first character on the meal ticket.

It is strongly advised that the IRM allocate a resource for a total of two full days to troubleshoot the auto-login/meal-ticket printer. It is crucial to the success of site implementation to set up, test, troubleshoot, and instruct staff on the use of the auto-login kiosks.

Before setting up the kiosk, you will need to obtain the following:

- To install the Star SP200 printer and configure the workstation's local policies.
  - WinZip
  - VSS_Kiosk_20030422.zip. This file is available for download at the VistA Documentation Library (http://www.va.gov/vdl/application.asp?appID=135). Use the link in the "HTML/Zip" column for "System Policy Editor for Windows Clients." **NOTE**: This download contains the files for setting local policies AND the drivers required for installing the Star printer.
  - A DB9F to DB25M serial printer (Null Modem) cable
- Station Number that corresponds to your site.

If a site wants to use a kiosk for Games, a dedicated workstation for the Games kiosk is required and should point to the Station Number for the Games rather than the Timekeeping Station Number. The Timekeeping kiosk cannot be used for Games.

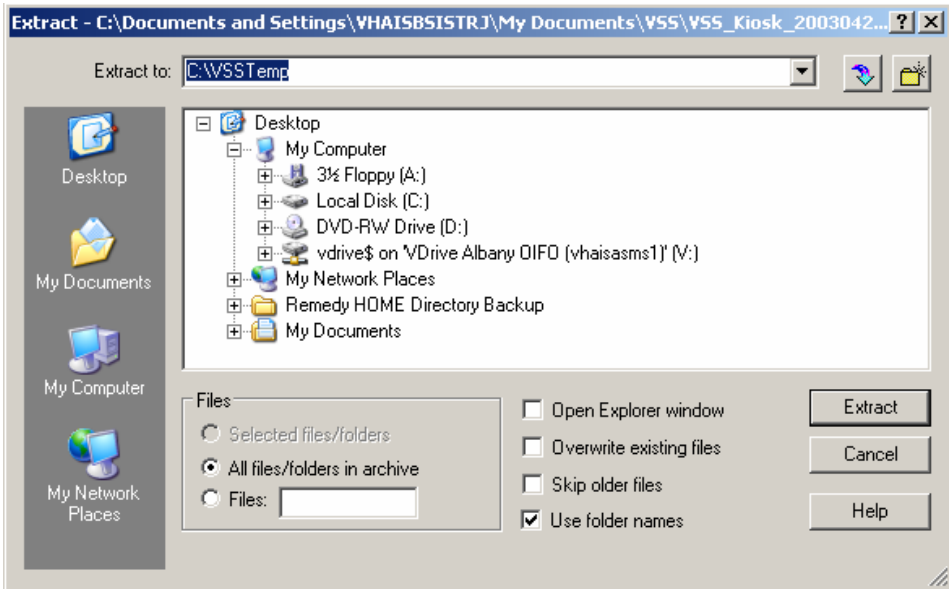
For the auto-login policy definitions, see *Appendix A* of this document.

KIOSK SETUP STEPS

This section is a detailed instructional guide for showing how to properly configure a Voluntary Services System (VSS) kiosk station. The kiosk station allows volunteers to login to the Voluntary Services System, post their time for the day, and print a meal ticket if earned. If you have any problems, contact your local IRM.

Setup for Windows XP Operating System

1. ***Logon as a local machine administrator.***
    a. Install WinZip.
    b. Download **VSS_Kiosk_20030422.zip**. This file is available at the VistA Documentation Library at http://www.va.gov/vdl/application.asp?appID=135. Use the link in the **HTML/Zip** column for **System Policy Editor for Windows Clients**.
    NOTE: This download contains the files for setting local policies AND the drivers required for installing the Star printer.
        i. Double click on **VSS_Kiosk_20030422.zip.** When the file list window appears, click **Extract**.
        ii. When prompted by WinZip, enter **C:\VSSTemp** as the file destination.



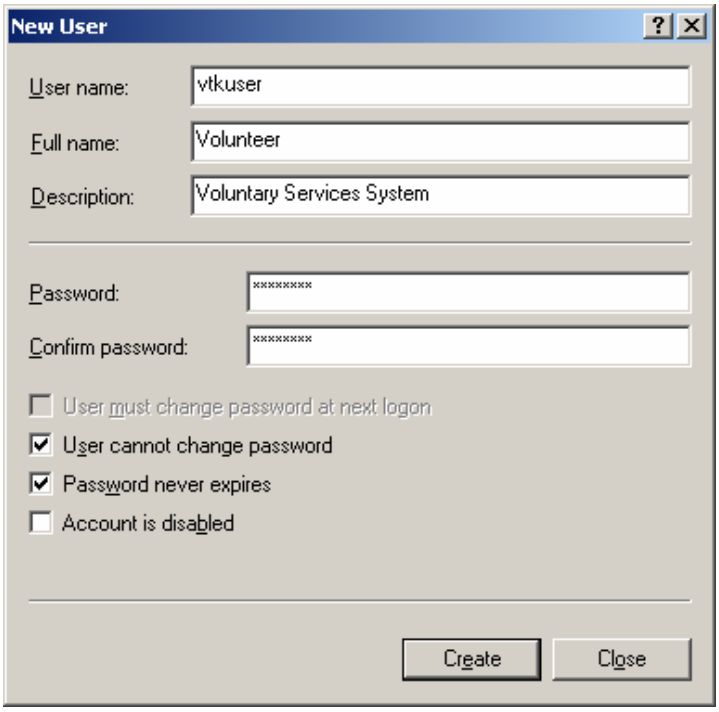
        iii. Click **Extract**.
        iv. Close the WinZip window.
        v. This will create the following two folders in the VSSTemp directory:
            1. Policy: Contains files required for configuring local policies.
            2. Printer: Contains the executable for installing the printer drivers.

c. Create a new local user account: ***vtkuser***.

i. Open **Start | Control Panel,** followed by **Administrative Tools | Computer Management.**

ii. In the console tree, open **Local Users and Groups | Users.**

iii. Select **Action | New User…** and complete the **New User** dialog. **NOTE**: Choose a password for this account that complies with the organization's guidelines for secure passwords.



iv. Clear the **User must change password at next logon** check box and select the **User cannot change password** and **Password never expires** check boxes.

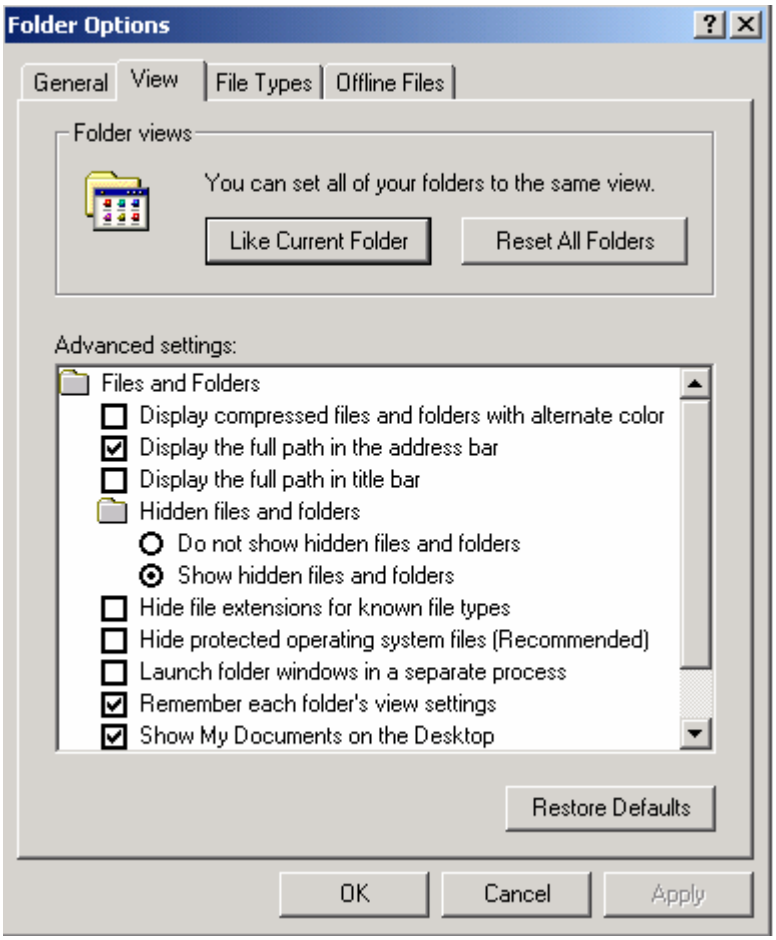
v. Click **Create** and then **Close**.

vi. Close the Computer Management Window.

d. Open Windows Explorer and configure it to see hidden files and folders and file extensions.

i. Open **Start| All Programs | Accessories| Windows Explorer,** followed by **Tools | Folder Options.**

ii. On the **View** tab of the **Folder Options** dialog box, make the following changes in the **Advanced Settings** window.



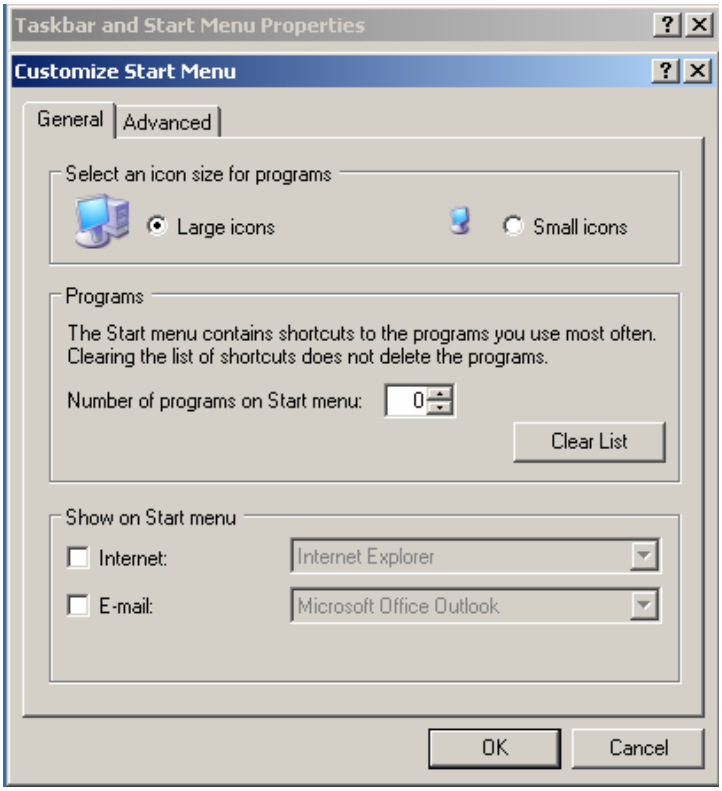
iii. Select **Show hidden files and folders.**

iv. Clear the checkbox for **Hide file extensions for known file types**.

v. Clear the checkbox for **Simple file sharing.**

vi. Click **OK**.

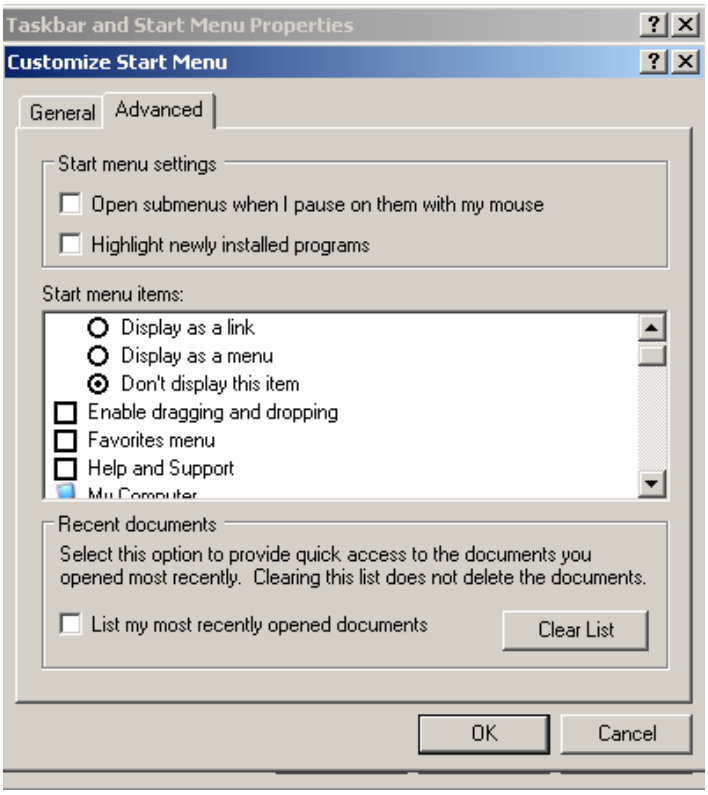
2. ***Logon as vtkuser***. Make sure you log on to the local machine and not the domain. The correct account is **<XXX (this computer)\vtkuser>.**
    a. Disable the Quick Launch bar.
        i. Right-click on an empty area on the Taskbar and select **Properties**.
        ii. Select **Taskbar** Tab and uncheck the following:
            - Lock the taskbar
            - Keep taskbar on top of other windows
            - Group similar taskbar buttons
            - Show Quick Launch
            - Show the clock.
    b. Modify the Start Menu.
        i. Select **Start Menu** Tab and click **Customize**.
        ii. Click the **General** tab.
        iii. Set **Number of programs on Start menu** to 0.
        iv. Clear the **Internet** and **E-mail** check boxes.



v. Click the **Advanced** Tab.

vi. Clear all check boxes.

vii. In the **Start Menu Items** area, choose **Don't display this item** for all radio buttons and clear all the check boxes **EXCEPT** "**Run**" and "**Printers and Faxes**."



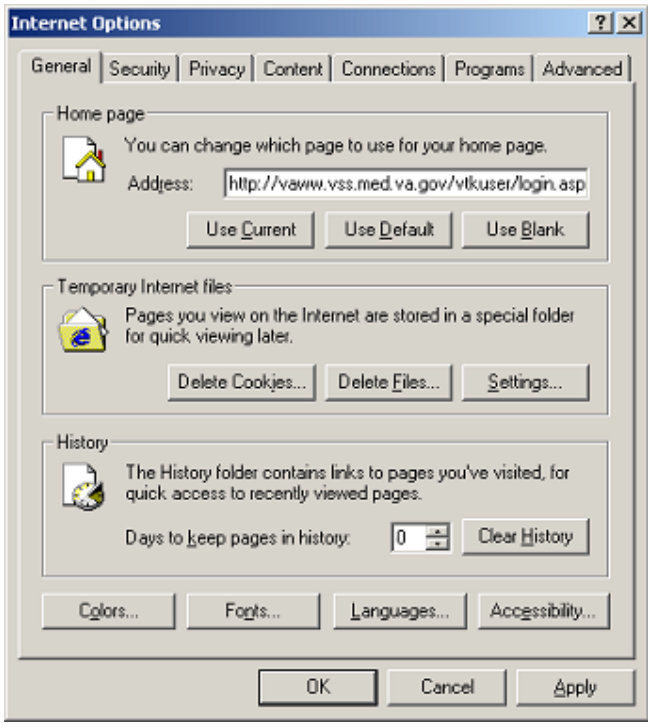
viii. Click **OK** to close the Customize window.

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

c. Launch Internet Explorer (**Start | Run | iexplore.exe**) and configure the browser.

i. Open **Tools | Internet Options** and complete the **General** tab of the **Internet Options** dialog box using the screen shot below as a guide.

1. **Home Page**. Enter the URL/Station Number in the Address box. **NOTE**: Each site has a corresponding station number assigned to it and this value should be appended to the default URL (as an argument to the site's default page; login.aspx). If you do not know your station number, contact VSS Support to obtain it. **EXAMPLE**: Palo Alto (Station 640) uses the following URL: ***http://vaww.vss.med.va.gov/vtkuser/login.aspx?StationNumber=640***



2. **History**: Set to **0.**
3. Click **OK**.

d. Close the Internet Explorer window and open a new one. Verify browser operation and access to the VSS application with the new settings.

e. Log off of the computer, then log on again (as ***vtkuser***). Open Internet Explorer and confirm that the settings remain in effect.

3. ***Logon as a local machine administrator***.

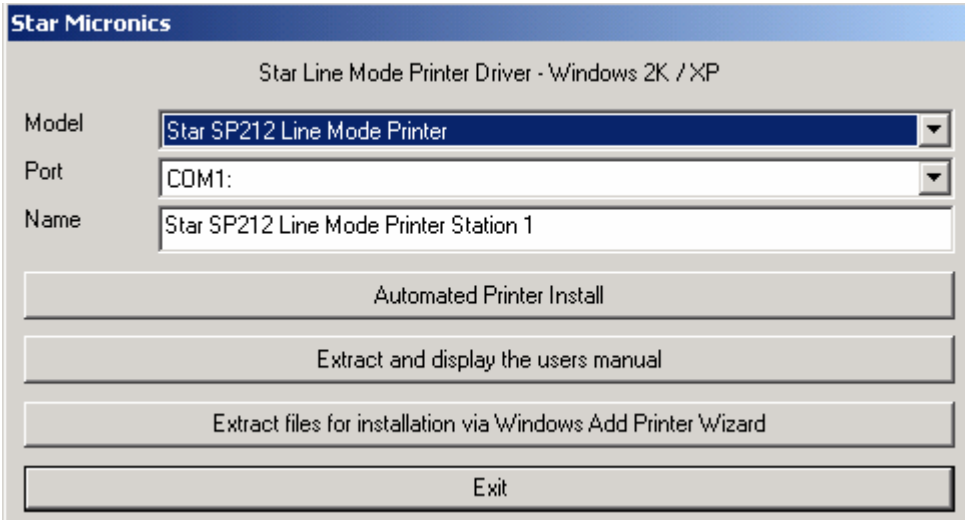
   a. Delete all items except the Startup folder from *vtkuser's* Start Menu (i.e., all items in **C:\Documents and Settings\vtkuser\Start Menu\Programs).**
   NOTE: Do not delete the Startup folder but delete any items in it.

   b. Setup the default printer. These instructions will use a local Star Micronics SP200/SP212 line-mode printer as an example.

      i. Attach the printer to the auto-login workstation using the correct cable. This cable is a DB9F to DB25M custom serial printer cable and can be connected to the computer in only one way. COM1 is the preferred serial port.

      ii. The driver for the Star Micronics SP200/SP212 printer is a self-installing driver. To start the printer installation process, double click **linemode_2k-xp_20020723.exe**, located in the **C:\VSSTemp\Printer** folder.

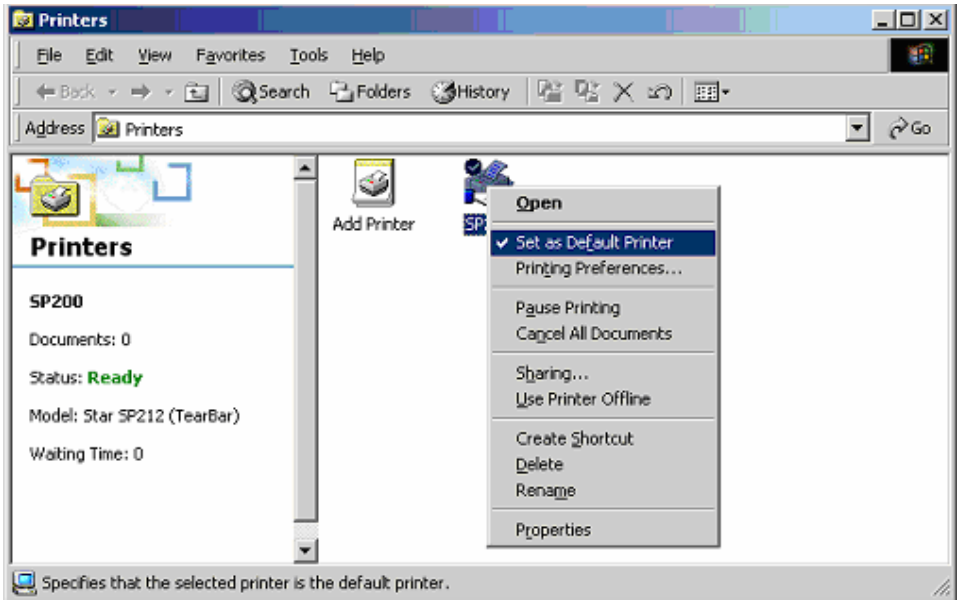
         1. At the Welcome screen, click **OK**.
         2. Configure the **Model**, **Port**, and **Name** fields as shown below.



         3. Click **Automated Printer Install.**
         4. Click **No** on Language Monitor screen.
         5. Click **Yes** on default printer screen.
         6. Click **Yes** to print a test page.
         7. Click **Exit**.

4. ***Logon as vtkuser.***

   a. Set the SP200 printer as the default (**Start | Settings | Printers).**

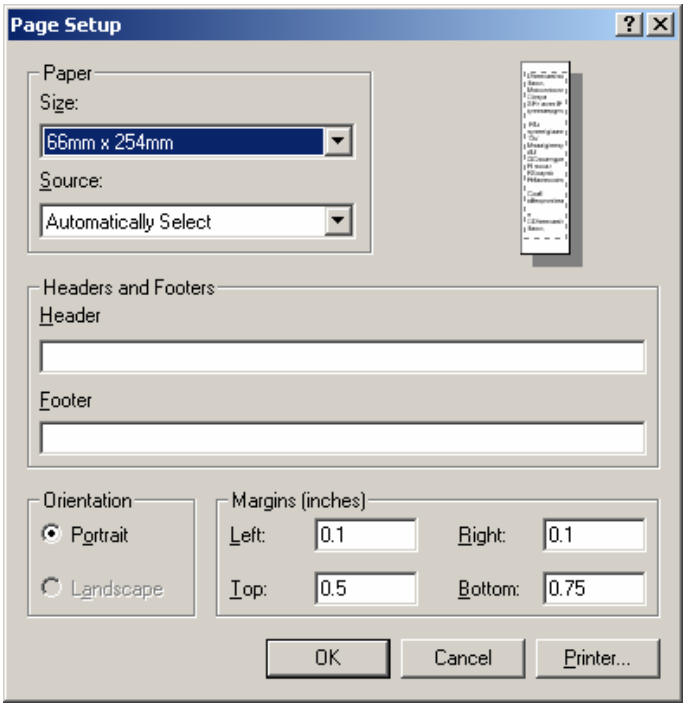


   b. Launch Internet Explorer (**Start | Run | iexplore.exe**). Set up the printer (**File | Page Setup).** Configure the printer as shown below**.**

      i. **Size –** 66 x 254 mm

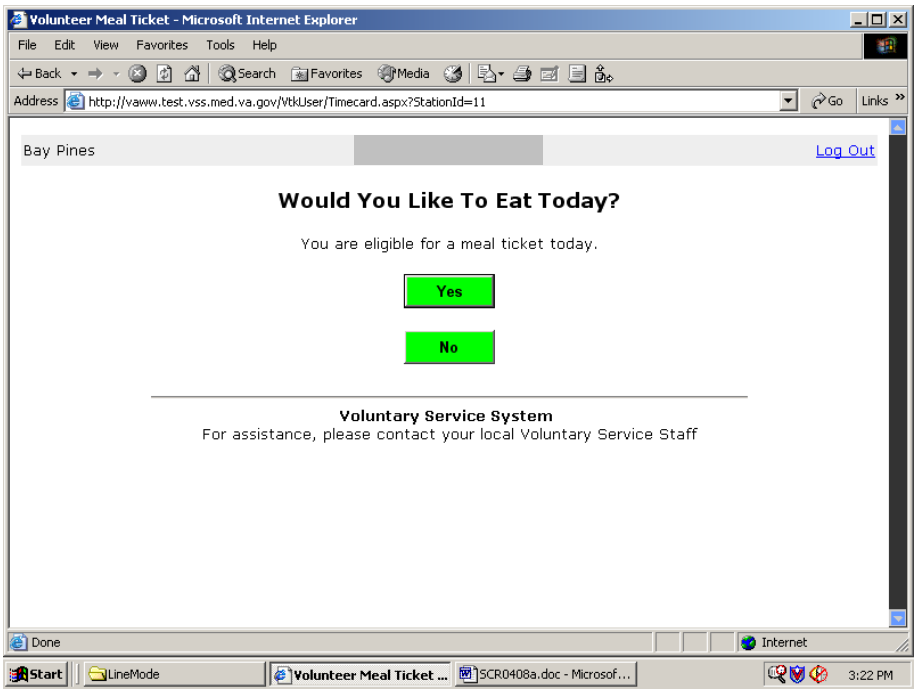
      ii. **Margins:** Left – 0.1, Right 0.1, Top – 0.5, Bottom – 0.75

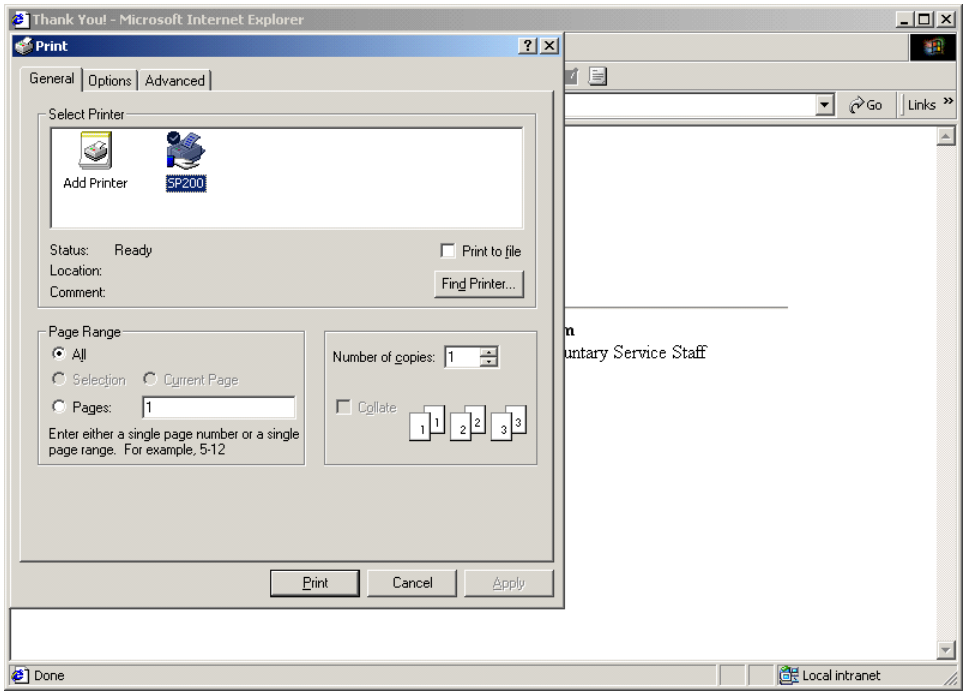
      iii. **Headers and Footers:** None



      iv. Click **OK**.

c. Generate a meal ticket using a valid volunteer ID and verify printing. To obtain volunteer IDs, run the **Sign-In Code List** report for your station from within the main Voluntary Services System application (not the Auto-Login application).





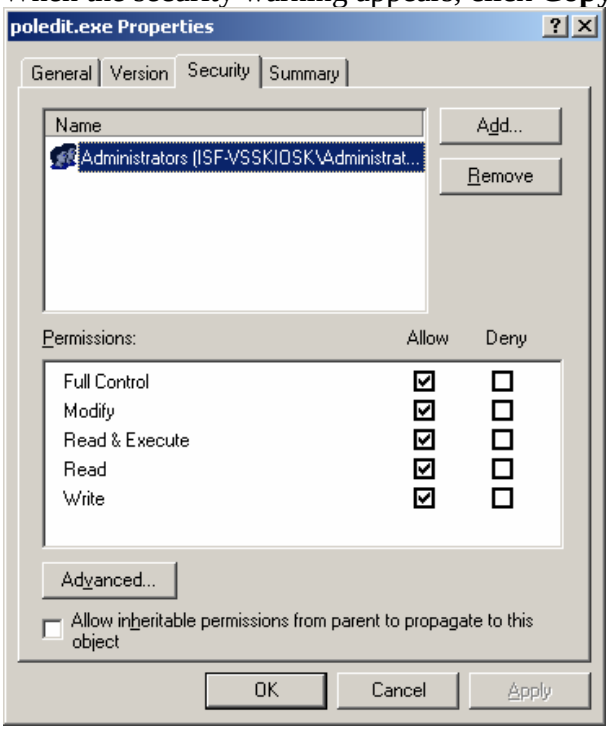
5. [**Optional Step**] To configure the kiosk to suppress the print dialog when printing meal tickets, an ActiveX control must be installed. If the ActiveX control is not installed, the meal tickets will still print. However, a print dialog, allowing the volunteer to change the print settings (in particular the number of tickets to print), will appear each time. Also, the OK or Cancel button will have to be clicked to continue. For instructions on installing the ActiveX control, refer to *Configure and Install the ActiveX Control* at the end of these Kiosk Setup Steps.

6. ***Logon as a local machine administrator.*** Install the System Policy Editor (POLEDIT) on the workstation.
   NOTE: For the auto-login policy definitions, see *Appendix A* of this document.

   a. Copy the files located in c:\VSSTemp\Policy folder to the required directory. The following table lists the files that you need and the location to which they must be copied.
      NOTE*:* For Windows XP, %SystemRoot% is typically C:\WINDOWS.
      NOTE: The %SystemRoot%\Inf\IEAK folder will need to be created.

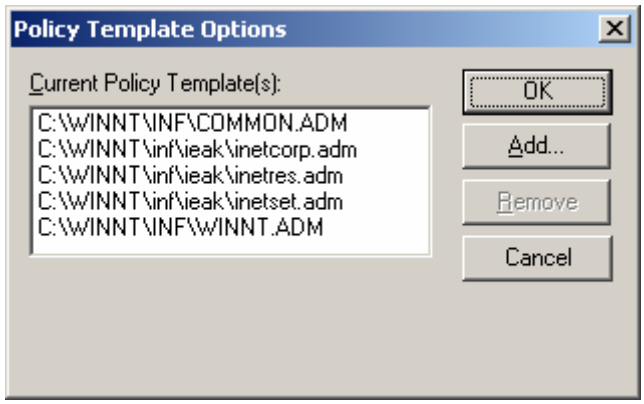
File name	Location
Poledit.exe	%SystemRoot%
Common.adm	%SystemRoot%\Inf
Winnt.adm	%SystemRoot%\Inf
Poledit.chm	%SystemRoot%\Help
Inetcorp.adm	%SystemRoot%\Inf\IEAK
Inetres.adm	%SystemRoot%\Inf\IEAK
Inetset.adm	%SystemRoot%\Inf\IEAK

b. Protect access to the **Poledit.exe** file. Limit access to Administrators only.
   i. Right-Click on the file, then choose **Properties**.
   ii. Select the **Security** tab and click the **Advanced** button.
   iii. Clear the **Inherit from parent the permissions…** check box.
   iv. When the security warning appears, click **Copy** to permit name deletions.



   v. Delete names as required, and click **OK.**

c. Attach the IEAK Policy Templates to System Policy Editor.
   i. Double click **Poledit.exe**. It will be located in %System Root%.
   ii. With no policy open, select **Options | Policy Template.**
   iii. Click **Add…** and add the **inetcorp.adm, inetres.adm** and **inetset.adm** files located in %SystemRoot%\Inf\IEAK.

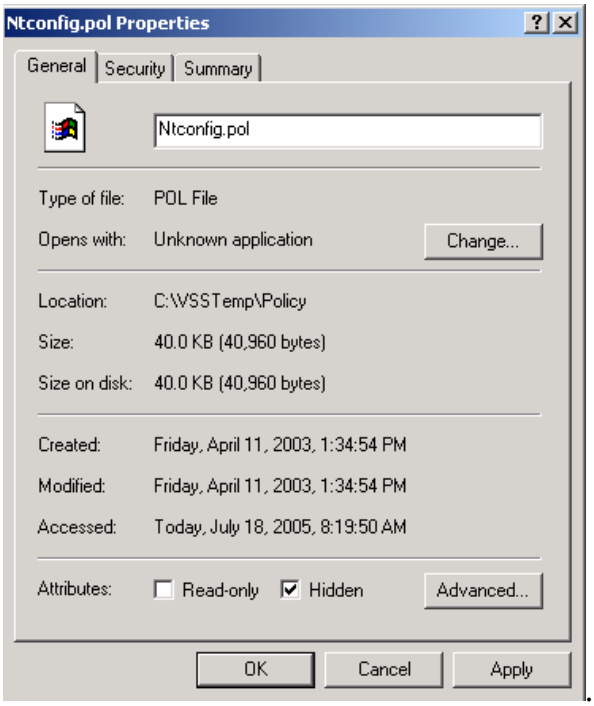


   iv. Click **OK** and then exit the System Policy Editor.

d. Install the Policy file and configure the workstation to load this file from the local drive (the default is from a domain controller on the network).

   i. Copy the policy file, **Ntconfig.pol** from c:\VSSTemp\Policy folder to %SystemRoot%.
   NOTE: For Windows XP, %SystemRoot% is typically C:\WINDOWS.

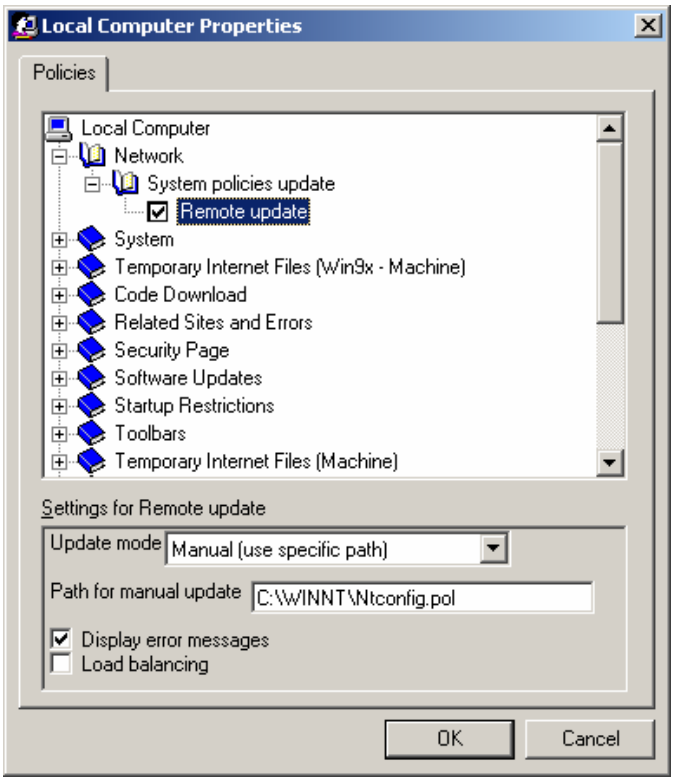
   ii. Right-Click on the file, then choose **Properties.** Give this file the **Hidden** attribute.



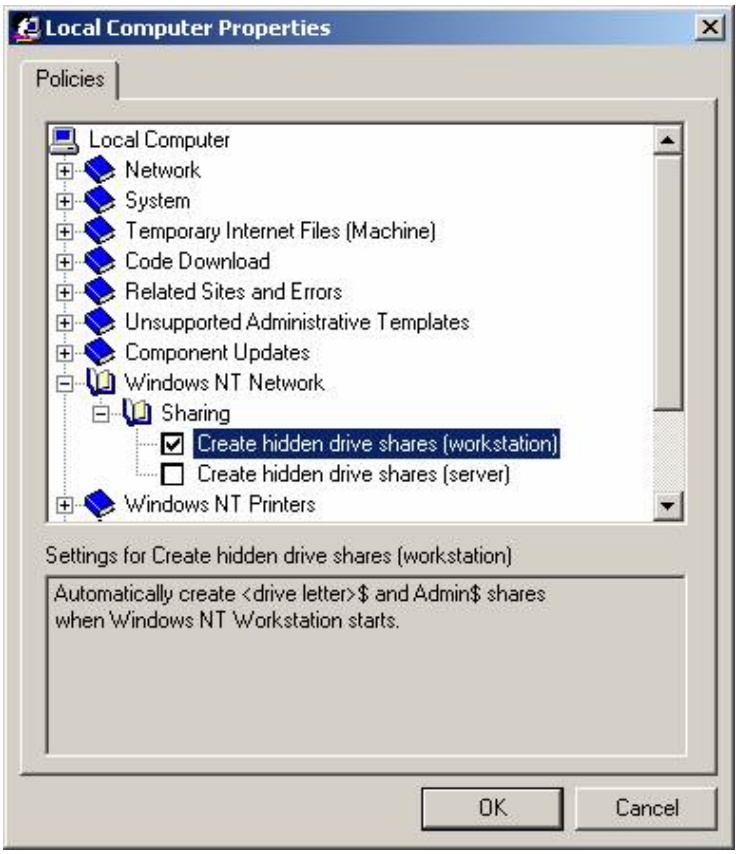
   iii. Click **OK**.

   iv. Run **Poledit.exe.** When the application starts, select **File | Open Registry** and open **Local Computer.**

   v. Expand **Network | System Policies Update.** Confirm **Remote Update** is checked. Setting for Update mode should be **Manual (use specific path)**. Path for manual update should be **C:\WINNT\Ntconfig.pol** or **C:\Windows\Ntconfig.pol**. Check the box **Display error messages**.



vi. Expand **Windows NT Network** | **Sharing**. Confirm **Create hidden drive shares [workstation]** is checked.



vii. Exit the System Policy Editor. Respond "**Yes"** to the "Do you want to save changes to the Registry?" dialog.

e. Further restrict the Start Menu, Taskbar, and Internet Explorer.

i. Start the Group Policy Editor **(Start | Run | gpedit.msc).**

ii. Perform the following steps in the Group Policy Editor :

1. **Local Computer Policy | User Configuration | Administrative Templates | Start Menu & Taskbar:**
Enable the following policies:
Remove common program groups from Start Menu
Remove Documents menu from Start Menu
Remove Help menu from Start Menu
Remove drag-and-drop context menus on the Start Menu
Prevent changes to Taskbar and Start Menu Settings
Remove access to the context menus for the taskbar

2. **Local Computer Policy | User Configuration | Administrative Templates | Windows Components | Internet Explorer:**
Enable the following policies:
Search: Disable Search Customization
Search: Disable Find Files via F3 within the browser

3. **Local Computer Policy | User Configuration | Administrative Templates | Windows Components | Internet Explorer | Browser Menus:**
Enable the following policies:
Disable Context Menu
Disable Open in New Window menu option

4. Close the Group Policy Editor.

f. Further restrict Internet Explorer's Search and Help functionality.

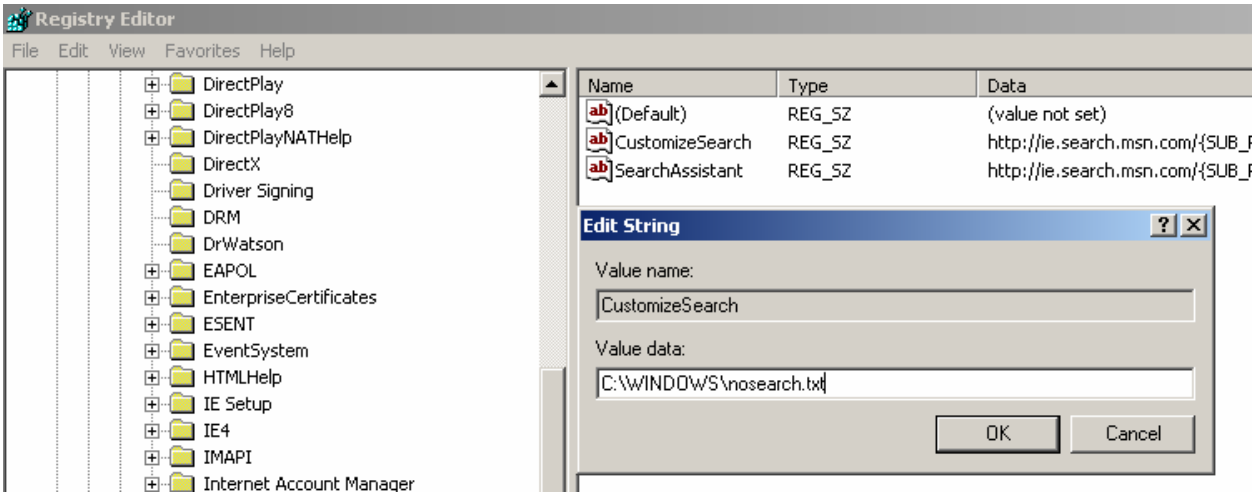
i. Disable Internet Explorer's help. Rename **iexplore.chm,** located in %System Root% \Help, to **iexplore.chm.old.** Click **Yes** on the Rename Warning.

ii. Using Notepad, create a text file with the following content: "Search is disabled." Save the file in the %System Root% as **nosearch.txt.** Assign it **Read-Only** and **Hidden** attributes.

iii. Start the Registry Editor **(Start | Run | regedit).**

1. Navigate to:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search.

2. Double click the **CustomizeSearch** and **SearchAssistant** Registry Keys and change the **Value data** fields to the following:
CustomizeSearch: %SystemRoot% \nosearch.txt
SearchAssistant: %SystemRoot% \nosearch.txt



NOTE: For Windows XP, %SystemRoot% is typically C:\\WINDOWS.

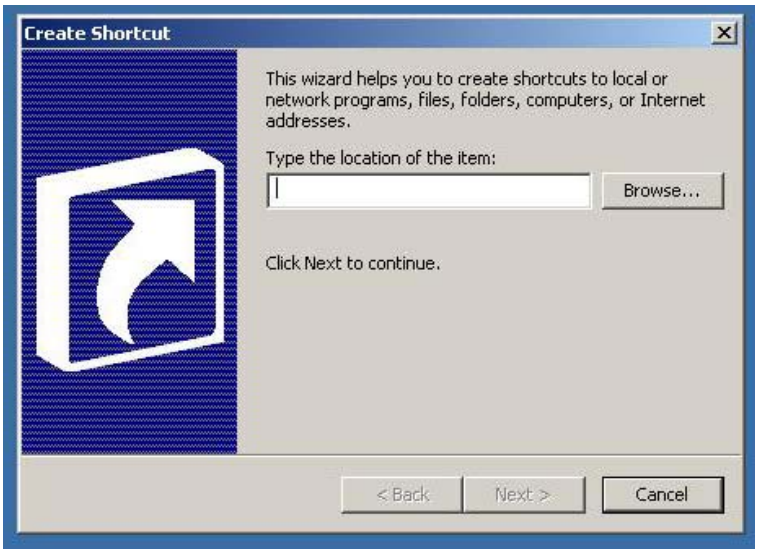
3. Exit the Registry Editor.

iv. Disable search in Internet Explorer.

1. Start Internet Explorer.
2. Click the **Search** button on the toolbar.
3. If the Search window displays “Search is disabled”, proceed to Step 7. If it is displaying the Search Companion window, accomplish the following steps.
   a. Click **Change Preferences** and then click **Change Internet search behavior**.
   b. Click **With Classic Internet Search** and then click **OK**.
   c. Restart Internet Explorer for the changes to take effect.

7. ***Login as vtkuser.*** Confirm that the application runs as intended with the implemented restrictions in effect.
   a. Open a new Internet Explorer window.
   b. Click the **Search** icon.
   c. Confirm the statement **Search is disabled** appears.

8. ***Logon as a local machine administrator***.
    a. Create a shortcut to Internet Explorer to run in "kiosk mode".
        i. Right-Click on an empty area on the desktop. Choose **New | Shortcut.**
        ii. In the **Type the location of the item** text box, enter:
        "***C:\Program Files\Internet Explorer\IEXPLORE.EXE" –k***



IMPORTANT: It is essential that a space character be inserted before the "-k" (dash k) for the shortcut to work. The "-k" switch causes Internet Explorer to open in Kiosk Mode.

        iii. Click **Next.**
        iv. In the **Name** text box, type ***VSS Kiosk.***
        v. Click **Finish.**

    b. Copy the shortcut to:
C:\Documents and Settings\vtkuser\Start Menu\Programs\Startup.

9. ***Logon as vtkuser.*** Verify that Internet Explorer runs at startup. When run in Kiosk mode, the Internet Explorer title bar, menus, toolbars, and status bar are not displayed and Internet Explorer runs in Full Screen mode.

10. ***Logon as a local machine administrator***.

    Start the Group Policy Editor **(Start | Run | gpedit.msc)** and perform the following steps.

    Local Computer Policy | User Configuration | Administrative Templates |
    Windows Components | Windows Explorer:
    Enable the following policies:
    Prevent access to drives from My Computer

Configure and Install the ActiveX Control [Optional]

These steps are referred to in Step 5 in the "Auto-Login Kiosk Setup Instructions" section.

Configuring a VSS Kiosk to use the ActiveX Print Controller consists of the following activities.

- Installing the VACertify Certificate
- Installing the Kiosk ActiveX Print Controller
- Enabling Kiosk ActiveX Printing

A. Installing the VACertify Certificate

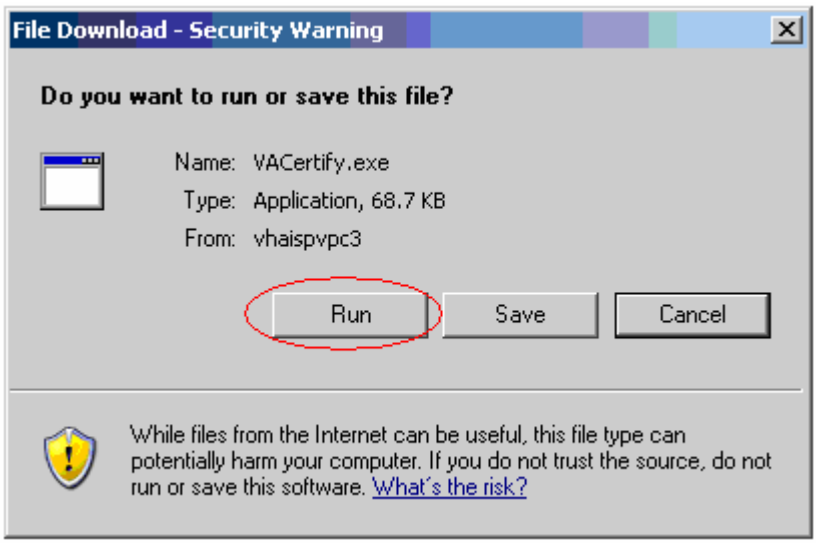
1. Logon as a **local machine administrator**.

2. **NOTE:** *This step may not be necessary if the control is being installed during an initial kiosk configuration. (Group policies have not been changed yet.)*

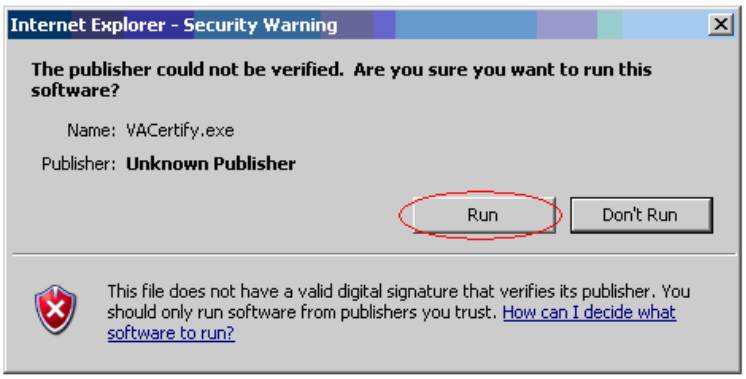
   Start the Group Policy Editor **(Start | Run | gpedit.msc)** and perform the following steps:

   Local Computer Policy | User Configuration | Administrative Templates | Windows Components | Windows Explorer:
   Disable the following policies:
   Prevent access to drives from My Computer

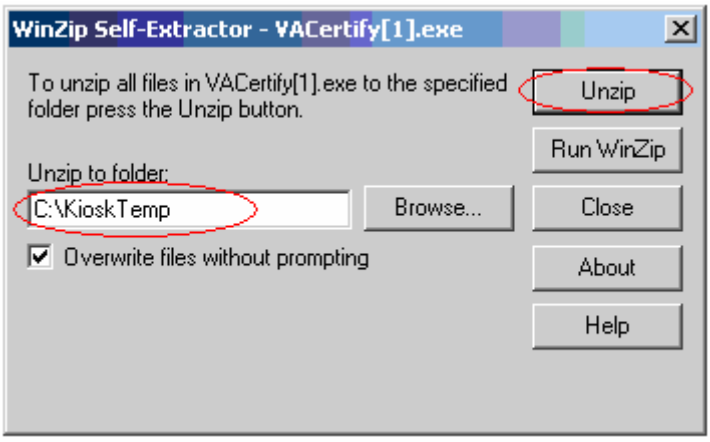
3. Open Internet Explorer and type the following URL: (http://vaww.vss.med.va.gov/VtkUser/Utility/VACertify.exe) into the address box and click the "Go" button to launch the File Download dialog. The VACertify.exe is a self extracting zip file which contains a certificate which needs to be installed on the kiosk. Click "*Run*".



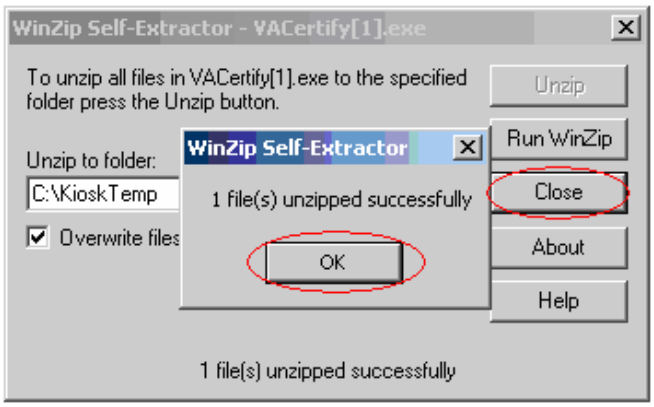
4. An Internet Explorer warning will appear saying "*The publisher could not be verified.*" This is an expected response. Click "*Run*".



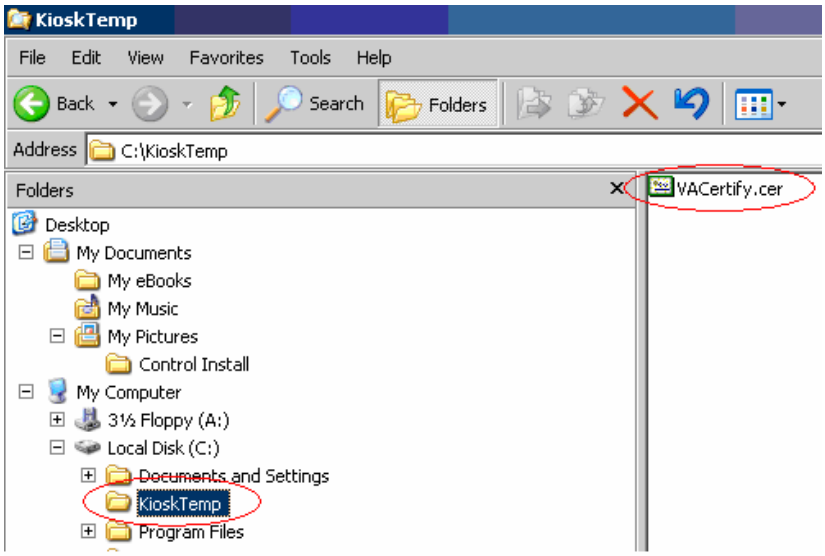
5. When the WinZip window appears, type "*C:\KioskTemp*" in the *Unzip to folder* window, and click "*Unzip*".



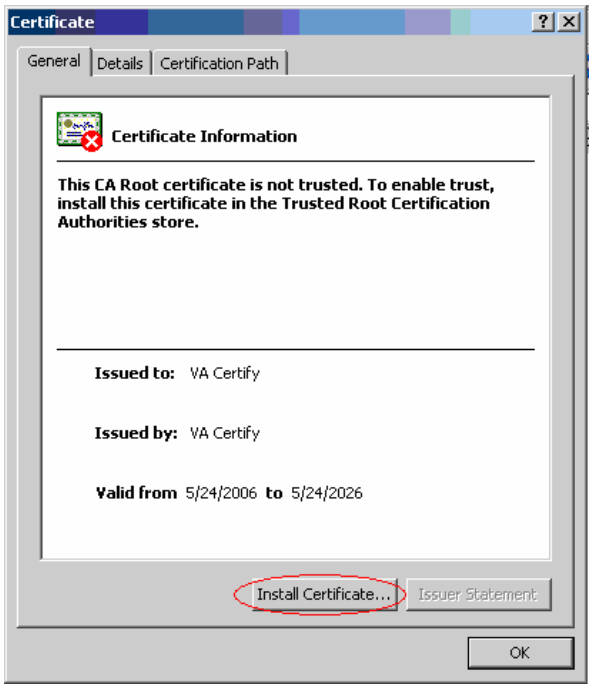
6. Click "*OK*" then "*Close*."



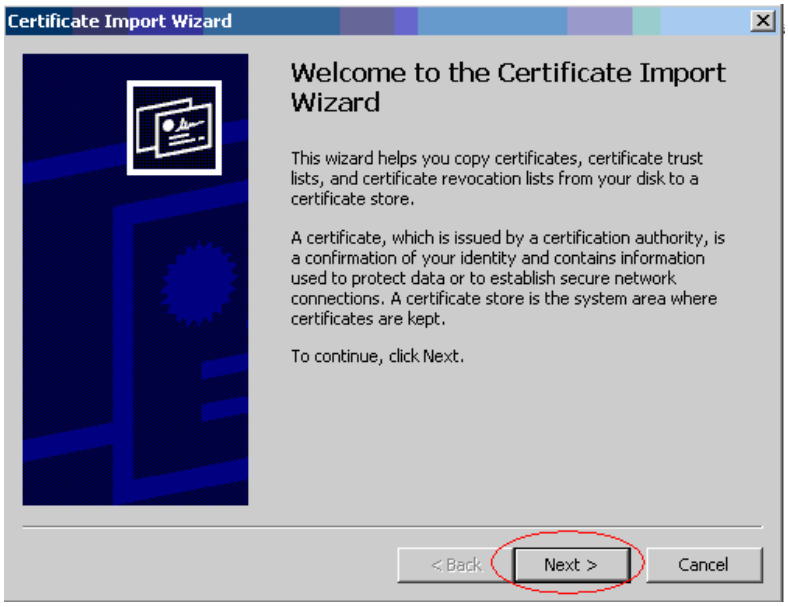
7. Open the *KioskTemp* folder and double-click on *VACertify.cer*.



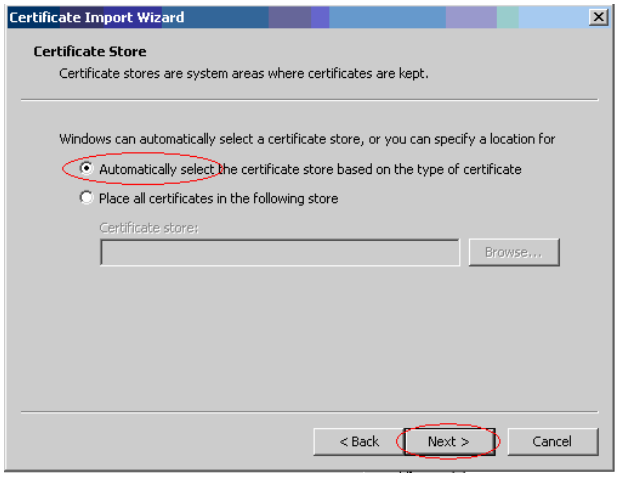
8. When the Certificate window appears, the General tab will say "*This CA root certificate is not trusted*." This is an expected response. Click the "*Install Certificate*" button.



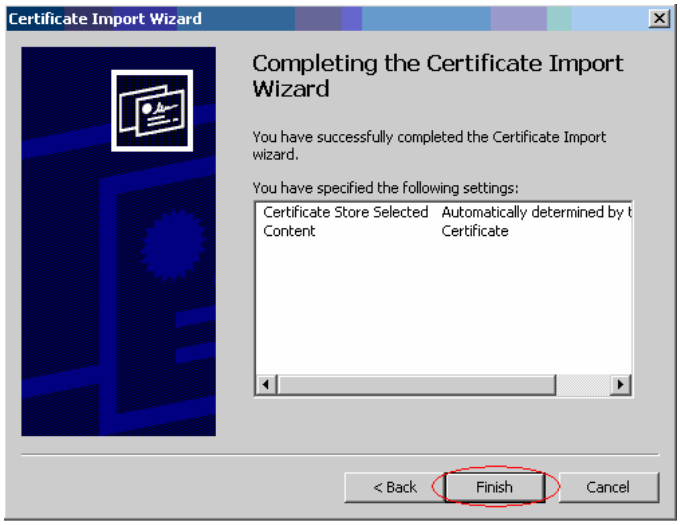
9. When *the Certificate Import Wizard* appears, click "*Next*."



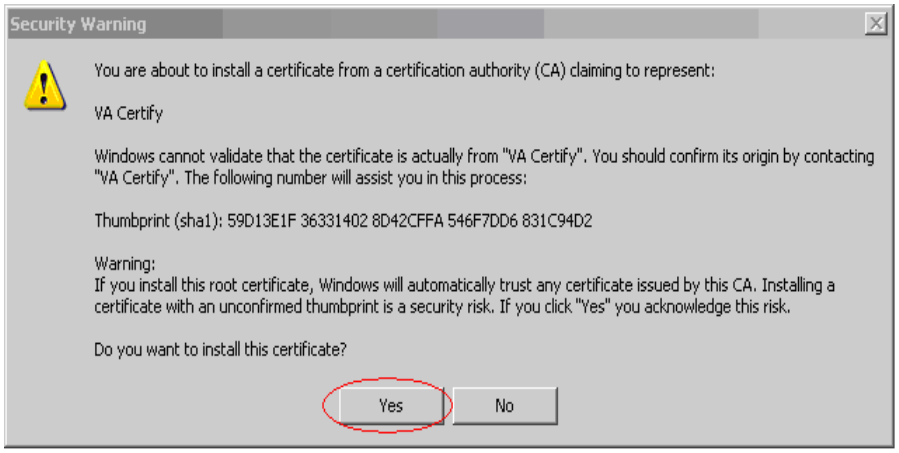
10. At the *Certificate Store* screen, ensure "*Automatically select. . .*" is chosen, then click "*Next.*"



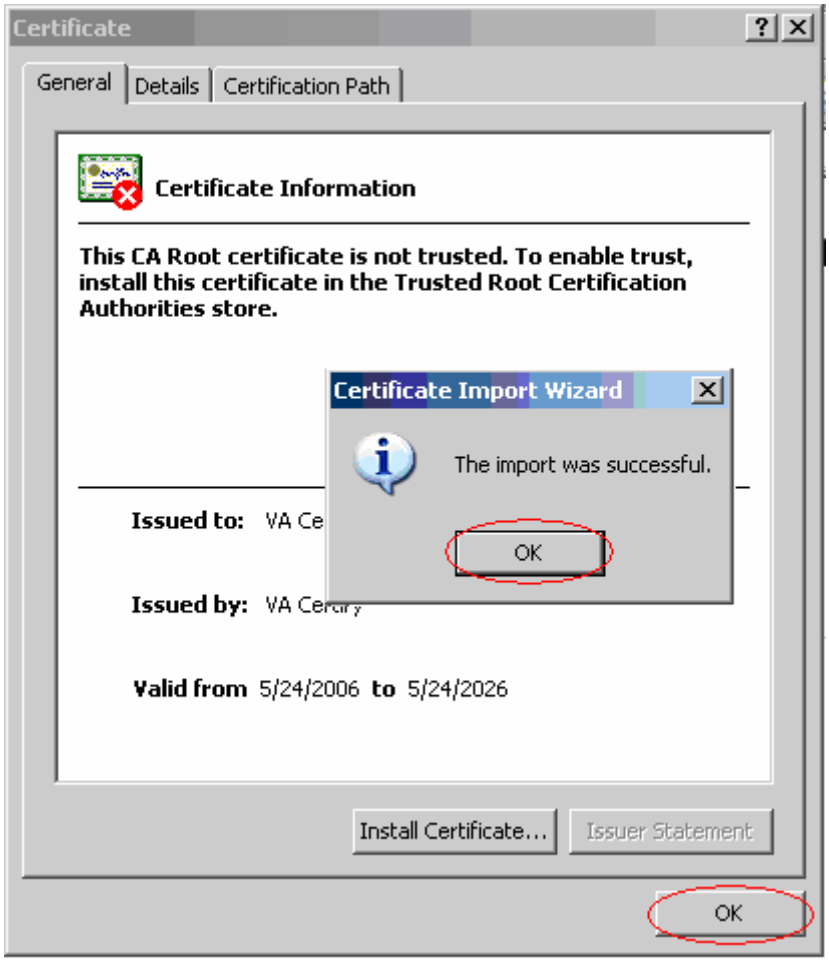
11. At the *Completing* page, click "*Finish.*"



12. A security warning will appear. This is an expected response. Click "*Yes.*"



13. Click *"OK"* on *"The Import was successful"* window, then click *"OK"* on the Certificate window. The certificate is now installed.



14. [**Optional Step**] The C:\Kiosk Temp directory that was created in Step 5 can be deleted (as well as the VACertify.cer file).

B. Installing the Kiosk ActiveX Print Controller

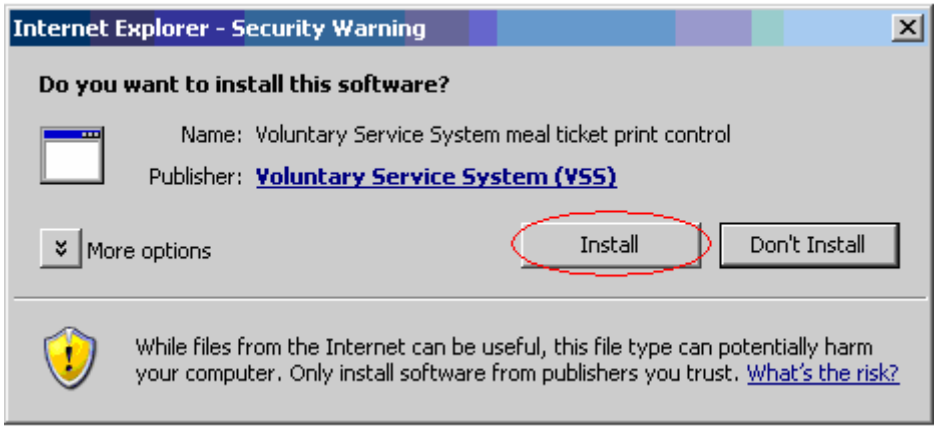
NOTE: These steps should be performed for ***all*** kiosks at a station ***before*** enabling ActiveX printing**.**

1. Logon as a **local machine administrator**.
2. Open Internet Explorer and type the following URL into the address box and click the *"Go"* button.

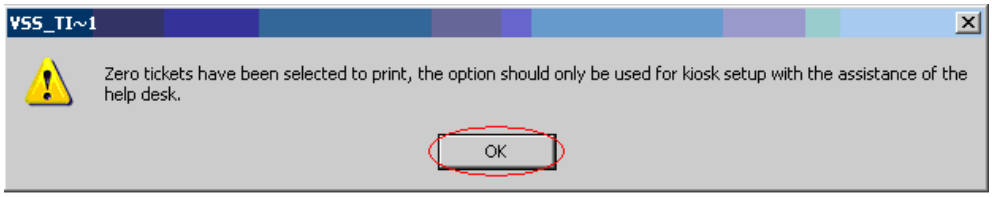
   (http://vaww.vss.med.va.gov/vtkuser/PrintMealTicketAx.htm?Time=0&Name=Test&Price=0&NumberOfMeals=0&VolId=0&SiteId=0)

   [This is done to access the web page containing the new control that needs to be downloaded to the kiosk. The initial download of the control has to be done by an administrator. Once downloaded, any user (even if not in the Administrators Group) will be able to use the control.]

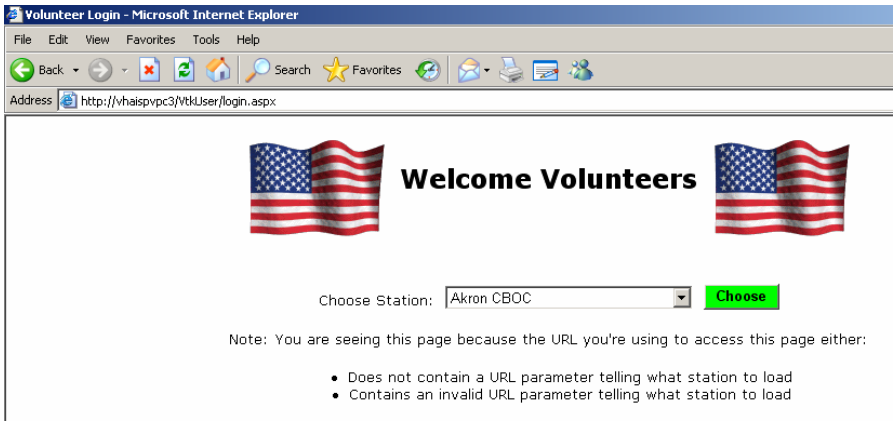
3. An Internet Explorer warning will appear saying "*Do you want to install this software*?" This is an expected response. Click "*Install*".



4. The "*Zero tickets have been selected. . .*" message will appear. This is an expected response. Click "*OK*."



5. You will be redirected to the generic VSS Login. The ActiveX print controller is now installed.

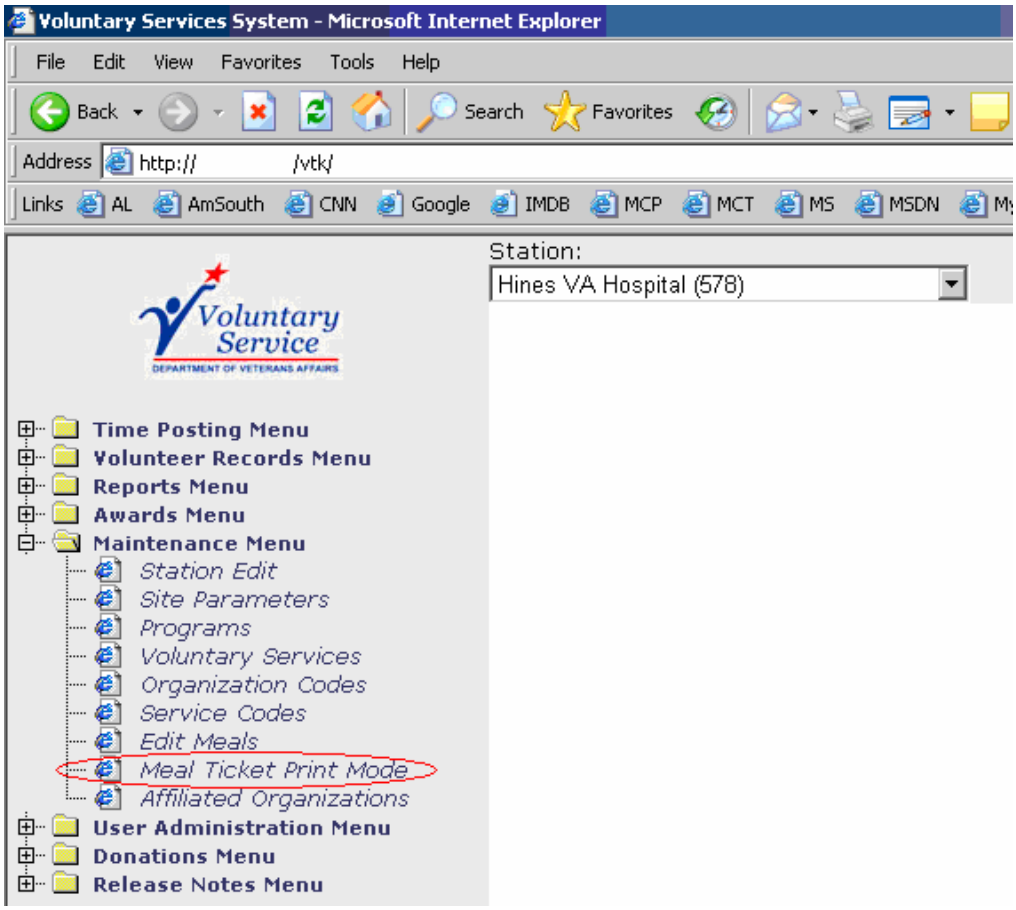


6. Use these same steps, as required, for multiple kiosk installations.

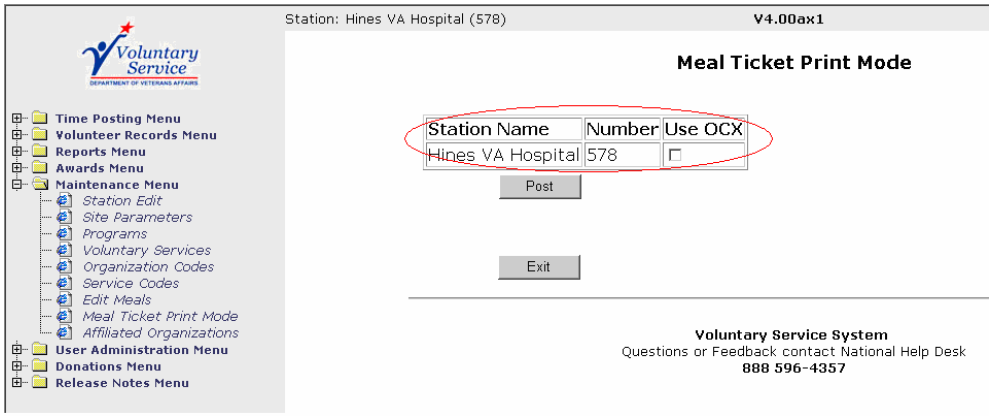
C. Enabling Kiosk ActiveX Printing

NOTE: These steps should be performed ***after*** the ActiveX print controller has been installed at ***all*** kiosks at a station**.** Any kiosks at your station that have not been configured for ActiveX printing will no longer print meal tickets once the station has been switched to OCX mode.

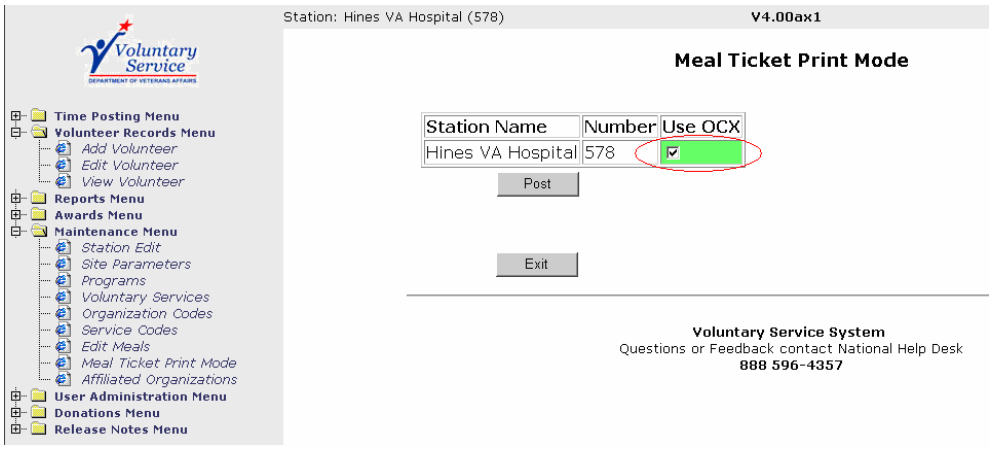
1. Open the VSS Timekeeping application.
2. Expand the *Maintenance Menu* and choose "*Meal Ticket Print Mode.*"



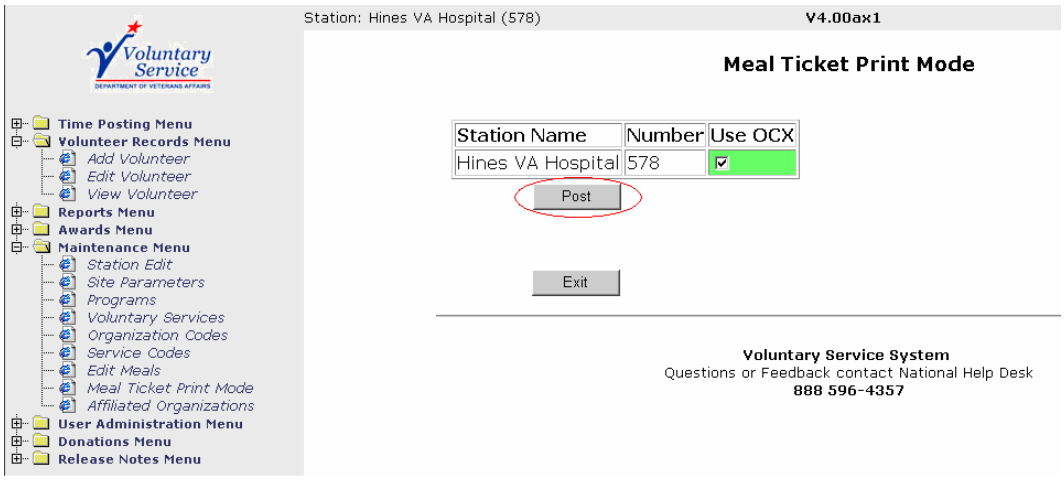
3. On the *Meal Ticket Print Mode* page, check the "*Use OCX*" box for the station you want to activate.



4. Note the "*Use OCX*" box turns green for the selected station.

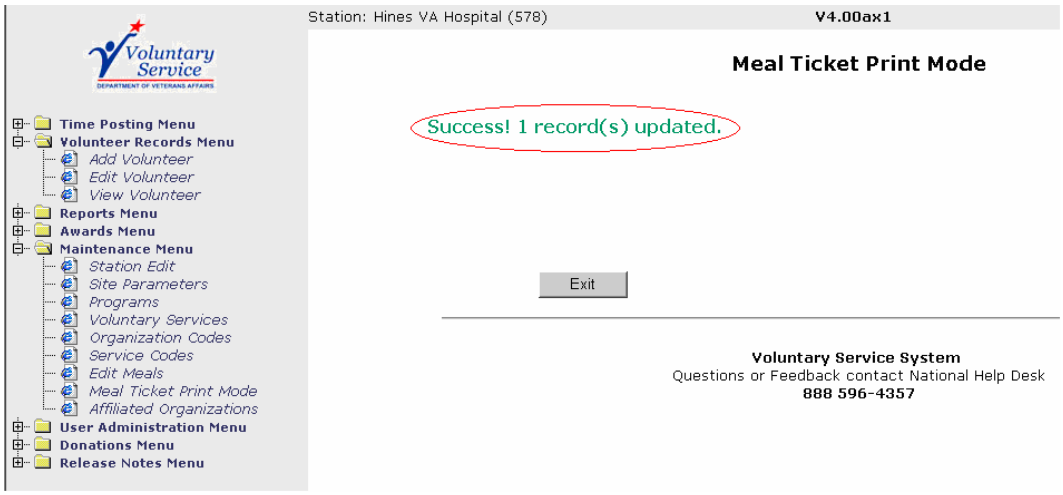


5. Click "*Post.*"

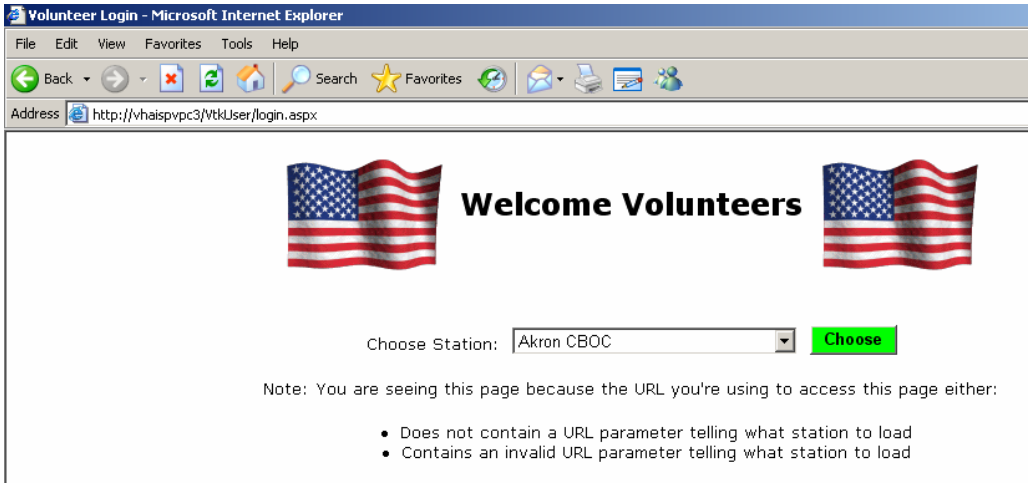


6. Confirm Success.

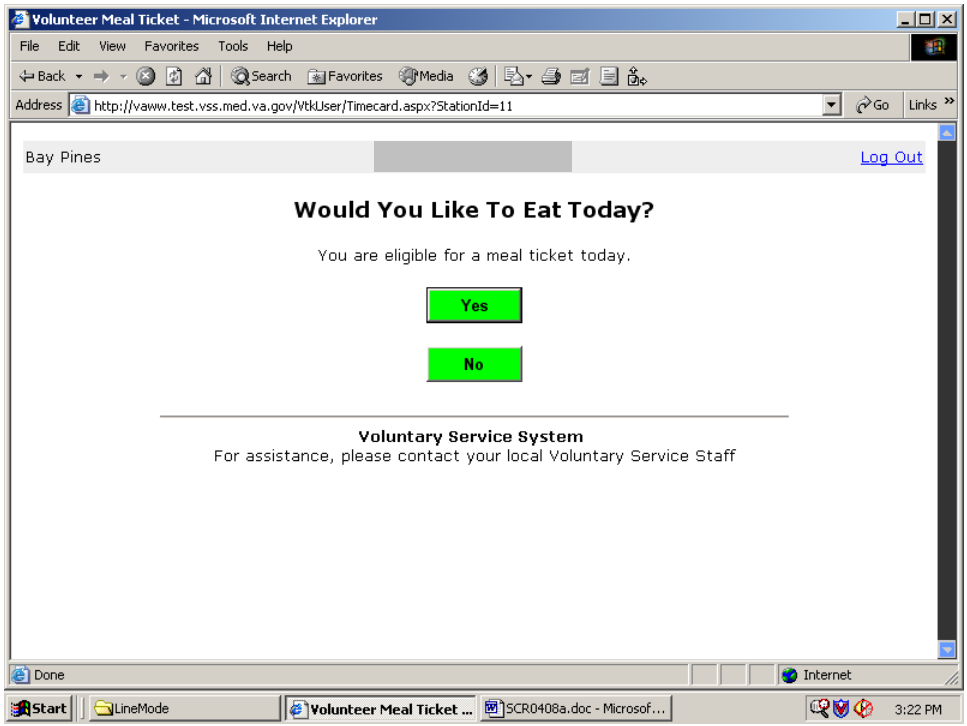
NOTE: The resulting confirmation screen will only appear for approximately 5 seconds before it returns to the *Meal Ticket Print Mode* page.



7. Close the Internet Explorer window then open a new one. Navigate to http://vaww.vss.med.va.gov/vtkuser. Choose the appropriate station from the dropdown list.



8. Generate a meal ticket using a valid volunteer ID and verify printing. Confirm the print dialog box does not appear during the print process.



9. Logon as ***vtkuser***.
10. Perform Steps 7 and 8 above to confirm proper printing.
11. Logon as a **local machine administrator**.
12. **NOTE:** *This step may not be necessary if the control is being installed during an initial kiosk configuration. (Group policies have not been changed yet.)*

    Start the Group Policy Editor **(Start | Run | gpedit.msc)** and perform the following steps:

    Local Computer Policy | User Configuration | Administrative Templates | Windows Components | Windows Explorer:
    Enable the following policies:
    Prevent access to drives from My Computer

TROUBLESHOOTING

The user policy is by design very restrictive. It is not possible to make even the smallest environment change when logged in as the local user. Use a local administrator account for this purpose – e.g., to change the Page Setup setting in Internet Explorer.

If you are not able to make a change as a local user, the only alternative is to delete the local user account, recreate it (it can have the same name), and redo the setup steps listed above. Therefore, you should finalize any environmental settings before applying the policy (Steps 2 through 7).

Appendix A - Auto-Login Policy Definitions

The following list displays the actual policy settings as implemented. Policy Editor defines three states of policy changes: set (checked), unset (cleared), and unchanged (grayed). All listed policies below are set except those preceded by the "!" character which represents "Not" (unset, cleared). All other settings are unchanged, "N/C". To view or edit these settings, run POLEDIT, confirm the kiosk setup templates are loaded, and open the policy file %SystemRoot%\Ntconfig.pol (on Windows XP the %SystemRoot% is typically C:\WINDOWS).

Each user policy has a properties dialog which displays all categories, policies, and parts for that user policy. You can open the properties dialog for a policy in two ways: you can double-click the icon corresponding to the user policy you want to edit (i.e., vtkuser) or you can select it with the mouse and use the **Edit | Properties...** command.

The upper part of the properties dialog shows a tree view of the categories within the active user policy. When you first open a user policy, the categories are all collapsed. You can expand or collapse individual items by clicking the small +/- icon next to the category's name.

As you expand categories, you'll see checkboxes appear beneath them. Unlike normal Windows checkbox controls, these checkboxes can have three states.

- When checked, the policy is set (active) and its settings will be applied to turn on the policy when appropriate.
- When cleared, the policy is unset (inactive) and its settings will be applied to turn off the policy.
- When unchecked and gray, the policy is unchanged (inert). No changes will be made to a policy or its parts when its checkbox is grayed.

You must pay careful attention to the wording of the policy to make sure that the effect is what you intend. For example, when the checkbox next to "Disable Registry editing tools" is checked, the tools are disabled. When it's cleared, the tools are not disabled, and when it's unchecked and gray, the settings currently in effect on each target machine, group, or user remain intact.

As you select individual policies within a category, notice that the contents of the settings area at the bottom of the properties dialog change. Some policies can have multiple parts; for example, the "Restrict display" policy has a total of five parts. You can set the value of each part independently of the others. Parts may accept on/off, numeric, or list selection choices, depending on what the policy template specifies.

You can move through the properties dialog making changes as you go. POLEDIT preserves the changes within the current editing session, but they'll be lost unless you save the policy file.

POLICY DEFINITIONS FOR: *vtkuser*

Implemented by templates from the Internet Explorer Administration Kit (IEAK)

Temporary Internet Files (User)
  N/C

Internet Property Pages
  Internet Property Pages
    Disable viewing the General Page
    Disable viewing the Security Page
    Disable viewing the Content Page
    Disable viewing the Connections Page
    Disable viewing the Programs Page
    Disable viewing the Advanced Page
    Disable changing any settings on the Advanced Page

General Page
  General Page
    Disable changing home page settings
    Disable changing Temporary Internet files settings
    Disable changing history settings
    Disable changing color settings
    Disable changing link color settings
    Disable changing font settings
    Disable changing language settings
    Disable changing accessibility settings

Connections Page
  Connections Page
    Disable Internet Connection Wizard
    Disable changing connection settings
    Disable changing proxy settings
    Disable changing Automatic Configuration settings

Content Page
  Content Page
    Disable changing ratings settings
    Disable changing certificate settings
    Disable changing Profile Assistant settings
    Disable AutoComplete for forms and saving of submitted strings
    Do not allow users to save passwords in AutoComplete for forms

Programs Page
  Programs Page
    Disable changing Messaging settings
    Disable changing Calendar and Contact settings
    Disable the Reset Web Settings feature
    Disable changing checking if Internet Explorer is the default browser

Browser Menus
  File Menu
    Disable Save As... menu option
    Disable New Window option from File menu
    Disable Open menu option
    Disable Save As Web Page Complete format
    Disable closing of the browser
    !Disable printing from the browser
  View Menu
    Disable Source menu option
    Disable Fullscreen menu option
  Favorites Menu
    Hide Favorites Menu
  Tools Menu
    Disable Internet Options... menu option
  Help Menu
    Remove 'Tip of the Day' menu option
    Remove 'For Netscape Users' menu option
    Remove 'Tour' menu option
    Remove 'Send Feedback' menu option
  Context Menu (right click)
    Disable Context Menu
    !Disable Open in New Window menu option
  File Download Dialog
    Disable Save this program to disk option

Favorites and Search
  Favorites Import/Export
    Disable importing and exporting of favorites
  Search
    Disable Search Customization
    Disable Find Files via F3 within the browser

Persistence
  N/C

Dial-Up Settings
  N/C

Language Settings
  Language Settings
    Default language for menus and dialogs: English

Temporary Internet Files (User)
  N/C

Toolbars
  Default Toolbar Buttons
    Show small icons
    Back button: Turn button off
    Forward button: Turn button off
    Stop button: Turn button off
    Refresh button: Turn button off
    Home button: Turn button off
    Search button: Turn button off
    History button: Turn button off
    Favorites: Turn button off
    Folders button: Turn button off
    Fullscreen button: Turn button off
    Tools button: Turn button off
    Mail button: Turn button off
    Font size button: Turn button off
    Print button: Turn button on
    Edit button: Turn button off
    Discussions button: Turn button off
    Cut button: Turn button off
    Copy button: Turn button off
    Paste button: Turn button off
    Encoding button: Turn button off
    Print preview button: Turn button off

Advanced Settings
  Browsing
    !Launch browser in full screen mode

AutoComplete
  N/C

Display Settings
  N/C

Advanced Settings
  Browsing
    !Disable script debugging
    !Show friendly URLs
    Use smooth scrolling
    Enable page transitions
    Enable page hit counting
    !Automatically check for Internet Explorer updates
    Underline links: Always
    !Enable folder view for FTP sites
    !Show Go button in Address bar
    Show friendly http error messages
    !Display a notification about every script error
    All others N/C

URL Encoding
  N/C

Implemented by standard Windows templates

Control Panel
  Display
    Restrict display
      Deny access to display icon
      Hide Background tab
      Hide Screen Saver tab
      Hide Appearance tab
      Hide Settings tab

Desktop
  !Wallpaper
  Color scheme
    Scheme name: Windows Default

Shell
  Restrictions
    Remove Run command from Start menu
    Remove folders from Settings on Start menu
    Remove Taskbar from Settings on Start menu
    Remove Find command from Start menu
    Hide drives in My Computer
    Hide Network Neighborhood
    No Entire Network in Network Neighborhood
    No workgroup contents in Network Neighborhood
    Hide all items on desktop
    Remove Shut Down command from Start menu
    Don't save settings at exit

System
  Restrictions
    Disable Registry editing tools
  All others N/C

Windows NT Shell
  Custom user interface
    N/C
  Custom folders
    N/C
  Restrictions
    Remove View->Options menu from Explorer
    Remove Tools->GoTo menu from Explorer
    Remove File menu from Explorer
    Remove common program groups from Start menu
    Disable context menus for the taskbar
    Disable Explorer's default context menu
    Remove the "Map Network Drive" and "Disconnect Network Drive" options
    Disable link file tracking
    Remove NT Security item from Start menu
    Remove Disconnect item from Start menu
    Prevent user from changing file type associations
    All others N/C

Windows NT System
  Disable Task Manager
  Disable Change Password
  !Show welcome tips at logon
  All others N/C

Windows NT User Profiles
  N/C