

Windows
Embedded
Standard 7
(WES7)

Administration Guide



Notes, Cautions, and Warnings



NOTE: A NOTE indicates important information that helps you make better use of your computer.



CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.



WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Information in this publication is subject to change without notice.

Contents

- Introduction6**
 - What is Windows Embedded Standard 7 (WES7)?6
 - WES7 Features6
 - WES7 Installation7
 - First Boot Wizard.....7

- Understanding Your Thin Client8**
 - Users and Groups8
 - Creating New User Accounts.....10
 - File-Based Write Filter (FBWF).....12
 - Installing MUI Packs16
 - Setting a Language17

- Using Your Thin Client29**
 - Customizing Your Thin Client29

Thin Client Options	31
Echo Agent System Information	31
Installing or Removing Peripherals	33
Installing a Printer	33
Installing a Scanner or Camera	34
Installing a CD-ROM	36
Uninstalling Software	37
Uninstalling or Updating a Media Device	37
Freeing Local Drive Space	38
Networking	39
Setting Static/Dynamic IP	39
Naming Your Thin Client, Joining a Domain or Workgroup	40
Using Connections	42
Using Remote Desktop	42
Using Citrix ICA	43
Using VMware View	45
OS Build Date, Echo Agent, and Re-Imaging	46

Verifying OS Build Date	46
Verifying the Echo Agent Version and Status	47
Re-Imaging the Thin client.....	48
Echo Control Panel.....	49
Network Tools	50
Connections	51
Citrix ICA	53
Internet Explorer Browser	57
VMware View	59
rDesktop	61
VDI In A Box.....	67
Getting Help.....	68

Introduction

What is Windows Embedded Standard 7 (WES7)?

Windows Embedded Standard 7 (WES7) is a fully componentized operating system that is the successor of Windows Embedded Standard. It also provides the full Windows 7 interface and is available for embedded systems.

WES7 Features

- **Multimedia Web Browsing**-WES7 comes equipped with Internet Explorer 8 with improved navigation and supports CSS styling and RSS feeds. Windows Media Player 12 is included to manage your digital music, photo, and video libraries. WES7 also comes with Microsoft Silverlight for running interactive applications right from your Thin Client, DirectX 11 for 3D and full-color video, and supports both digital and analog television for streaming your favorite shows or even video recording.
- **Modern Networking**-WES7 can connect to hosted desktops using the industry's best protocols: PCoIP, Citrix, RDP 7.1 compatibility with RemoteFX, and VMware View. WES7 also uses 802.11, 802.1X, and WPA2 for wireless connections and protection, Plug and Play support for intelligent devices, USB 2.0 support, and Internet Connection Sharing.
- **Third Party Clients**-Acer thin clients also include commonly used client server applications such as the Citrix Online Plug-in and VMware View.
- **File-Based Write Filter (FBWF)**-Allows the administrator to select individual files or folders to be protected from change while other files/folders on the same partition can be updated.
-

- **USB Flash Boot**-The Acer thin clients are capable of being re-imaged from a bootable USB Flash Device with the .EXE executable image file on it.
- **Centralized Management**-Acer thin clients with WES7 can be easily managed with Acer Echo Management Console.

WES7 Installation

Windows Embedded Standard 7 operating system is preinstalled on WES7 based systems. A USB Re-Imaging Utility is available at **acer global download center** if you need to reinstall the operating system.

First Boot Wizard

The first time your terminal boots up, you will be taken through a first boot wizard. This wizard can help you to configure a variety of settings in order to better utilize your terminal. It is advised that you are familiar with the material in this guide as well as the Acer Echo Administration Guide to best utilize the first boot wizard.

Understanding Your Thin Client

Users and Groups

What is a User Account?

The term user account should not be confused with the actual User account that is the default account upon log-in. For each person using the terminal, the owner can create an individual account. Each user account created can have certain rights or permissions as chosen by the Administrator account. The Administrator account can create, delete, and edit each of the users' settings whenever needed.

User Account

The User account is the account that will automatically log-in at every boot. It is also the account that should be used for guests or any user what should be prohibited from modifying the thin client or its local drive in any way. There is no password on this account by default. The User account holder can change his or her account picture and create, delete, or change their account password. The user account cannot change their own account name or account type, nor can they install or uninstall any software. They may, however, use software installed by the Administrator account.

Administrator Account

By default, the User account is automatically logged in. To bypass this, you can hold <Shift> during the boot process or hold <Shift> and click **Log Off**, which can be seen by selecting the right arrow next to the **Shut Down** button option.



NOTE: The default password for the Administrator account is Administrator (case sensitive).

Logging into the Administrator account should be very similar to the User account, with some additional icons on the desktop. Unlike the User account(s), the Administrator account can:

- Install and uninstall hardware and software.
- Create and delete user accounts on the terminal.
- Create account passwords for user accounts on the terminal.
- Change names, pictures, and passwords.
- Change a user's *account type* to administrator account.

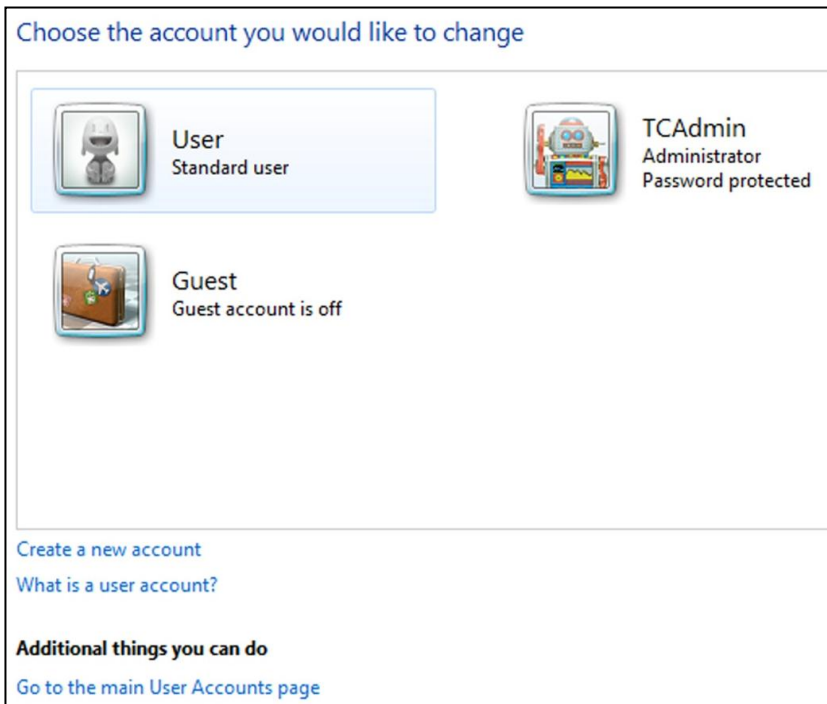


NOTE: The Administrator account cannot change its own account type to a limited User account type unless there is at least one other account with administrator-privileges on the thin client. This ensures that there is always at least one administrator-level account on the thin client.

Creating New User Accounts

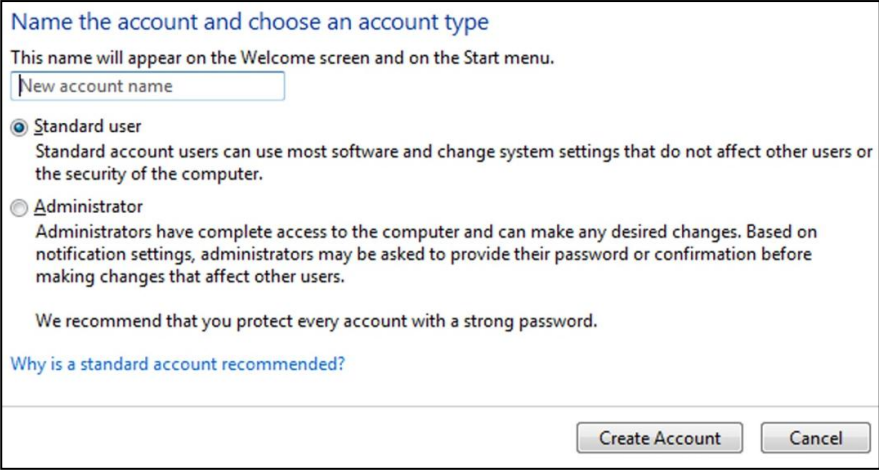
This section details how to create new users. You must first log-in using the Administrator user or an account with administrator privileges.

- 1 Select **Start->Control Panel**.



- 2 Select **User Accounts**.
- 3 Select **Add or remove user accounts**.
- 4 Select **Create a new account**.

- 5 Type a name for the new user account.



The screenshot shows a Windows dialog box titled "Name the account and choose an account type". Below the title, it says "This name will appear on the Welcome screen and on the Start menu." There is a text input field labeled "New account name". Below the input field, there are two radio button options: "Standard user" (which is selected) and "Administrator". Each option has a descriptive paragraph below it. At the bottom of the dialog, there is a link that says "Why is a standard account recommended?" and two buttons: "Create Account" and "Cancel".

Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

☒ **Standard user**
Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

☐ **Administrator**
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

[Why is a standard account recommended?](#)

- 6 Select either **Administrator** or **Standard user** account type.
Select **Create Account**.

What is the Acer Echo Management Console?

As more and more corporate networks switch to Thin Clients due to their low power consumption, low cost, and productivity, many developers have scrambled to create new and more efficient ways to centrally manage and reconfigure thin client terminals. Echo is the latest in thin client management software.

With the Echo virtual appliance, you can use broadcast and IP Range Walk to discover the thin clients, then remotely reboot, add connections and settings, add user profiles, shadow, clone settings, or even Re-Imaging some models.

File-Based Write Filter (FBWF)

What is Disk Management?

Disk Management is the management of your terminal's internal local drive disk. It is quite literally the brain of your unit and taking care of the unit's disk is the best way to ensure the unit will perform for as long as possible. A carefully preserved local drive will work more efficiently, last much longer, and perform better overall. In addition, proper security techniques will greatly reduce the chance of fatal error messages and/or accidental malicious software downloads.

Another definition of the word management literally refers to managing several thin clients from an Administrator terminal. The Administrator terminal logs into a secure Echo server and can manage multiple thin clients simultaneously. Your terminal is designed with both management techniques in mind, and this chapter explains the steps required to manage your terminal correctly. The terminal's local drive disk is protected by a *Write Filter*, which acts like a barrier between the internet and your actual local drive. The user can use this barrier to protect and manage the terminal's actual local drive from unwanted changes. The terminals can also be managed remotely from another terminal using the Echo Thin Client Management Software. Both ideas are introduced in this section.

Write Filters

A write filter allows the user to decide which files are saved to the local drive, and which files or changes are discarded. Use the write filter to configure which files are written to the disk permanently, and which files are only written to an overlay in the memory. The write filter, when turned on, will make disk changes like installing new hardware, upgrading internet browsers and plug-ins, or isolating a virus to the terminal's memory, in an overlay. The changes are not saved to the local drive. The next time the terminal is rebooted, the new hardware is not installed, your browser or plug-in is not upgraded, and the virus is gone. All of the changes are stored on a memory overlay and are erased on reboot. Once the memory overlay is wiped clean, the original underlying image remains unchanged, still in the state it was in since the last reboot. It is a good practice to leave the filter turned on unless you are upgrading or installing new hardware or software. After the installation is complete, it is recommended you re-enable the write filter.

All attacks on the terminal's security or unwanted changes can be thwarted by simply rebooting the machine if the filter is turned on. Operating the machine with the Filter turned off can be dangerous to the terminal and the important OS files inside it.

Introduction to FBWF

The File-Based Write Filter, more commonly referred to as the FBWF, is an intelligent filtering system that allows you to protect specific volumes of your local drive from write access, while simultaneously keeping less important files like anti-virus databases or a user's **Documents and Settings** folder persistent. The FBWF allows users to decide which directories are persistent and which are transient. Persistent files are files that are not protected by the FBWF filter, and all changes, good or bad, will survive after rebooting. Transient files are files that are protected by the FBWF filter and all changes that are made to these files are neglected and forgotten upon rebooting the terminal.

How Does FBWF Work?

When the FBWF is enabled, it makes your files secure from that instance. Rebooting the terminal will revert your system immediately back to the state it was in when you enabled it, like a restore point. As long as your FBWF is enabled, it is in a safe state. It stays safe because it writes all changes made on the system on an *overlay* in the RAM memory cache. An overlay can be thought of as a protective layer over the disk. All changes made to the disk are written on the transparent layer instead of the actual disk. When the terminal looks for information on the disk, all upgrades and new installs can be found and accessed because it is written on the overlay which is covering the disk.

However, once the terminal is rebooted, the memory cache is erased, and the overlay is wiped clean, with no changes made. The system automatically resumes from the same point it was at when you enabled the filter.

To install new hardware and software, or to upgrade any existing programs or applications on your system, you will have to disable the FBWF. It is important to re-enable the File-Based Write Filter as soon as the installation is complete so you can protect your terminal from unnecessary disk writes. As long as you are not installing or upgrading, it is necessary to leave the File-Based Write Filter in an enabled state for correct performance. As long as it is enabled, your terminal is safe from malicious network attacks or accidental uninstalls.

Using the FBWF

The FBWF operates by providing a *shadow write* to the system RAM. When enabled, any writes that are normally written to the storage media, are instead redirected to the RAM overlay. During a reboot, this overlay is discarded so the operating system remains in its original state. As its name implies, FBWF is based on files. This means you can exclude certain files and directories from the protection of the write filter. Any files that are in this list are ignored by FBWF and subject to modification (or deletion) just as they normally would on any standard Windows environment. Acer thin clients include a management utility for configuring FBWF. The FBWF Manager utility can only be accessed by Administrators.

To open the **FBWF Manager**, log-in as the administrator.

- Click **Start-> All Programs-> Echo Control Panel**.
- Click **FBWF**

By default, FBWF is enabled with basic exclusions set for the **Persistent Registry** and **Documents and Settings** for all users. This means any changes made under the **C:\Documents and Settings** folder, such as desktop icons, start menu items, and browser favorites, will be written directly to the flash device immediately and without overlay protection.

What is Persistence?

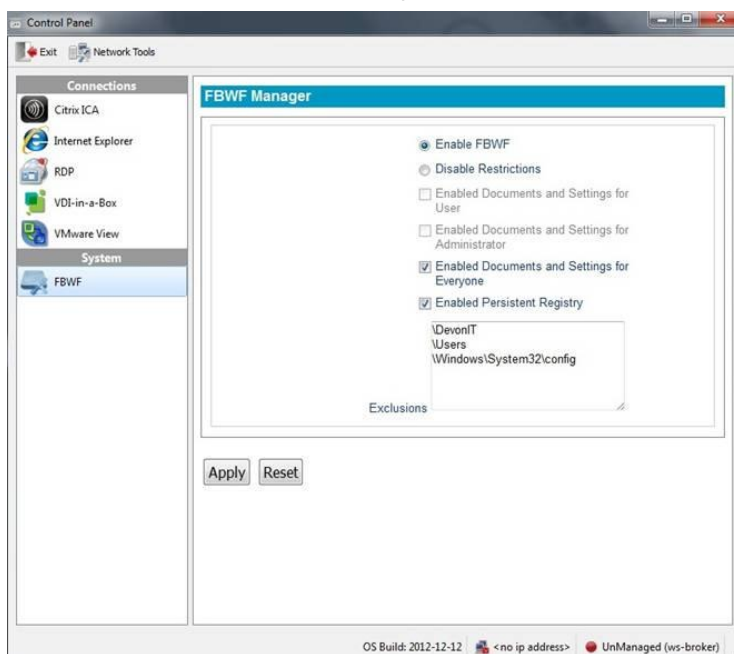
Persistence in its simplest definition is the term used to describe data on a local drive or disk that exists and survives from session to session. Persistent data will be secure after every reboot and every change made will be applied until another user reconfigures your changes. If you do not have the File-Based Write Filter installed on your terminal for protection, your local drive remains in a Persistent state. All changes made to the desktop, program files, user settings files, or important Windows system files are permanently stored on the drive or disk. In the unfortunate event of a malicious network attack or virus, your files may be harmed in the process if Persistence is left on. When the FBWF filter is enabled and files can be protected, all changes made, including accidental virus entries, are wiped upon reboot.

Installing Additional Software

You may install third party licensed software as long as there is adequate space on the flash media.

To install additional software applications:

- 1 Log-in as an Administrator. Click **Start->type “Echo Control Panel” in search bar->FBWF**.
- 2 Temporarily disable the write filter by clicking the **Disable Restrictions**, and press the **Apply** button.



- 3 Reboot the terminal.
- 4 Log-in again as Administrator and install the new software.
- 5 After installation, verify the application is working as expected.
- 6 Launch the FBWF Manager and click the **Enable FBWF**. Also, make sure to re-enable the **Basic Exclusions**. For default exclusions, this would mean selecting the buttons for **Enabled Documents and Settings for Everyone** and the **Enabled Persistent Registry**.

- 7 Click **Apply** and Reboot the terminal one last time.

Installing MUI Packs

You may install MUI (Multilingual User Interface) packs to enable the operating system to support different languages and language settings on your terminal as needed. The MUI pack installation file may not be located on the disk, it must be installed from an external drive or over the network due to disk size limitations.



NOTE: Installing a MUI pack will reboot the system, so be sure to save and close all programs before starting the process to avoid losing your work.

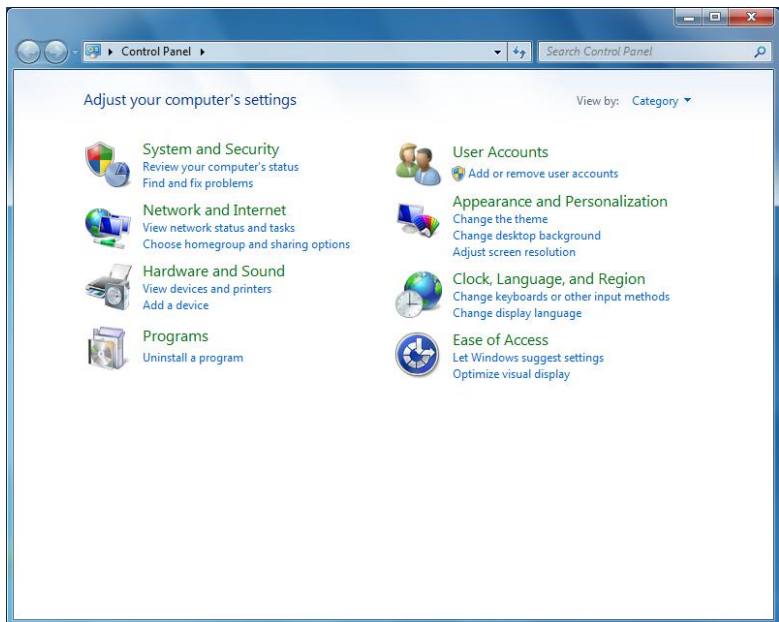
To install a MUI pack:

1. Log-in as an Administrator. Click **Start->All Programs-> Echo Control Panel**.
2. Temporarily disable the write filter by clicking the **Disable FBWF** button, and press the **Apply** button.
3. Reboot the terminal.
4. Log back in as an Administrator.
5. Launch the MUI installer for the desired language.
6. Click on **Run** in the security warning screen.
7. A command shell window will open noting the files being copied. Be sure to leave it open.
8. A dialog box will open and keep track of the files as they are installed.
9. Once the installation is completed, the system will reboot. Make sure to let the system reboot itself without interruption or the installation process may be unsuccessful.

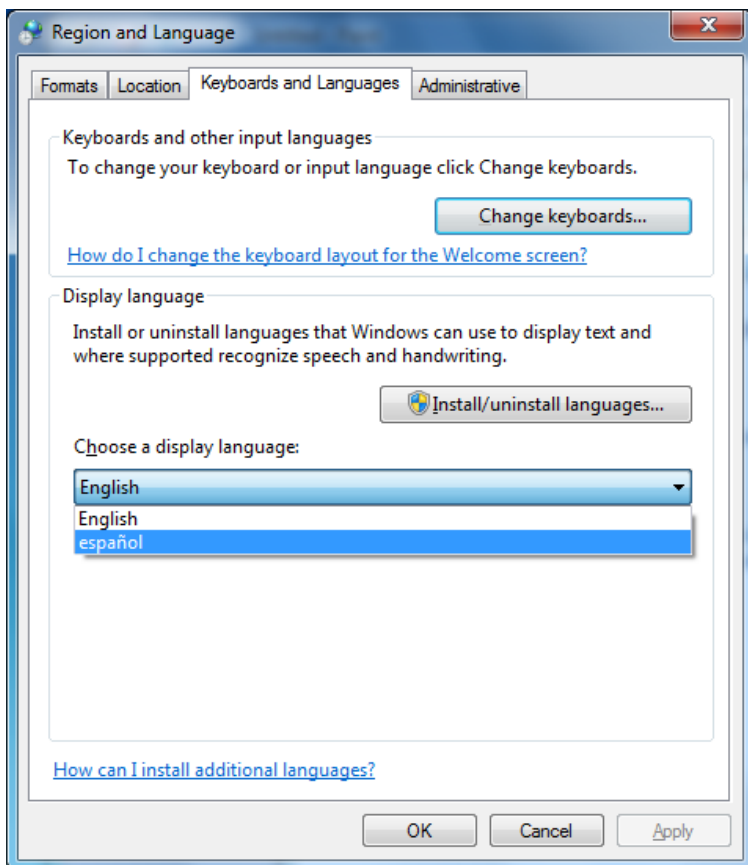
Setting a Language

To change your display language in WES 7

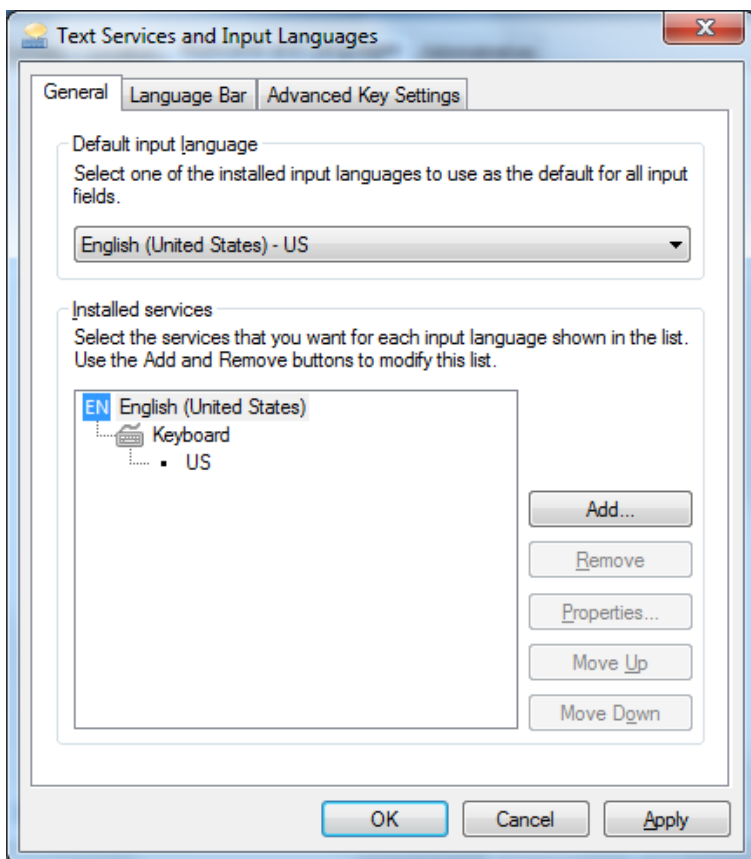
1. Launch your Control Panel and, under **Clock, Language, and Region**, Choose **Change display language**



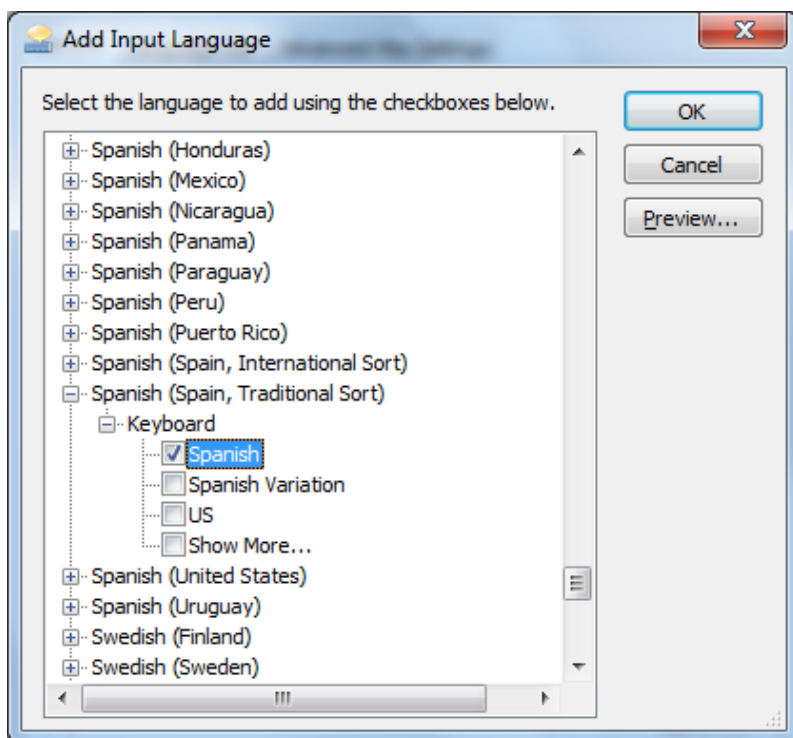
2. In the **Keyboards and Languages** tab, choose your display language from the drop-down menu. We will use Spanish for our demonstration.



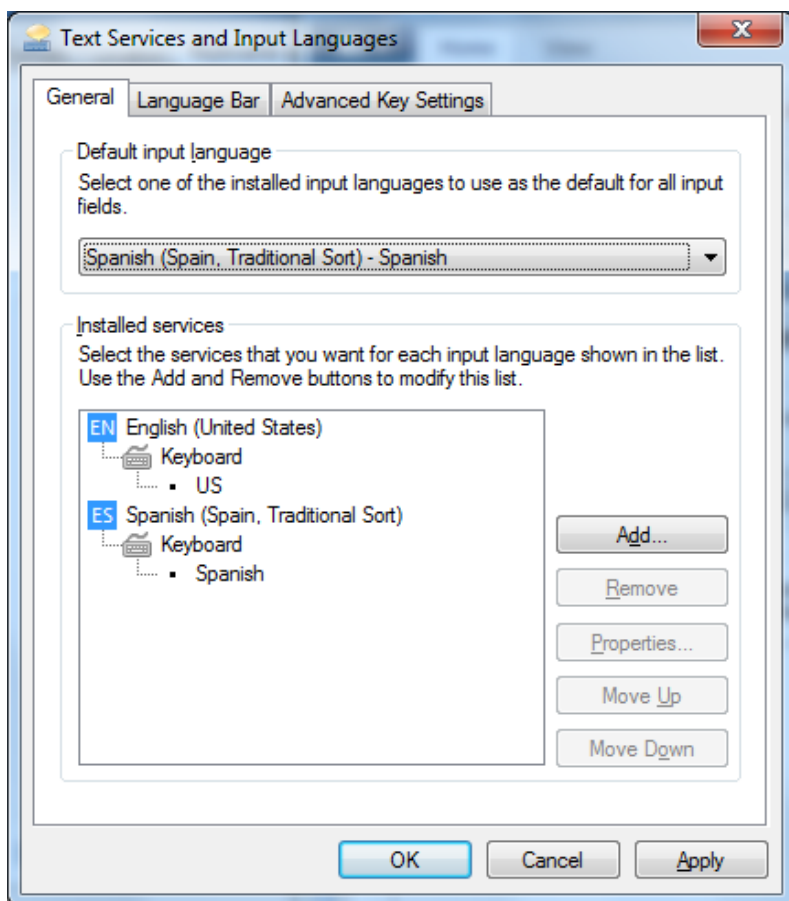
3. Next, click the **Change keyboards...** button. Here, we can add a new keyboard/IME configuration. Click the **Add...** button.



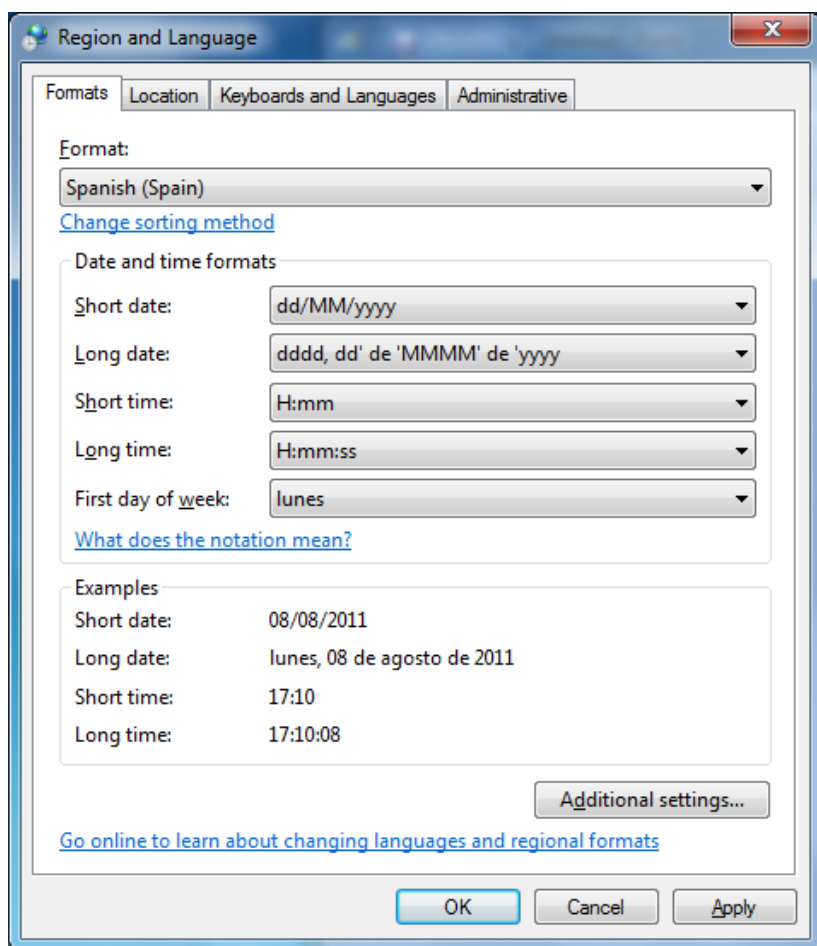
4. Choose your language and keyboard setting here. Some languages have multiple different keyboard layouts. The first selection is usually the desired selection, but you can add as many as you want. After making your selection(s), click **OK**.



5. Your new keyboard layout should appear in the Installed services section. To make it your new default setting, select it from the drop-down menu above.

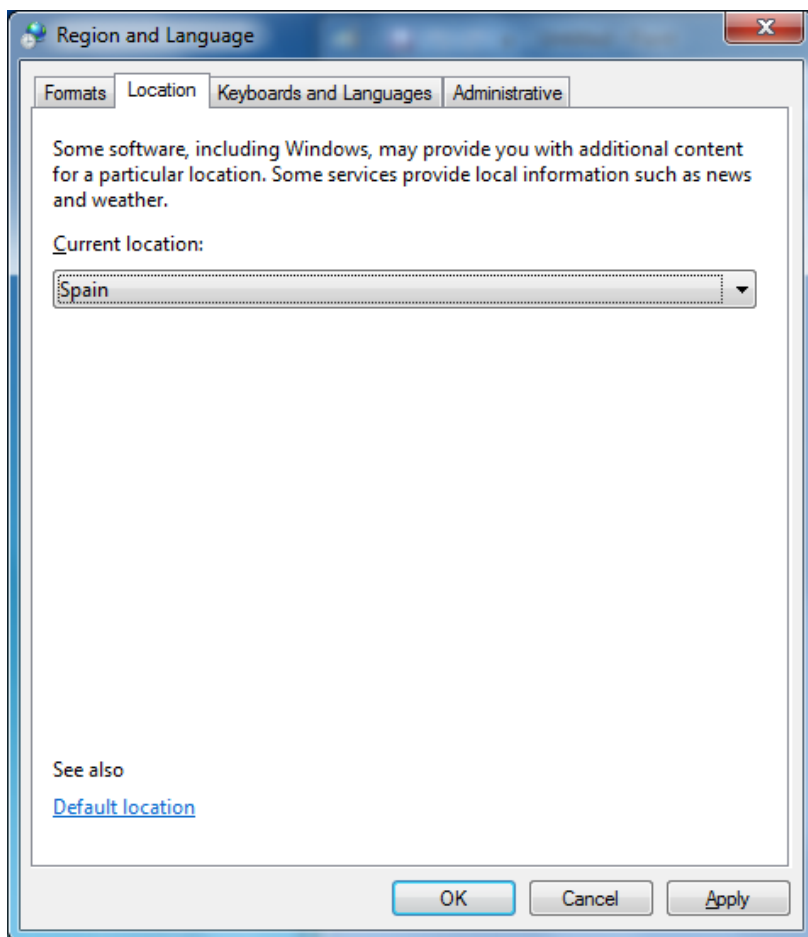


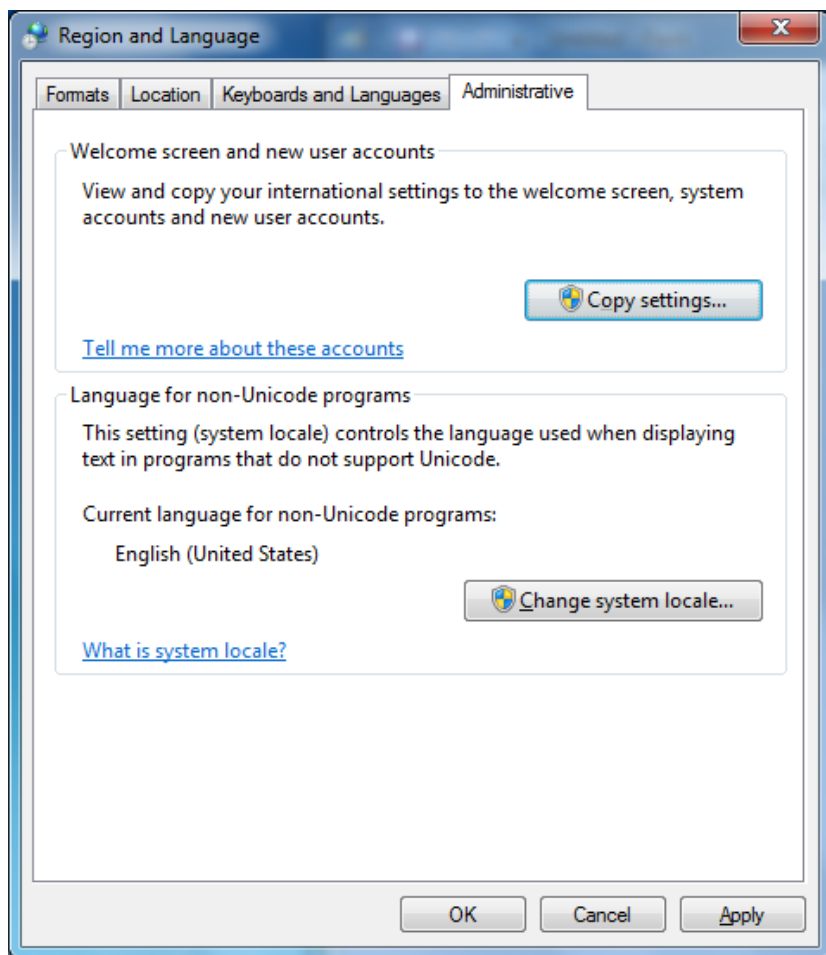
6. In the **Formats** tab, choose your language/country from the drop-down menu.



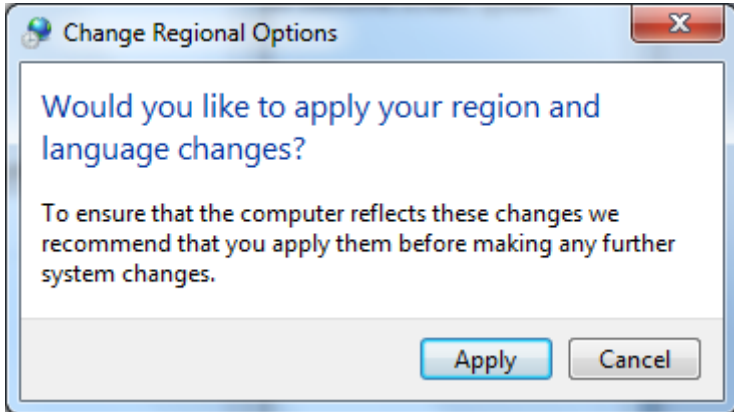
7. In the **Location** tab, select the country/location you are in.

- 8 In the Administrative tab, click the Change system locale... button.

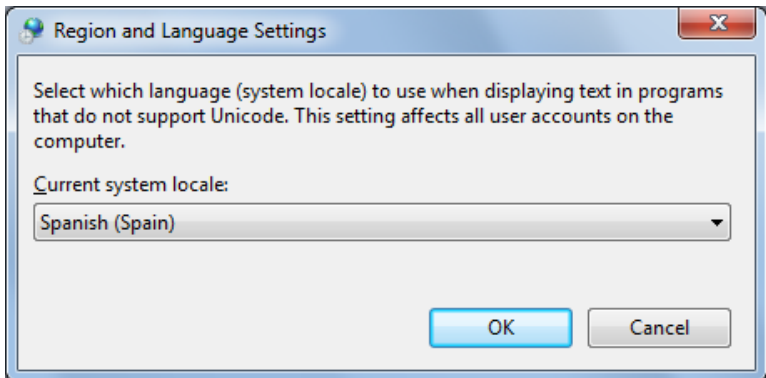




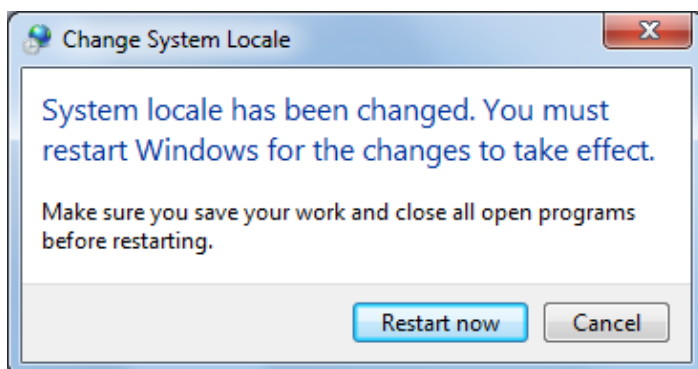
8. Windows will ask you if you would like to apply your region and language settings. Click **Apply**.



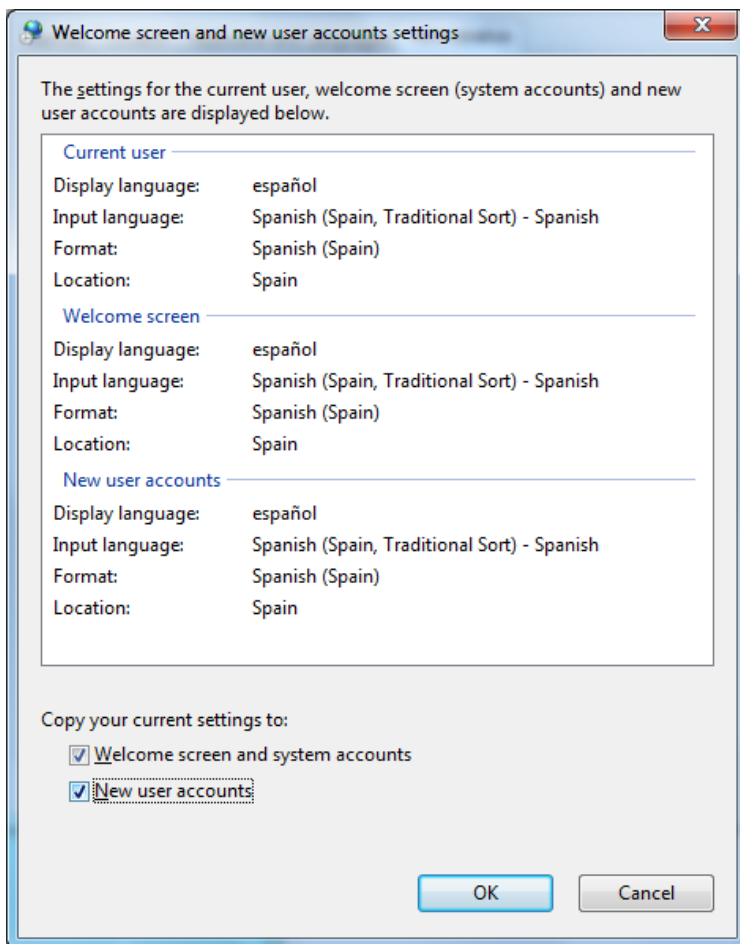
9. In the drop-down menu, choose the language/country that you are in and click **OK**.



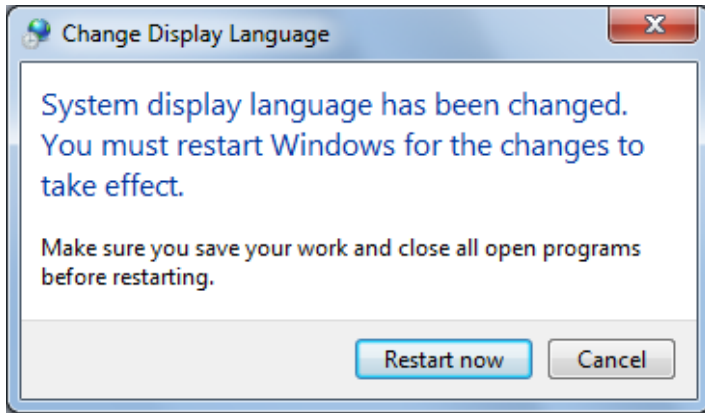
10. When Windows asks you to restart, click **Cancel**.



11. Returning to the **Administrative** tab, click the **Copy Settings** button. Select both check boxes to ensure that all accounts, including the system account, are set to your desired language/input configuration. Click **OK**.



12. Again, Windows will ask if you would like to restart. Click **Restart now**. When the machine reboots, your machine will be configured to your language/location/keyboard style of choice.



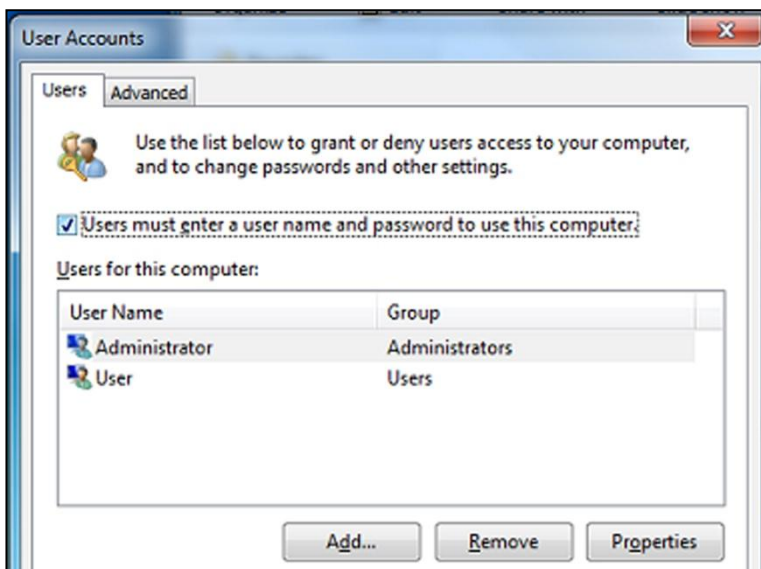
Using Your Thin Client

Customizing Your Thin Client

This section details how to change some of the options on your thin client to fit the needs of your business or your home.

Disabling the Automatic Log-In

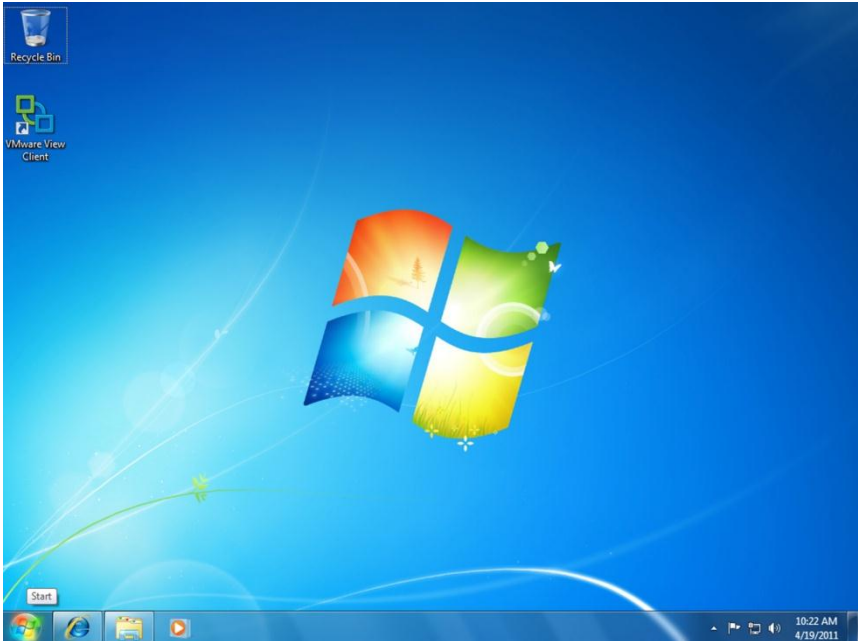
- 1 Holding down the **Windows** button, press **<R>** to access the Run: dialogue box.



- 2 Check the box that says **Users must enter a user name and password to use this computer**. Select **Administrator account** and then click **Apply** to save all changes.

After the initial boot up, or when booting up after using the re-imaging utility, your thin client will display the Windows Embedded Standard desktop, taskbar, and system tray.

The *desktop* should resemble that of a physical desktop, with pencils, folders, agendas, clocks, and calendars. The user can add icons to the desktop that provide shortcuts to frequently used notes, programs, files, or folders and avoid having to search for items on their drive.



The *taskbar* is the focus point of the Windows operating systems since Windows 95. It is the bar located at the very bottom of the desktop, and it houses the **Start** button, system tray, and the current time. The taskbar also shows all of the currently running programs. If the user is running Internet Explorer, Microsoft Word, and the **Control Panel**, there would be at least three shortcuts in the taskbar representing the three programs running. If the user clicks a shortcut, the selected program becomes the active program and shows up in front of all other programs. If the user minimizes a program, the program minimizes into the task bar, in the corresponding window tab.

The system tray, or *systray*, is located to the right of the taskbar; it is a collection of icons opposite of the Start button. Some default icons include the clock and volume control, but other programs may put their own icon and shortcut in the system tray after they are installed. Double-clicking an icon in the systray allows quick and easy access to programs or control settings.

Thin Client Options

Connections-Your terminal has the ability to connect to remote servers utilizing several types of protocols. The Remote Desktop client uses the RDP protocol and allows you to connect to Microsoft Windows Terminal Servers. The Citrix ICA client is used to establish connections to the Citrix Xen servers via the Citrix Online Plug-in. The VMware View client allows you to connect to a VMware View server, which in turn, provides the end-user with their own virtual desktop session. Lastly, you may connect with Internet Explorer to surf the web. This can be used for several purposes:

- Connect to web applications; e.g., a webmail server.
- Connect to a connection broker web interface; e.g., Citrix Online Plug-in.

System Settings-These are the display, sound, keyboard, mouse, printer and date/time configurations for your terminal. Also in the **Control Panel** section you have the ability to set a password for the thin client and change the local disk settings.

Echo Agent System Information

Echo Management-This displays the current status and information of the Echo Management server that your terminal is connected to.

- **Management Status** displays when the terminal is being managed by an Echo server.
- **Management Server** displays the current address of the Echo server.
- **Change Management Server** allows you to change the Echo server.
- **UUID** displays the current UUID assigned to the terminal.

Network Information-This displays information about the current network connection.

- **IP Address** displays the current IP address assigned to the terminal.
- **MAC Address** displays the current MAC address assigned to the terminal.
- **Hostname** displays the name assigned to the terminal.
- **Network Tools** allows you to run diagnostics test with the network connection and to check on the current status of the network connection.

The screenshot shows a window titled "System Information" with three main sections: Management, Network Information, and System Information. The Management section includes fields for Management Status (UnManaged), Management Server (ws-broker), and a UUID (03000200-0400-0500-0006-000700080009), along with a "Change Management Server" button. The Network Information section includes fields for IP Address (<no ip address>), MAC Address, and Hostname (WINDOWS-ARG8T2B), along with a "Network Tools" button. The System Information section includes fields for Operating System (WES7 (2012-12-12)), Processor (AMD G-T 56N Processor), Memory (1.61807 GB), DOM Size (7,46122 GB), and Hardware Model (Veriton N2110G). A "Close" button is located at the bottom right.

Management	
Management Status	UnManaged
Management Server	ws-broker
<button>Change Management Server</button>	
UUID	03000200-0400-0500-0006-000700080009

Network Information	
IP Address	<no ip address>
MAC Address	
Hostname	WINDOWS-ARG8T2B
<button>Network Tools</button>	

System Information	
Operating System	WES7 (2012-12-12)
Processor	AMD G-T 56N Processor
Memory	1.61807 GB
DOM Size	7,46122 GB
Hardware Model	Veriton N2110G

System Information-This displays information about the operating system, as well as information regarding the terminal.

- **Operating System** displays the name of the image or operating system that is in use.
- **Processor** displays the processor that the terminal is using.
- **Memory** displays the total internal memory of the thin client.

- **DOM Size** displays the total storage capacity size of the terminal.
- **Hardware Model** displays the name of the terminal in use.

4

Installing or Removing Peripherals

This section describes the correct way to install add-on hardware or software. Always make sure that the terminal is logged into the Administrator account and that the FBWF is disabled.

Installing a Printer



NOTE: The Administrator account is the only account that can disable or enable the File-Based Write Filter (FBWF). It is important to disable it before you install third party software, and re-enable it when the installation is complete.

- 1 If the printer is a Plug and Play printer that connects with a USB, there is no need for installation of any sort. Simply plug in the printer to the terminal using the USB and follow the on screen instructions. If the printer does not automatically install itself you will have to manually install the drivers.
- 2 You can insert a USB flash drive or a CD on an external drive that contains the printers' drivers into the terminal. If you do not have drivers available on a media device, search the manufacturer's website and download the correct driver that is compatible with your printer model and the operating system.
- 3 Select **Start->Control Panel->Devices and Printers**.



NOTE: If you are unable to find **Printers and Faxes** in the **Control Panel**, click **View by Small Icons** on the top right.

- 4 Select **Add a printer**. The wizard will begin. Decide if the printer will be local or a network printer. Depending on the printer, you may have to deselect the Plug and Play check box to continue.
- 5 Pick the connection type or port name and click **Next**. The printer should be listed in the box. Click the printer and then click **Have Disk**. Browse through your terminal and select the correct driver for your printer. After it is highlighted, click **OK** to install the driver.



NOTE: When you install drivers for any hardware connected to your thin client, make sure you use the correct and most recent drivers. Older drivers may not be compatible with the software.

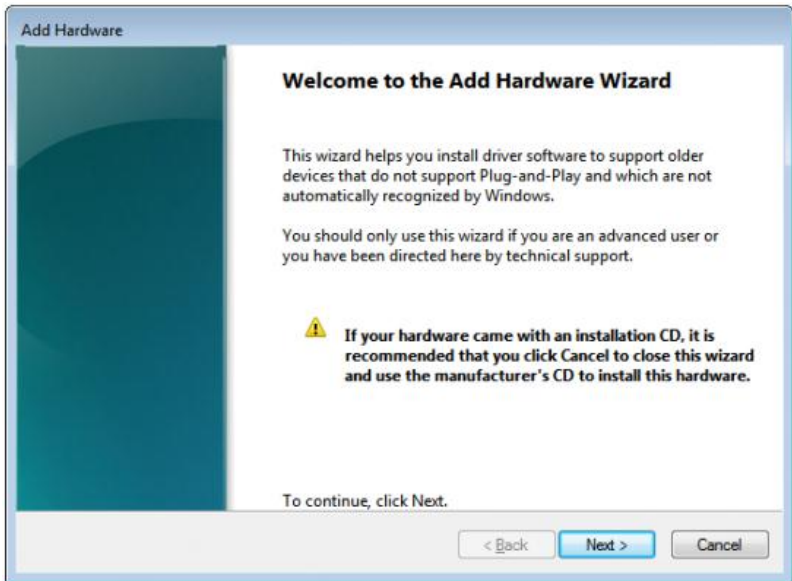
Installing a Scanner or Camera

- 1 Power the scanner or camera on and plug the USB cord into the photo device and into the terminal. Depending on the model, your device may install automatically.
- 2 If the device is not Plug and Play ready, you may have to install the drivers manually. You can insert a USB flash drive or a CD on an external drive that contains the device's drivers into the terminal. If you do not have the drivers available on a media device, search the manufacturer's website and download the correct driver that is compatible with your scanner or camera model and the operating system.
- 3 Connect your scanner or camera to the terminal using a USB cord. Your operating system should recognize the new hardware. If not, select **Start->Control Panel->Devices and Printers**. A wizard will guide you through the installation process.



NOTE: If the device comes with its installation files on a CD, there are ways you can install them onto your terminal. The easiest way is to use a Plug and Play CD-ROM. Another way is to use a second thin client and copy the entire installation folder from the CD onto a USB storage device. You can then use this USB device in the terminal. Also, you can search the manufacturer's website for the correct drivers for your device.

- 4 During the installation process, you are prompted to find the driver file for the device. Click **Browse** and locate the driver file from Step 2. Once the installation is complete, your thin client will recognize the device.



- 5 Click the **Finish** button to exit the **New Hardware Wizard** and complete installation. A restart may be required.

Installing a CD-ROM

Inserting a Plug and Play CD-ROM into your Acer thin client is the easiest way to utilize software and driver installation disks; however, not every external USB CD-ROM is Plug and Play compatible. If your device does not automatically recognize your CD-ROM upon insertion, follow the procedure below:

- 1 If the drivers are not currently available on a separate flash drive or media storage device, search the manufacturer's website and download the correct drivers that are compatible with both the CD-ROM model and the operating system that are being used onto the separate device. You may also access a second system with a functional CD-ROM, and copy the installation CD's driver files into a portable storage or flash device. Once the files are downloaded or copied, plug the storage or flash device into the thin client.
- 2 Select **Start->Control Panel**. Under **Hardware and Sound**, select **Add a device**. A wizard will appear to guide you through the installation process.
- 3 At some point, the wizard will ask you to select the specific driver file for your CD-ROM. Click **Browse** to locate the directory that stores the driver files from the manufacturer.
- 4 Highlight the correct driver file and install it. Your terminal should now recognize your CD-ROM. You may have to reboot your terminal for the changes to be made.



NOTE: Sometimes when installing some peripherals or certain software, you may be prompted to install files from the Windows Install CD. If you do not have a CD or an external CD-ROM handy, try browsing the **i386** folder. The **i386** folder is located at **C:\Windows\Driver Cache\i386**. This folder holds the important files that can install, modify, update, or repair Windows. It is recommended you do not delete these files or modify them in any way.

Uninstalling Software

To uninstall any software from the terminal, use the following procedure:

- 1 Access the **Uninstall or change a program** window by selecting **Start->Control Panel**.
- 2 Under **Programs**, select the **Uninstall a program** option. This will show an inventory of programs installed on your terminal.
- 3 Highlight the program you would like to uninstall and then click the **Uninstall** option to start uninstalling.
- 4 After you confirm the uninstall process of the software, a progress bar will appear showing the status of the update. After the bar reaches completion, the program should be removed from your terminal.

Uninstalling or Updating a Media Device

To uninstall or upgrade any device drivers from the terminal, use the following procedure:

- 1 To uninstall devices, access the **Add or Remove Devices** window by using the following path. Select **Start->Control Panel**.
- 2 Under **Hardware and Sound**, select **View devices and printers** to list all devices connected to the terminal. To uninstall, highlight the device and click **Remove device** at the top context menu.
- 3 Another way to uninstall devices or update your device to the latest driver is by selecting **Start->Control Panel->System and Security**. Then click **Device Manager** located under **System**. The **Device Manager** will have list all of the hardware and media devices recognized by the thin client. Clicking the plus [+] sign will drilldown each category and list specific devices related to that topic.
- 4 After drilling down and finding the device you want to uninstall or upgrade, right click it to open a context menu that will allow you to Uninstall, Update Driver, or Scan for any new hardware changes.

Freeing Local Drive Space

Sometimes you will want to free up some space on your local drive to make room for other software, applications, or programs. You can free up space by uninstalling some of the programs that you rarely use, and/or use Disk Cleanup.

Uninstalling Programs

Much like uninstalling media devices, you can uninstall programs to free up local drive space.

- 1 Access the **Uninstall or change a program** window by using the following path. Select **Start -> Control Panel**.
- 2 Under **Programs**, select the **Uninstall a program** option. This will show an inventory of programs installed on your terminal.
- 3 Highlight the program you would like to uninstall and then click the **Uninstall** option to start uninstalling.
- 4 After you confirm the uninstall process of the software, a progress bar will appear showing the status of the update. After the bar reaches completion, the program should be removed from your terminal.

Using Disk Cleanup

Disk Cleanup is a utility that finds temporary files, old compressed files, or other non important files and sorts them into those categories, allowing you to decide which categories to delete and which to keep. To use Disk Cleanup:

- 1 Select **Start->All Programs->Accessories->System Tools->Disk Cleanup**.
- 2 By default, your terminal should be the **C:** drive. Select your terminal's drive and click **OK**.
- 3 Disk Cleanup may take a few minutes to gather your temporary or disposable files.
- 4 Click the all check boxes of the files you wish to delete. Click **OK** when finished. Confirm the selection by clicking either **OK** or **Delete Files**.

Networking

Setting Static/Dynamic IP

By default, your thin client has its IP assigned automatically by DHCP, making it dynamic. If you want your IP to be a static number on your network, follow these steps:

- 1 Select **Start->Control Panel**. Under **Network and Internet**, select **View network status and tasks**
- 2 Click your connection. This will be called **Local Area Connection** if using an Ethernet card. The **Local Area Connection Status** window will appear. Click **Properties**.
- 3 A **Local Area Connection Properties** window should appear. Scroll to the bottom of the dialogue box with the down arrow and highlight the **Internet Protocol Version 4(TCP/IPv4)** option.
- 4 Once the **(TCP/IPv4)** option is highlighted, click **Properties** again. This will bring up your IP properties window.
- 5 Choose **Use the following IP address**: Complete the information boxes with your desired static IP, subnet mask, default gateway, and DNS server(s).
- 6 Click **OK** when all fields are entered correctly. Closing the menus will reconfigure your IP address immediately.



NOTE: Some problems can occur if you attempt to change your IP addresses to an IP address already in use. Ping the IP to make sure it is not in use before changing it. Ask your network administrator for the subnet mask, default gateway, and DNS servers if you are unsure.

Naming Your Thin Client, Joining a Domain or Workgroup

Naming Your Thin Client

- 1 To access an Active Directory Domain, you should rename your thin client. Begin by selecting **Start->Control Panel->System and Security -> System**. To continue, select the **Advanced system settings** on the left-hand sidebar.
- 2 Click the **Computer Name** tab then click the **Change** button at the bottom to enter the desired name.
- 3 Type in a name that will identify your terminal on the network neighborhood. If you rename a terminal while it is not connected to the network, duplicate names could occur. Always check with your network administrator before renaming a terminal.
- 4 After naming your terminal, click the **OK** button to confirm your rename. In most cases, your terminal will require a reboot.

Joining a Domain or Workgroup

- 1 Select **Start->Control Panel->System and Security -> System**. To continue, select the **Advanced system settings** on the left-hand sidebar.
- 2 Click the **Computer Name** tab and then click the **Change** button to bring up the **Computer Name/Domain Changes** window.
- 3 Enter the domain or workgroup name you want to join and click the **OK** button. You will receive notification if you have, or have not, successfully joined the specified domain or workgroup.
- 4 Reboot your terminal to apply the changes you have made.

Using the Join a Domain or Workgroup Wizard

The Join a Domain or Workgroup Wizard may also be used to join a domain or workgroup. It presents a series of questions and information boxes about your network and configures the system accordingly.

- 1 Select **Start->Control Panel->System and Security -> System**.
- 2 Under the **Computer name, domain, and workgroup settings** category, click **Change settings**.
- 3 On the **Computer Name** tab, click the **Network ID...** button. The Join a Domain or Workgroup Wizard will appear.
- 4 Answer the questions to configure your Domain or Workgroup. Click **Finish** and reboot your terminal to apply the changes you have made.

Using Connections

This section describes how to configure your WES7-based terminal to connect to server-based services utilizing several different connection protocols.

Using Remote Desktop

Remote Desktop Protocol (RDP) is a secure communication method based on Microsoft Terminal Services. It provides connection to Windows-based machines and is efficient enough to run on high-latency networks.

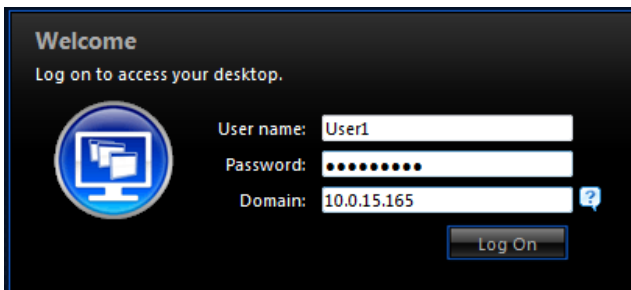
- 1 To open Remote Desktop and launch an RDP session, you can usually double-click the icon on your desktop called **Remote Desktop Connection**. If your desktop does not have an RDP icon, you can also use the following path: **Start->All Programs>Accessories>Remote Desktop Connection**.
- 2 In the **Computer** box, type in the IP address of your RDP server, and your user name. If your user name requires a domain you can type your name in the format DOMAIN\username.
- 3 Clicking the **Options** arrow at the bottom of the RDP window will allow you to set custom options available for your RDP session. Resolution, color options, printer and USB device redirection, and several other performance options are available from the drop down menu in various tabs.
- 4 After typing in your credentials, click **Connect** at the bottom of the menu. It may ask you to confirm your connection, and once you type in your password and hit Enter you will launch your RDP session.

Using Citrix ICA

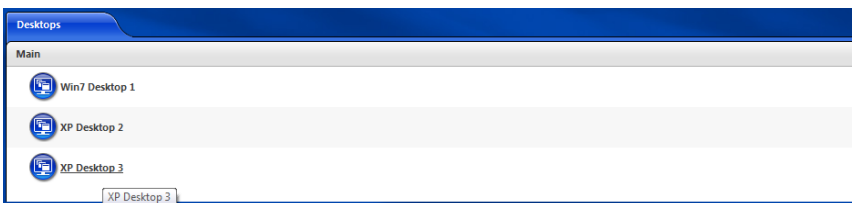
Citrix is one of the leaders in infrastructure solutions. It specializes in network access, VPN capabilities, remote control, and remote support applications. Citrix solutions, like the Citrix Online Plug-in, utilize the Citrix ICA protocol. ICA (Independent Computing Architecture) allows non-Windows systems (Macintosh, X terminals, UNIX workstations, etc.) to access Windows-based applications.

Using the Citrix Online Plug-in

- 1 To launch the Citrix Online Plug-in, open Internet Explorer and enter the IP address of your Xen Server in the address bar.
- 2 Enter in the Username, Password, and Domain

A screenshot of the Citrix Welcome login screen. It has a dark blue background. At the top, it says "Welcome" in white, followed by "Log on to access your desktop." in a smaller font. On the left is a circular icon with a computer monitor and a document. To the right of the icon are three input fields: "User name:" with "User1" entered, "Password:" with masked dots, and "Domain:" with "10.0.15.165" entered. A small blue question mark icon is to the right of the domain field. At the bottom right is a "Log On" button.

- 3 Left-click the desktop you wish to use to complete the process.






NOTE: If this is your first time loading the Citrix Online Plug-in, you will be taken to a screen that asks you to **Click Download to Access Your Desktop**. Along the right-hand side of the page, click on **Already Installed** to be taken to step 3.

Click Download to Access Your Desktop
☐ By selecting the check box, you confirm that you have read, understand, and accept the [Citrix license agreement](#).

↓ Download

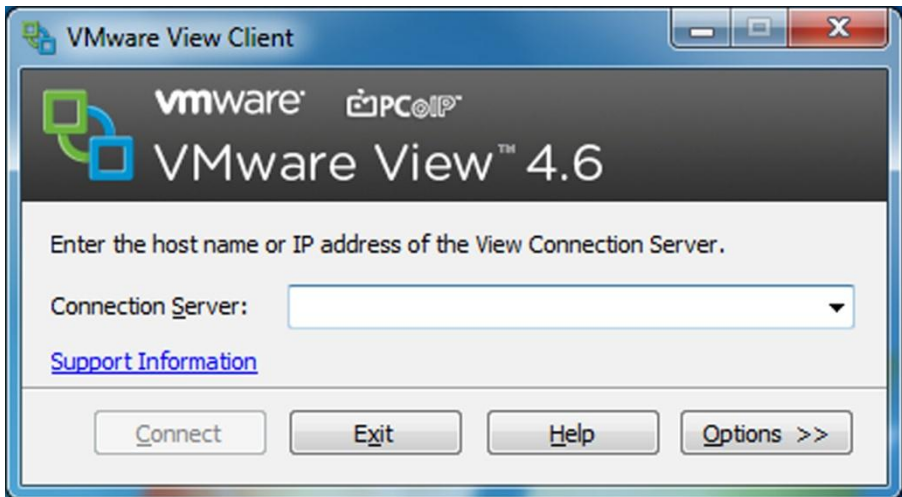
 Clicking **Download** will install software on your computer. [More information on security...](#)

Other Options
Already installed
Try later
Log off

Using VMware View

VMware View utilizes VMware's hypervisor technology to efficiently provide multiple instances of an operating system to remote users using the RDP or PCoIP (PC-over-IP) protocol.

- 1 To connect to a VMware View server, double-click the icon on your desktop called **VMware View Client**. Another way is using the path: **Start->All Programs->VMware->VMware View Client**.
- 2 In the bar that says **Connection Server**, type the IP address of your VMware server and click **Connect**.
- 3 Click the **Options** button at the bottom right to configure more advanced options like auto-connections or specifying which ports to use. After you are finished, hit the **Connect** button to access



the log-in screen.

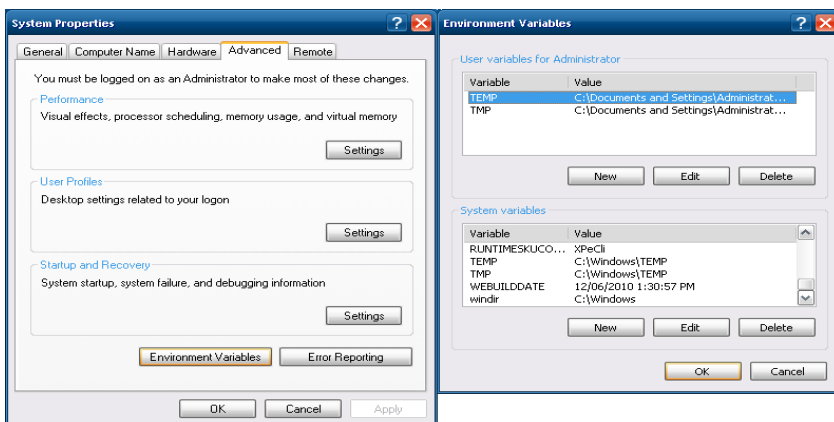
- 4 Type your User name and Password and select a Domain. After clicking on **Login**, it may require you to select a **Desktop** before opening the session.
- 5 Highlight the **Desktop** you want to use and then select **Connect** to complete the process.

OS Build Date, Echo Agent, and Re-Imaging

Verifying OS Build Date

To verify the OS Build Date, power-on and boot-up the thin client.

- 1 After the boot process has been completed log-in to the Administrator account.
- 2 Use to path: **Start -> Control Panel -> System and Security -> System**. Select the **Advanced system settings** on the left sidebar.

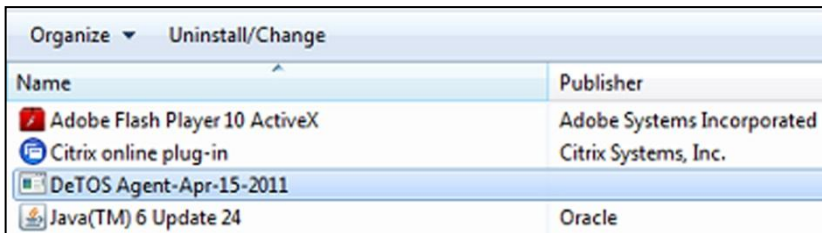


- 3 Under the Advanced tab, select **Environment Variables**.
- 4 Scroll down to the bottom of the window. The build date will be listed as: (example) **WEBBUILDDATE 04/15/2011 1:30:57PM**.

Verifying the Echo Agent Version and Status

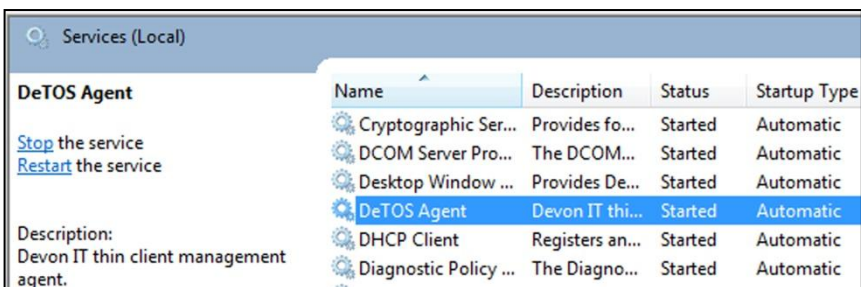
To verify the Echo Agent version and status, power-on and boot-up the thin client.

- 1 After the boot process has been completed log-in to the Administrator account.
- 2 Select **Start->Control Panel->**. Under **Programs**, select **Uninstall a program**.



Organize ▾ Uninstall/Change	
Name	Publisher
Adobe Flash Player 10 ActiveX	Adobe Systems Incorporated
Citrix online plug-in	Citrix Systems, Inc.
DeTOS Agent-Apr-15-2011	
Java(TM) 6 Update 24	Oracle

- 3 The Echo agent will be the installed program labeled **DeTOS Agent-month-date-year** as shown above.
- 4 To verify the status of the Echo Agent, use the path: **Start -> Control Panel -> System and Security -> Administrative Tools**. Finally, double-click **Services**.
- 5 Scroll down to the DeTOS Agent Service. The DeTOS Agent status must be **Started** and the startup type must be **Automatic** for the Echo Agent to be fully functional.



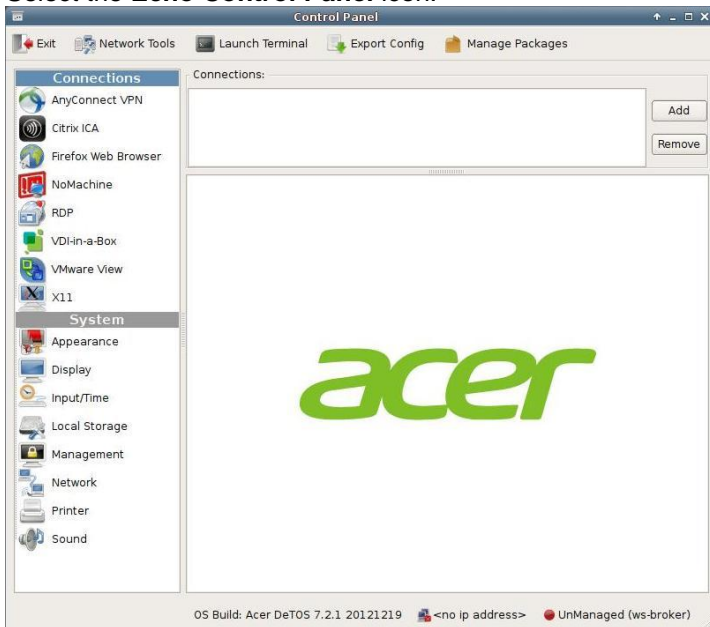
Re-Imaging the Thin client

For information about re-imaging your thin client, please consult the Re-Imaging guide.

Echo Control Panel

There is a control panel in WES that can be used to create new connections and customize them to suit your needs. This tool, the **Echo Control Panel**, can be opened by following these steps:

1. Open the **Start** menu and select **Control Panel** to open the Windows control panel.
2. Select **Large icons** from the **View by:** dropdown menu near the top of the window.
3. Select the **Echo Control Panel** icon.



The **Echo Control Panel** is the local tool for accessing your **Network Tools**, as well as configuring **Connection** settings on your thin client.

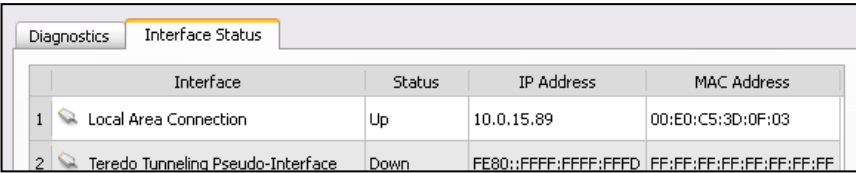
- **Connection Settings** - Your terminal has the ability to connect to remote servers utilizing several types of protocols. The rDesktop client uses the RDP protocol and allows you to connect to Microsoft Windows Terminal Servers. The Citrix ICA client is used to establish connections to Citrix Presentation and XenApp servers. The VMware View client allows you to connect to a VMware View server, which in turn, provides the end-user with their own virtual desktop session. Lastly, you may create an Internet Explorer web browser connection to surf the web. This can be used for several purposes:
 - Connect to a web applications; e.g., a webmail server.
 - Connect to a connection broker web interface; e.g., Citrix XenDesktop.
 - Use the thin client as a Kiosk (select the **Enable Kiosk Mode** button under the **Kiosk Mode** panel)

Network Tools

The toolbar along the top of the **Echo Control Panel** window contains a button named **Network Tools**. Clicking this button will open a separate, smaller window that provides you with current network status and useful diagnostic programs.

Interface Status

Click the **Interface Status** tab along the top of the **Network Tools** window to view the IP address that is currently assigned to this terminal. The MAC Address for this machine is also reported on this screen.

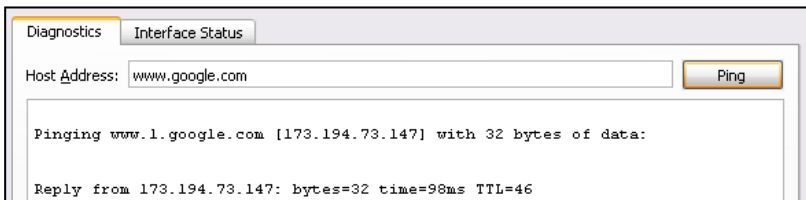


	Interface	Status	IP Address	MAC Address
1	Local Area Connection	Up	10.0.15.89	00:E0:C5:3D:0F:03
2	Teredo Tunneling Pseudo-Interface	Down	FE80::FFFF:FFFF:FFD	FF:FF:FF:FF:FF:FF

Diagnostics

If you are experiencing difficulty connecting to servers on certain segments of your LAN, then you may want to use the ping command to verify you are reaching specific servers and/or gateways on the subnet in question. To use ping:

1. Select the **Diagnostics** tab from the **Network Tools** window.
2. In the **Host Address** field, type in the IP address or website you want to test against and then press the **Ping** button.



3. If there is an error in the delivery to the destination, the ping command displays an error message. Otherwise, replies will continuously display for each packet successfully sent and received.
4. Press the **Stop** button to terminate the ping loop.

Connections

Adding New Connections

6. Open the **Echo Control Panel**.
7. Click the icon you wish to create; it is listed under the **Connections** bar, on the left-hand side of the **Echo Control Panel**.
8. The main window will split into two separate frames. The top frame will list all existing connections for this particular type or protocol. To add a new connection, click the plus [+] button.
9. You will be prompted to enter a name for this connection. Enter a name for this connection and press the **OK** button to continue.

- 10 The bottom frame will display configuration fields that are specific to the connection type you are creating. Some connections, like **Internet Explorer**, will only have a couple of fields required for configuration and be listed on a single form. Connections that have several configuration options associated with them, like RDP and Citrix, will have their settings grouped and sorted under separate sections, called form panels. These panels can be opened and closed by clicking the plus [+] and minus [-] buttons found along the top, right-hand side of each panel box.



NOTE: The number of form panels will vary, depending on the type of connection you are creating. Click the plus [+] or minus [-] buttons to expand and collapse these sections.

- 11 Once you are finished setting up your connection, click the **Apply** button along the bottom of the frame. An icon for the new session will be created on the desktop. The end user can double-click this icon to launch the connection.
- 12 As you create connections in the **Control Panel**, icons for those sessions will appear on the desktop. Double-click the icon to launch that session.

How to Rename or Delete Connections

It is possible to rename a connection on the desktop by right clicking it and selecting **Rename** from the context menu. However, if you do not do so within the **Echo Control Panel**, the name will revert back to the original if any changes are made to that connection through the **Echo Control Panel**. To rename a connection through the **Echo Control Panel**:

- 13 In the **Echo Control Panel**, the top center panel lists your currently added connections in the **Connections** window.
- 14 Select the session type to view the list of available connections, and then select the specific name of the connection you want to edit.
 - **To Rename**-Double-click the entry. Your pointer will change to a [I] cursor and highlight the connection name, allowing you to type

in a new name for this connection. Press <Enter> to save your changes.

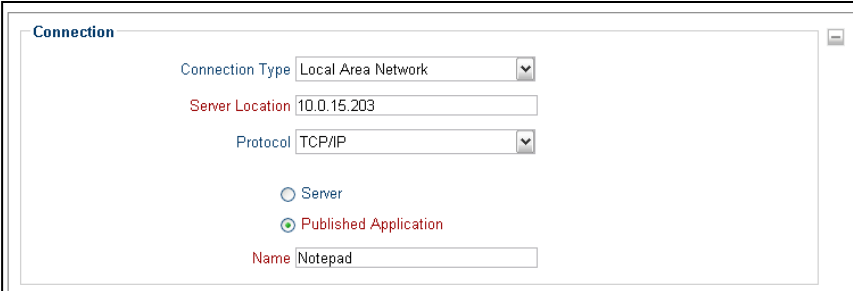
- **To Delete**—Press the **Remove** button to remove that connection. You will be asked to confirm the removal. Click **Apply** to remove that connection completely.

Citrix ICA

The Citrix Receiver client in WES allows you to connect to Citrix Xen Servers (formerly known as Presentation Server). This Citrix client also contains the necessary plug-in used for connecting to XenDesktop via the thin client's local web browser.

The Connection Section

The first section displayed for a Citrix ICA session is **Connection**. This form panel will already be expanded for you.

The screenshot shows a web form titled "Connection" in a blue header bar. The form contains several fields: "Connection Type" is a dropdown menu set to "Local Area Network"; "Server Location" is a text input field containing "10.0.15.203"; "Protocol" is a dropdown menu set to "TCP/IP"; there are two radio buttons, "Server" (unselected) and "Published Application" (selected); and "Name" is a text input field containing "Notepad". A small minus icon is visible in the top right corner of the form panel.

- **Server Location**—Type in the IP address or hostname of your Citrix server.

- **Protocol**-Select the appropriate protocol needed to connect to your Citrix Server.
- There are two methods for connecting to your Citrix Server:
 - **Server**-To connect to the desktop of your Citrix Server, click the radio button called **Server**.
 - **Published Application**-To connect to a published application on your Citrix Server, select the radio button called **Published Application**.
- **Name**-Enter your server name or published application name here.

The screenshot shows the 'Options' dialog box with the following settings:

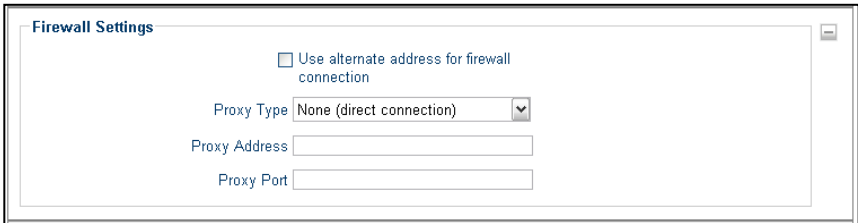
- Window Size: Fullscreen
- Window Colors: High Color (16 bit)
- Sound Quality: Medium
- Mouse Click Feedback: Auto
- Local Text Echo: Auto
- Encryption: Basic
- ☐ Autostart - Start this session upon device bootup
- ☐ Use data compression
- ☐ Use disk cache for bitmaps

The Options Section

- **Window Size**-Select the type of window you want your ICA session to display in.
 - Full screen-The ICA session will take up the entire display.
 - Fixed Size-You may select fixed sized windows, such as **640x480**, **800x600**, and **1024-x768**.
 - Percentage Based-You may select a size based on the percentage of available desktop display, such as **25%**, **50%**, and **75%**.

- **Seamless**-When using the **Published Application** feature, you can select Seamless mode to launch Windows applications like **Notepad** without using the Citrix Window.
- **Windows Colors**-Color depth options are 16 colors, 256 colors, 16-bit, and 24-bit.
- **Sound Quality**-Adjust the sound from Low, Medium, or High Quality.
- **Citrix SLR (Speed Screen Latency Reduction) Options**-Enabling the following two options are usually only needed when high latency is occurring or poor bandwidth conditions exist.
 - **Mouse Click Feedback**-The mouse cursor will change to an hourglass as soon as a user performs a mouse click on an event and will wait for a response from the server before it changes back.
 - **Local Text Echo**-This option allows a user to see the character they type into their session on the screen, without this key press hitting the actual server at that time.
- **Encryption**-Select the appropriate level of encryption to be used when connecting to this Citrix Server.
- **Autostart**-Enable this checkbox to automatically launch this session each time the thin client completes its boot procedure.
- **Auto Restart**-Select **Yes** or **Prompt** to automatically restart the connection.
 - **Yes**-Once the session is terminated, the session will automatically restart. There is no way for the end-user to stop it from occurring every time it closes.
 - **Prompt**-Once the session is terminated, the user will receive a **YES/NO** prompt asking them if they wish to reconnect to the session.
- **Use data compression**-In an environment where system and client resources are not a concern, data compression can be used to decrease the amount of data that must be sent across the network.
- **Use disk cache for bitmaps**-Allows graphical objects to be stored in the local disk cache on the client device.

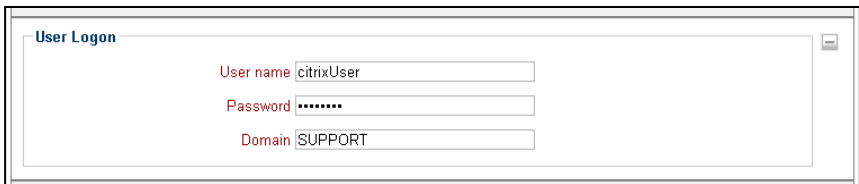
The Firewall Settings Section



The screenshot shows the 'Firewall Settings' window. It contains a checkbox labeled 'Use alternate address for firewall connection'. Below it is a 'Proxy Type' dropdown menu currently set to 'None (direct connection)'. Underneath the dropdown are two text input fields: 'Proxy Address' and 'Proxy Port'.

- **Use alternative address for firewall connection**-Mark this checkbox if you need the ICA session to connect to the Citrix server's external IP address. The *external* address for the server is specified as the *alternate* address.
- **Proxy Settings**-If your Citrix environment utilizes a proxy server, then choose the appropriate type from the **Proxy Type** field. Enter the address of the proxy server and port number in the **Proxy Address** and **Proxy Port** fields, respectively.

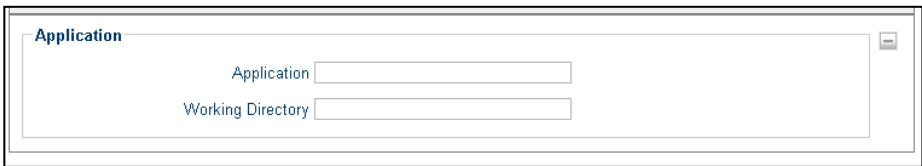
The User Log On Section



The screenshot shows the 'User Logon' window. It contains three text input fields with labels to their left: 'User name' with the value 'citrixUser', 'Password' with masked characters '*****', and 'Domain' with the value 'SUPPORT'.

- **User Name**-Specify the name of a user account to log on as. This is an optional field.
- **Password**- Enter the password associated with the user name, if entered.
- **Domain**-Specify the domain to log on to. This is an optional field.

The Application Section



The screenshot shows a configuration window titled "Application". It contains two text input fields: "Application" and "Working Directory". The "Application" field is currently empty, and the "Working Directory" field is also empty. There is a small icon in the top right corner of the window.

- **Application**-Specifies the path of the application on the Citrix server to be automatically launched when the connection is made. This is an optional field.
- **Working Directory**-Specifies the working directory used for the application.

Internet Explorer Browser

The following section describes the steps for configuring the local Internet Explorer web browser in WES.

The General Section



The screenshot shows a configuration window titled "General". It contains a "Start URL" field with the value "http://support.devonit.com/". Below this field are two checkboxes: "Enable Kiosk Mode" and "Autostart - Start this session upon device bootup". Both checkboxes are currently unchecked.

- **Start URL**-Specifies the initial web page to appear when the browser is first launched.
- **Enable Kiosk Mode**-If you want to run this Internet Explorer connection as a Kiosk, toggle this checkbox on.



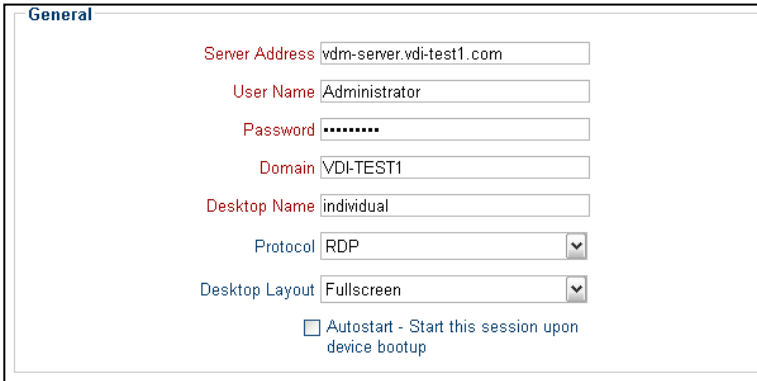
NOTE: To use Kiosk Mode correctly, make sure you have a Starting URL in the requested field. Launching Internet Explorer in Kiosk Mode will automatically launch a Full Screen, inescapable Internet Explorer session for end-users with Internet-ONLY access. The only way to leave the browser is to shut down the thin client.

- **Autostart**-Enable this checkbox to automatically launch this session after the thin client completes its boot procedure.
- **Auto Restart**-Select **Yes** or **Prompt** to automatically restart the connection.
 - **Yes**-Once the session is terminated, the session will automatically restart. There is no way for the user to stop it from occurring.
 - **Prompt**- Once the session is terminated, the user will receive a **YES/NO** prompt asking them if they wish to reconnect to the session.

Click the **Apply** button to save the connection. Double-click the Internet Explorer icon the desktop to launch the browser session. Browser plug-ins for Flash Player and Java have been pre-installed.

VMware View

The VMware View client allows you to connect to a VMware server, which in turn, provides the end-user with their own virtual desktop session. The following section describes the basic steps for configuring the View Client in WES.



The screenshot shows the 'General' tab of the VMware View client configuration window. It contains the following fields and options:

- Server Address:** vdm-server.vdi-test1.com
- User Name:** Administrator
- Password:** (masked with dots)
- Domain:** VDI-TEST1
- Desktop Name:** individual
- Protocol:** RDP (dropdown menu)
- Desktop Layout:** Fullscreen (dropdown menu)
- Autostart:** ☐ Autostart - Start this session upon device bootup

- **Server Address**-Enter the Hostname or IP address of your VMware View Broker.
- **Credentials**-Specify the User Name and Password of a user account you wish to log on as.
- **Domain**-Specifies the domain to log on to.
- **Desktop Name**-If the user of this thin client should always connect to the same desktop, then you may consider entering its name into this field. If you choose to leave the field empty, then the user will be prompted to select an available desktop at the time they connect to the VMware View server.
- **Protocol**: Choose whether to connect to your VMware View server using the RDP or PCOIP protocol.
- **Desktop Layout**: Choose the desktop option that best suits your display setup.
- **Autostart**:-Enable this checkbox to automatically launch this session after the thin client completes its boot procedure.

- **Auto Restart:** Select **Yes** or **Prompt** to automatically restart the connection.
 - **Yes**-Once the session is terminated, the session will automatically restart. There is no way for the user to stop it from occurring.
 - **Prompt**-Once the session is terminated; the user will receive a **YES/NO** prompt asking them if they wish to reconnect to the session.

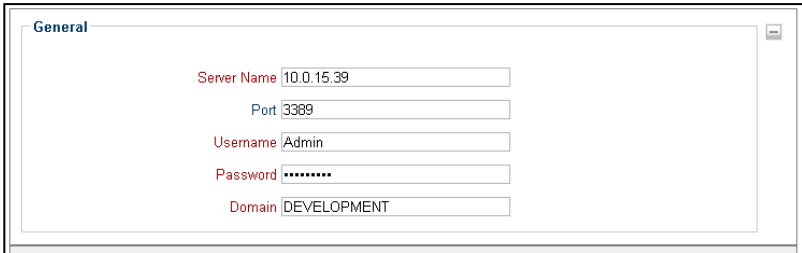
Troubleshooting Tips for VMView Connection

- If you set your session to full screen but the display covers only a fraction of the entire screen, then your allocated RAM for the virtual desktop may need to be set a little higher.
- If certain features like foreign keymaps, CD-ROM, USB stick, or printer redirection are not passing through to the virtual desktop session, check if your VM is at the correct version. You can download the latest agent software executables at VMware's website at: <http://www.vmware.com/downloads>.
- If you plan to use USB flash drives within your session, it is best to use sticks formatted in FAT or NTFS. Long delays sometimes occur when using flash drives formatted in FAT32. Other USB troubleshooting tips can be found at the following VMware site: <http://kb.vmware.com/kb/1026991>.

rDesktop

The General Section

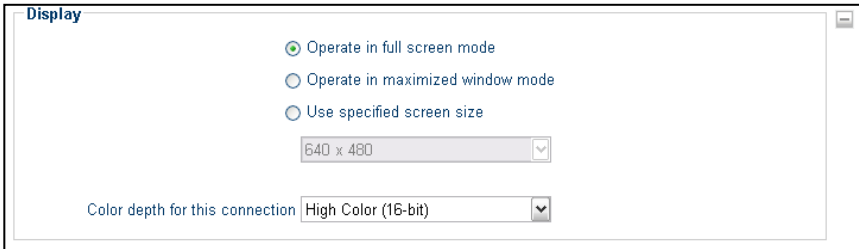
The first section displayed for an rDesktop session, is named General. This form panel will already be expanded for you.

A screenshot of the 'General' section of the rDesktop configuration window. The window has a title bar with the word 'General' and a close button. Inside, there are five labeled text input fields arranged vertically. The labels are in red: 'Server Name', 'Port', 'Username', 'Password', and 'Domain'. The values entered are: '10.0.15.39' for Server Name, '3389' for Port, 'Admin' for Username, '*****' for Password, and 'DEVELOPMENT' for Domain. Each field has a small cursor icon at the end of the text.

Server Name	10.0.15.39
Port	3389
Username	Admin
Password	*****
Domain	DEVELOPMENT

- **Server Name**-Enter the hostname or IP address of the Windows Terminal Server.
- **Port**- Enter the port number used in this connection.
- **User Name**-Specifies the name of a user account to log in as. This is optional.
- **Password**-Enter the password that coincides with the username given, if applicable.
- **Domain**-Specifies the domain to log on to.

The Display Section

The screenshot shows a window titled "Display" with a light gray background. It contains three radio button options: "Operate in full screen mode" (selected with a green dot), "Operate in maximized window mode", and "Use specified screen size". Below these is a dropdown menu showing "640 x 480". At the bottom, there is a label "Color depth for this connection" followed by a dropdown menu showing "High Color (16-bit)".

Display

☒ Operate in full screen mode

☐ Operate in maximized window mode

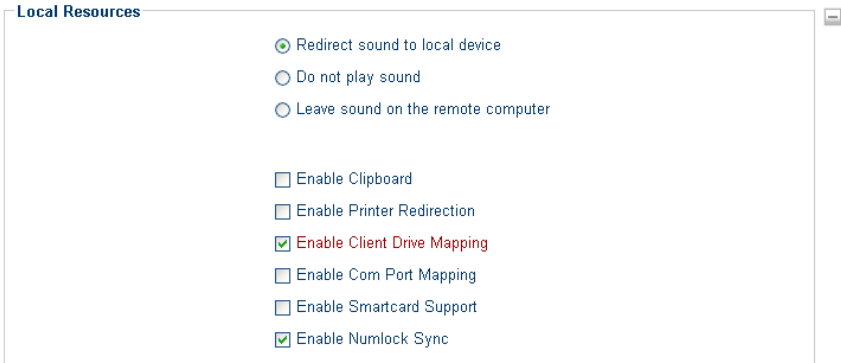
☐ Use specified screen size

640 x 480

Color depth for this connection High Color (16-bit)

- **Operate in full screen mode**-The rDesktop session will take up your entire display and will not allow minimization.
- **Operate in maximized window mode**-This option will display the rDesktop session in a window within WES. You will be able to maximize and minimize this window if you want.
- **Use specified screen size**-The session will launch in a fixed sized window, specified by the dimensions chosen in the dropdown list below. You can ONLY minimize this window, the fixed size is the MAX size allowed.
- **Color depth for this connection**-Select the desired color depth for this session.

The Local Resources Section



Local Resources

☒ Redirect sound to local device

☐ Do not play sound

☐ Leave sound on the remote computer

☐ Enable Clipboard

☐ Enable Printer Redirection

☒ **Enable Client Drive Mapping**

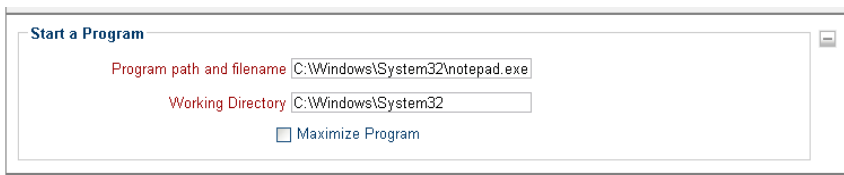
☐ Enable Com Port Mapping

☐ Enable Smartcard Support

☒ Enable Numlock Sync

- **Sound Redirection Options**-By default, sound from the server will redirect to the local thin client. If you do not want sound to be sent to the local device, then select either the **Do not play sound** or **Leave sound on the remote thin client** radio buttons below **Redirect sound to local device** (selected by default).
- **Enable Clipboard**-Determines the ability to copy things to the clipboard while using this session.
- **Enable Printer Redirection**-Mark this checkbox to redirect printing to a printer attached the local terminal.
- **Enable Client Drive Mapping**-Allows the user plug USB Flash Drives locally into the terminal and access the contents of the drive via the RDP session.
- **Enable Com Port Mapping**-Redirects serial devices on your terminal to the server.
- **Enable Smartcard Support**-Specifies whether redirection of Smart Cards is permitted during server authentication.

The Start a Program Section



Start a Program

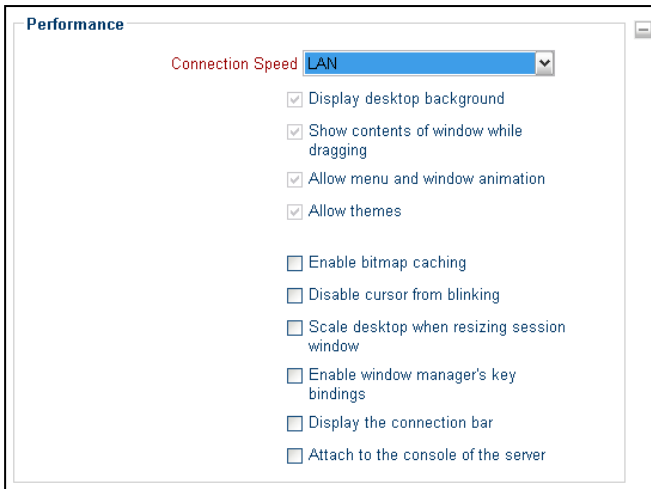
Program path and filename

Working Directory

☐ Maximize Program

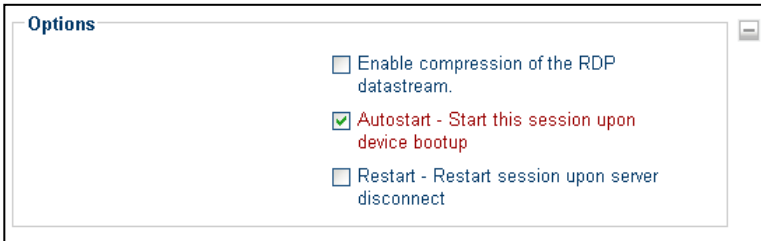
- **Program path and filename**-Specifies the path of the application on the Terminal server to be automatically launched when the connection is made. This will launch the application in a window within WES, not rDesktop.
- **Working Directory**-Specifies the working directory used for the application.

The Performance Section



- **Connection Speed**-Specifies the RDP Experience. As you change connection options in this dropdown box, associated behaviors in the checkboxes below will be selected or deselected accordingly.
- **Enable bitmap caching**-Enable caching of bitmaps to disk (persistent bitmap caching).
- **Disable cursor from blinking**-Indicates that *cursor blinking* should be disabled during the RDP session.
- **Enable window manager's key bindings**-By default rDesktop attempts to grab all keyboard input when it is in focus.
- **Attach to the console of the server**-The session will connect to the console of the server (requires Windows Server 2003 or newer).

The Options Section



- **Enable compression of the RDP DataStream**-In an environment where system and client resources are not capable, data compression can be used to decrease the amount of data that must be sent across the network.
- **Autostart**-Enable this checkbox to automatically launch this session after the thin client completes its boot procedure.
- **Auto Restart**-Select **Yes** or **Prompt** to automatically restart the connection.
 - **Yes**-Once the session is terminated, the session will automatically restart. There is no way for the user to stop it from occurring.
 - **Prompt**-Once the session is terminated, the user will receive a **YES/NO** prompt asking them if they wish to reconnect to the session.

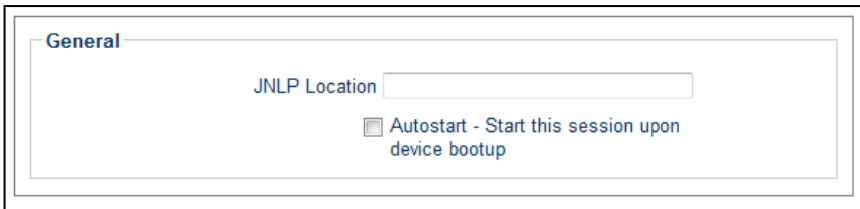
VDI In A Box

Your thin client running WES comes pre-configured with Java Web Start and Citrix that enables users to creation connections to Kaviza servers. Since the client does not reside natively on the thin client, you will need a web address that points to your **kavizaclient.jnlp** file.

The General Section

You will need the location of the JNLP (Java Network Launching Protocol) which resides on your remote Kaviza server.

- **JNLP Location**-Type in the appropriate location of the **kavizaclient.jnlp** file. The typical format will look something like the following: **http://10.0.15.79/dt/kavizaclient.jnlp**.



The screenshot shows a window titled "General" with a light blue header. Inside the window, there is a label "JNLP Location" followed by a text input field. Below this, there is a checkbox labeled "Autostart - Start this session upon device bootup". The checkbox is currently unchecked.

- **Autostart**-Enable this checkbox to automatically launch this session each time the thin client completes its boot procedure.

Getting Help

Getting the latest software and Echo Management software

Visit the website page through following

<http://us.acer.com/ac/en/US/content/drivers> or

<http://www.devonit.com/acer> to get the latest software for clients and the latest Echo Management software for server.