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.

2014 - 02 **Rev. A05.**

Contents

1

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 9 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 compatibility with RemoteFX, and VMware Horizon 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-**Devon IT thin clients also include commonly used client server applications such as the Citrix Online Plug-in and VMware Horizon 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-**Thin clients are capable of being re-imaged from a bootable USB Flash Device with the .EXE re-imaging executable file on it and the compressed image file in the .gz format.
- **Centralized Management-**Devon IT thin clients with WES7 can be easily managed with the Devon IT Echo Management Console.

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. We recommend that you are familiar with the material in this guide as well as the Echo Administration Guide to best utilize the first boot wizard.

2

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 that 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 it's own account name or account type, nor can they install or uninstall any software. It 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 000000 (six zeros).

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.

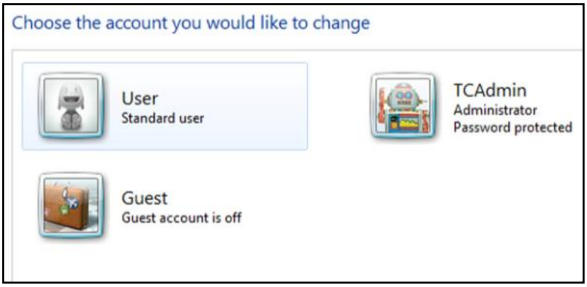
Creating New User Accounts

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 **Manage another account**.



4 Select **Create a new account**.

5 Type a name for the new user account.

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

Introduction to EWF and FBWF

By default, the EWF (Enhanced Write Filter) is enabled when a terminal with WES7 is first powered on. This write filter makes it so the terminal is in a non-persistent state. Any changes made to the software, any new software installed, and any settings that are changed will revert to their original state upon a reboot. However, there are times when an administrator may want to install new software, such as language MUI packs, and must disable the EWF. When enabled, the EWF allows for no changes to remain, without exception.

If desired, the EWF can be disabled and the FBWF can be enabled. The difference between the two is that it is possible to make exceptions to the FBWF, such as allowing Administrators to make changes, but not users.

The File-Based Write Filter, more commonly referred to as the FBWF, is a 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 XP environment. Devon IT thin clients include a management utility for configuring FBWF. The FBWF Manager utility can only be accessed by Administrators.

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

- Click **Start→ All Programs→ Echo Control Panel**.
- This will open the **Echo Control Panel. The FBWF/EWF Manager** is the top selection on the left hand side.

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?

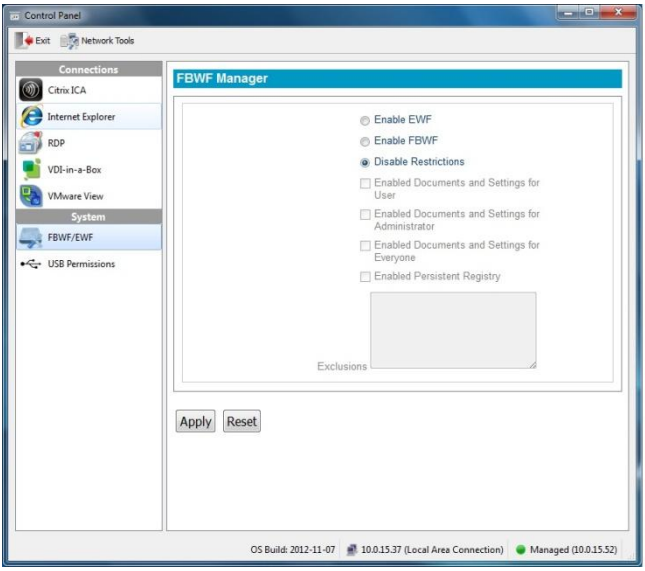
Persistence in its simplest definition is the term used to describe data on a local drive or disk that exists and survives from session to session. Persistent data will be secure after every reboot and every change made will be applied until another user reconfigures your changes. If you do not have 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

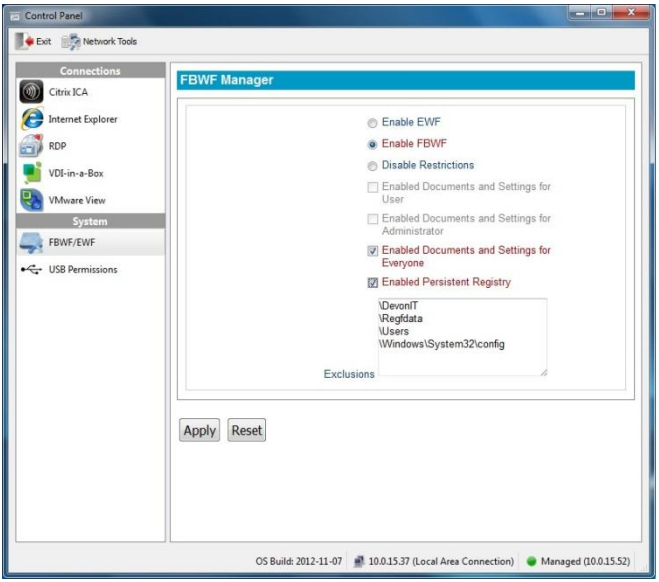
You may install third party licensed software as long as there is adequate space on the flash media.

To install additional software applications:

1. Log-in as an Administrator. Click **Start→ All Programs→Echo Control Panel**.
2. In the **FBWF/EWF Manager** tab, temporarily disable the write filter by clicking the **Disable Restrictions** button, 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** button. Also, make sure to re-enable the **Documents and Settings for Everyone** and **Persistent Registry** features. If you choose to enable EWF, there will be no exclusions.

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

3

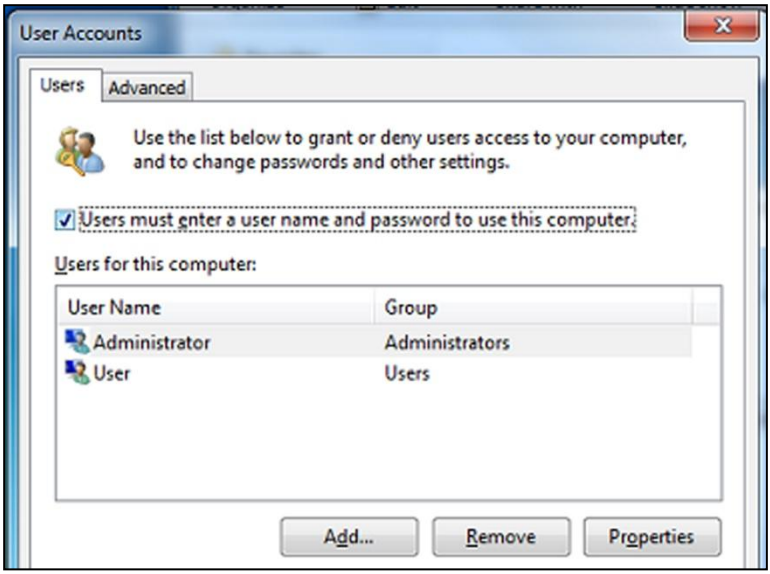
Using Your Thin Client

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. Enter "control userpasswords2" without the quotation marks and press enter.



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.

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 Horizon View client allows you to connect to a VMware Horizon 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.

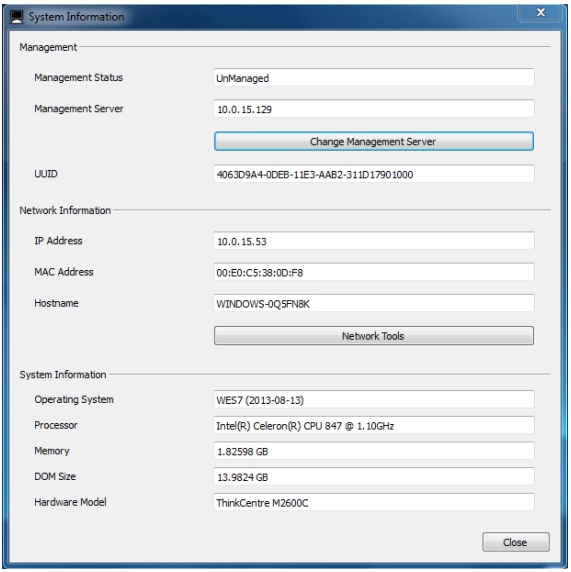
Echo Agent System Information

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.



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.

USB Redirection in VMware

By default, USB redirection in VMware Horizon View is not installed. In order to enable USB redirection in VMware Horizon View:

1. Log-in as an Administrator and disable the FBWF from the Echo control panel.
2. Download VMware Horizon View, which can be found here: https://download3.vmware.com/software/view/viewclients/VMware-viewclient-5.4.0-1219906.exe
3. Double click the EXE file to open the client application.
4. Select **Modify** from the radio button and then click **Next.**
5. Select **USB Redirection** from the drop down menu.
6. Select **This feature will be installed on local hard drive**, then click Next.
7. Click **Finished** to complete the process. Once this is completed, you may re-enable FBWF if desired.

4

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. While logged in as an Administrator, select **Start->Control Panel**. Under **Network and Sharing Center**, 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.

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. While logged in as an Administrator, select **Start→ Control Panel→ 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

NOTE: Performing the following steps may require Domain administrative rights.

1. While logged in as an Administrator, select **Start→ Control Panel→ 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 fields about your network and configures the system accordingly.

NOTE: Performing the following steps may require Domain administrative rights.

1. While logged in as an Administrator, select **Start→ Control Panel→ 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.

5

OS Build Date and Echo Agent

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. Click on the computer shaped icon in the task bar to open the **Echo Agent** system information menu.
3. The current OS build is posted in the **Operating System** field.

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→ Programs**. Select **Uninstall a program**.
3. The Echo agent will be the installed program labeled **Echo Agent-month-date-year**.
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.