YE*Station* User's Guide for Windows-Based Terminals Models 2xx9 with Embedded Standard 7

2419

2739

Copyright 2014 Affirmative Technology Group®
www.affirmativetg.com
April 2014

YES*tation* Limited Warranty

General Terms and Conditions

LIMITED PRODUCT WARRANTY. Affirmative Technology Group warrants that the YES*tation* Hardware Product shall be free from defects in materials and workmanship that arise under proper and normal use and service for three years from the date of purchase. A warranty extension of two years is available at extra cost, if obtained at the time of the original YES*tation* purchase. In the event that the YES*tation* Hardware Product fails to comply with the warranty set forth above, Affirmative Technology Group will repair or replace the Product. **Note:** Advanced Replacement for warranted units is only available for user sites in the United States and Canada.

SOFTWARE WARRANTY. Affirmative Technology Group warrants that, for a period of ninety (90) days from the date of purchase by the End User, its Software Products shall conform to its published specifications under normal usage. AFFIRMATIVE TECHNOLOGY GROUP DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT ALL SOFTWARE DEFECTS WILL BE CORRECTED. In the event that a Software Product fails to comply with the warranty set forth above, Affirmative Technology Group will replace the product. End User must, however, return all copies of the Software, along with proof of purchase, to Affirmative Technology Group within 90 days from the Software purchase date.

WARRANTY LIMITATIONS. End User's sole remedy under any Warranty provided by Affirmative Technology Group shall be limited to the replacement or repair of the Product or, at Affirmative Technology Group' sole discretion, a refund of the purchase price. AFFIRMATIVE TECHNOLOGY GROUP GRANTS NO WARRANTY, EXPRESS OR IMPLIED, OTHER THAN THE WARRANTIES STATED ABOVE. EXPRESSLY EXCLUDED ARE THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL AFFIRMATIVE TECHNOLOGY GROUP BE LIABLE FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INSTALLATION COSTS, LOST REVENUE OR PROFITS, OR ANY OTHER COSTS INCURRED AS A RESULT OF THE USE OF ANY AFFIRMATIVE TECHNOLOGY GROUP PRODUCT, WHETHER OR NOT USED IN ACCORDANCE WITH INSTRUCTIONS.

WARRANTY PROCEDURE. Affirmative Technology Group will replace or repair any defective, undamaged units for which a Return Material Authorization number (RMA#) has been obtained from the Technical Support Department. (Contact 855-437-1220 or 602-437-1220 or support@affirmativetg.com)

Copyright and Trademarks

Copyright Notice

This manual, as well as the software described in it, is furnished under license. No part of this publication may be reproduced, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of the copyright owner.

Note: Information in this document is subject to change without notice.

Trademarks Notice

- YES*tation*® is a registered trademark of Affirmative Technology Group®
- Microsoft® is a registered trademark of Microsoft® Corporation.
- Windows® is a registered trademark of Microsoft® Corporation.
- ICA® is a registered trademark of Citrix® Systems Inc.
- MetaFrame® is a trademark of Citrix® Systems Inc.
- Adobe®, the Adobe logo, Acrobat®, the Acrobat logo, and Acrobat Reader are trademarks or registered trademarks of Adobe Systems Incorporated.
- Ericom® and PowerTerm® are registered trademarks of Ericom® Software Ltd.
- Other company and brand, product and service names are trademarks or registered trademarks of their respective holders.

Table of Contents

AFFIRMATIVE TECHNOLOGY GROUP

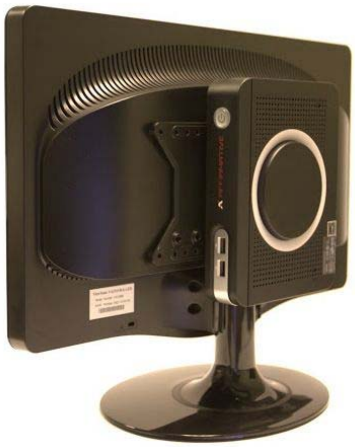
Installing Your Terminal

- Your terminal has no internal fan, and relies on natural airflow for cooling. When you mount it, *make sure to keep as many ventilation holes, as possible, unobstructed*.
- **DO NOT USE** any AC-DC adapter other than the one provided with the terminal or acquired from Affirmative Technology Group or its distributors.

Mounting

Horizontal mounting will obstruct the airflow required to cool the terminal. These terminals can either be mounted vertically on a flat surface, using the provided stands as shown in the picture on the front cover of this manual, or on the rear of LCD monitors using optional VESA mounting plates as shown here. Such a plate can be attached to most of the current crop of LCD monitors, as shown in the following figure.

VESA Mounting Plate on a 17" LCD Monitor



2419 Mounted on an LCD Monitor

2739 Mounted on an LCD Monitor

Cabling and Indicators

2419

Please make all cable connections before turning on the power. The 2419 has the following controls and ports:

- **Power Switch** (front)
- **USB** (two front and three rear)
- **DVI-I** (rear)
- **RJ-45 LAN** (rear)
- **Printer Parallel** (rear)
- **Serial** (two rear)
- **Earphone Output** (rear)
- **Microphone Input** (rear)
- **16V DC Power** (rear)
- **Kensington Lock** (knockout in left rear)

There are three LED indicator lights:

- **Power**. The translucent **Power** button serves as the Power indicator. This indicator turns blue when the terminal is powered up.
- **Network Connection**. This amber indicator at the upper right corner of the RJ-45 Ethernet connector is on when there is a good physical connection to the Local Area Network.
- **Network Activity**. This green indicator at the upper left corner of the RJ-45 Ethernet connector flashes to indicate LAN activity.

2739

Please make all cable connections before turning on the power. The 273x has the following controls and ports:

- **Power Switch** (front)
- **USB** (two front and three rear)
- **DVI-I** (rear)
- **VGA** (rear)
- **RJ-45 LAN** (rear)
- **Serial** (two rear)
- **Audio Output** (rear)
- **Earphones Output** (front
- **Microphone Input** (fear)
- **16V DC Power** (rear)
- **Optional PCI-e or Two Additional Serial** (rear)
- **Kensington Lock** (knockout in left rear)

There are four LED indicator lights:

- **Power**. The translucent **Power** button serves as the Power indicator. This indicator is faint amber when AC power is connected at the rear connector, and turns green when the terminal is powered up.
- **Network Connection**. This amber indicator at the upper right corner of the RJ-45 Ethernet connector is on when there is a good physical connection to the Local Area Network.
- **Network Activity**. This green indicator at the upper left corner of the RJ-45 Ethernet connector flashes to indicate LAN activity.
- **Flash Memory Activity**. This green indicator flashes when there is read or write activity to the flash memory.

Power On and Boot Up

These terminals can be powered on in two ways:

- Locally by pushing on the **Power** switch on the terminal.
- Remotely using eProManager remote central management software and the Wake on LAN capability of the terminals.

In either case, the process is:

1. Turn on the terminal after all rear panel connections have been made.
2. The translucent **Power** button will change from faint orange to light green.
3. You will briefly see the message **Starting System. Please Wait …** on a black screen.
4. After several seconds, you will see the Windows Embedded 7 startup screen which looks very much like your desktop Windows 7 startup screens.

Note: If you wish to access the terminal BIOS, press **F2** at the beginning of the bootup cycle.

Shutdown

These terminals should be shut down gracefully in typical Windows fashion by going to **Start>Turn Off Computer**.

THIS PAGE INTENTIONALLY BLANK

Embedded Standard 7 LIMITATIONS (*Read this Section)*

Your terminal is pre-configured with the Windows Embedded Standard 7 operating system and a minimal set of applications. If you are familiar with Windows 7 on your desktop or laptop PC, you are familiar with this terminal. In general, you can install the same applications or peripherals on this terminal as you can on a PC, subject to memory and I/O port restrictions. However, primarily due to the limited amount of flash memory for program storage, *THERE ARE SOME LIMITATIONS.*

- These embedded operating systems use a utility called EWF (Enhanced Write Filter) Utility to control write access to the flash memory. If Write Protect is enabled, configuration changes can be made and new applications or peripheral drivers can be installed, but these modifications will not be saved after a reboot unless a special operation is executed, before the computer is turned off, to save them in non-volatile memory. This operation is called Write Filter Commit, and you can learn more about it at Configuring Terminal Properties|Administrator Control Center|Control Panel|EWF Manager. *This protects your terminal from viruses, malware, and user games*. If Write Protect is disabled, changes, new applications, and bad stuff will automatically be saved in flash. Users are separated into two classes: computer administrator, and limited; limited users cannot execute any operation from the EWF Utility. So remember that changes made by limited users or Internet hackers will not survive a reboot unless Write Protect has been disabled by a user with computer administrator privileges.

- Embedded OS' are designed for a minimal memory footprint. It is possible to generate a configuration that has the same full, rich feature set as W7 Professional, but this would then require, for installation, the same large amount of non-volatile storage space that is required for these desktop versions. In your PC, you have many Gigabytes of non-volatile storage on a hard disk; in your WES7 terminal, you have 4,096 Megabytes of non-volatile flash storage to hold the operating system and your choice of applications.

- When the software image is first created for an embedded terminal product, the developer chooses from a laundry list of OS features, trying to anticipate which ones are most likely to be required by the bulk of the terminal users. This restricted feature set is probably most likely to be noticed in the Windows Control Panel; you will see many, but not all, of the standard OS control utilities. Furthermore, within each utility you will probably not find all of the configuration parameters that you would find in your PC. See Configuring Terminal Properties|Control Panel for information on the typical Control Panel.

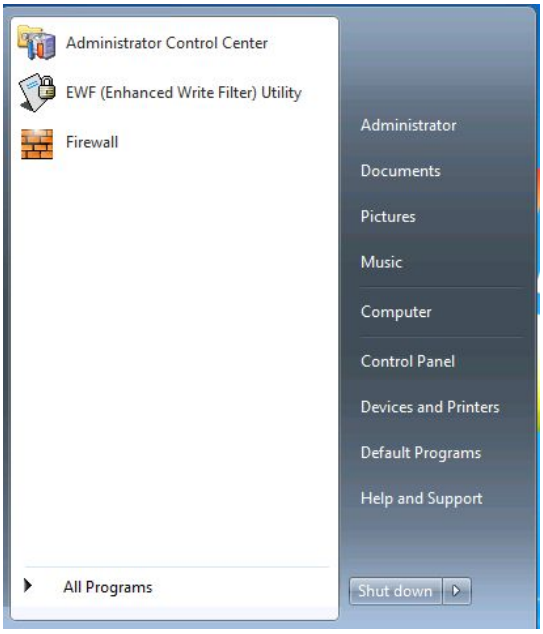
- As mentioned above, you can generally install and run the same applications on your WES7 terminal that can be installed on a W7 PC, if there is enough volatile and non-volatile memory. But be aware that some applications assume the availability of standard OS modules that may not have been included in your OS set. Therefore, these applications might install on the terminal, but they will not run. Unlike W7, which allows the installation or removal of some OS features in the field, embedded modules must be configured at build time; they cannot be added or removed in the field.

- If you are using Remote Desktop Protocol to access a Terminal Server, there is a further distinction between computer administrator rights and limited user rights. A limited user cannot store Terminal Server license information in the Registry, but a computer administrator can store such information. Hence a limited user using local rights cannot open an RDP session unless a computer administrator has already obtained a Terminal Server license for the terminal. See Configuring Terminal Properties|Administrator Control Center|Control Panel|EWF Manager.for more information on this subject.

This user guide will assume that the user or administrator is familiar with W7 administration and/or use as encountered on a PC. Therefore, this document will concentrate on those aspects of the embedded OS' which are significantly different from the PC versions..

Configuring Terminal Properties

Almost all of your terminal properties are configured from the Start window, but several require the use of the Affirmative Technology Group remote central manager, eProManager.

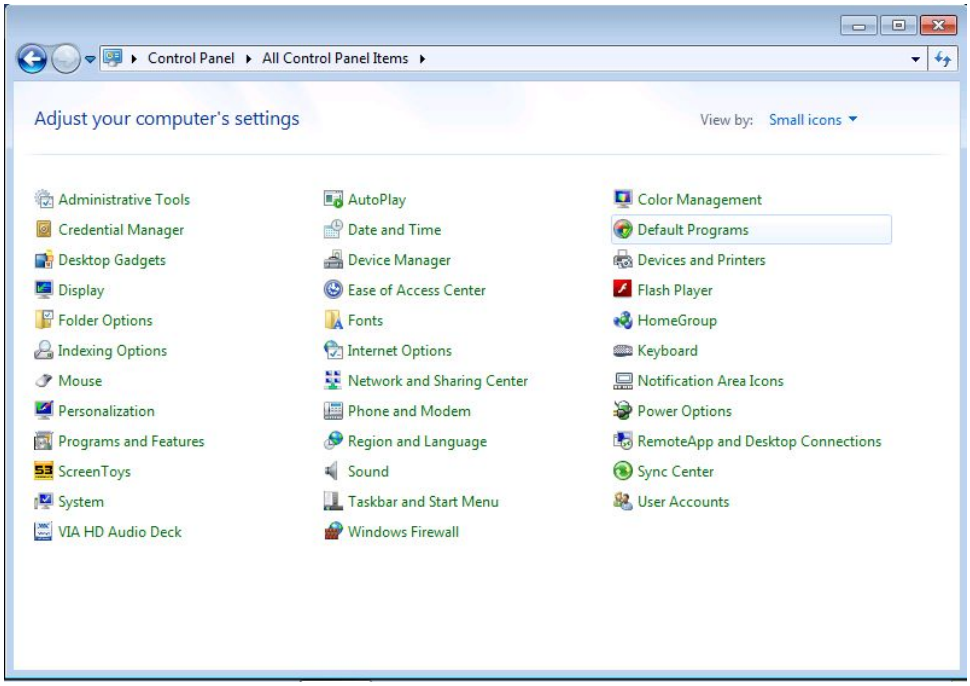


Start Window

Configuration changes and printer additions are initially stored in RAM. In order for these changes to be written permanently into non-volatile flash memory, thereby surviving a reboot, Write Protect must be disabled for the flash, or a Commit operation must be executed. See Administrator Control Center|Control Panel|EWF Manager for an explanation of the EWF (Enhanced Write Filter) utility, which provides Write Protect control.

Control Panel

Most terminal properties are configured in Control Panel.



Control Panel

As you can see, the YES*tation* build of WES7 does not include all of the configuration utilities available in W7. This is generally the case since each build is custom built to minimize memory footprint based upon expected customer usage. Also some utilities may not have all of the property parameters available in W7.

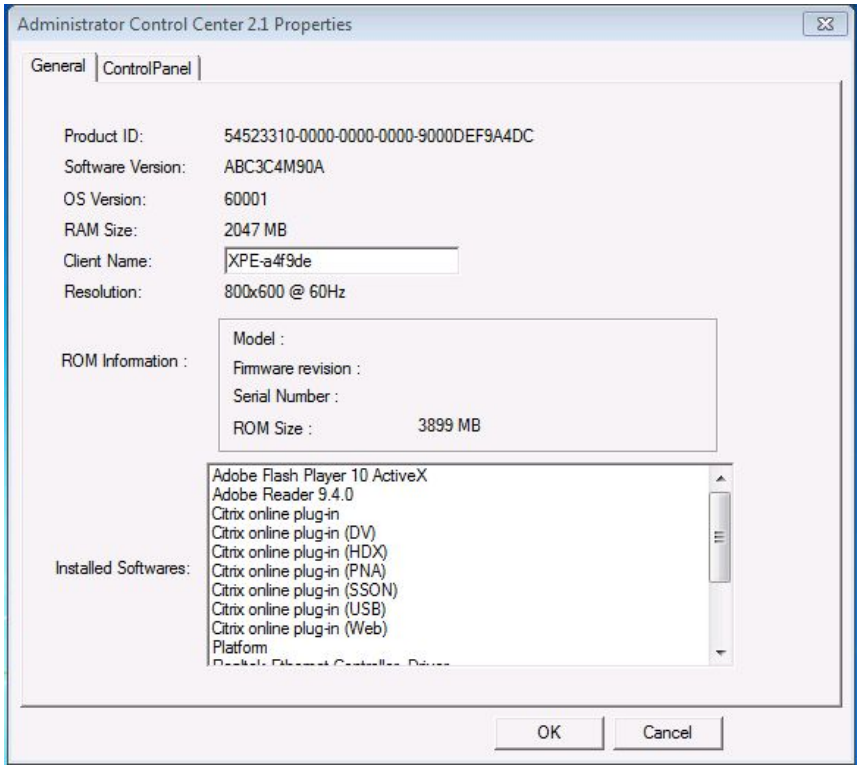
Administrator Control Center

Several properties are configured in Administrator Control Center, which is reached from the **Start** window. You will first see the Login dialog box.

Administrator Control Center Dialog Box

The default password is “guest”, but you can change that here by clicking on the **Change** button and following the dialog box. This same password is also used for the EWF Manager Utility. When you enter the correct password and click on **Login**, you will see the Administrator Control Center Properties-General window.

General



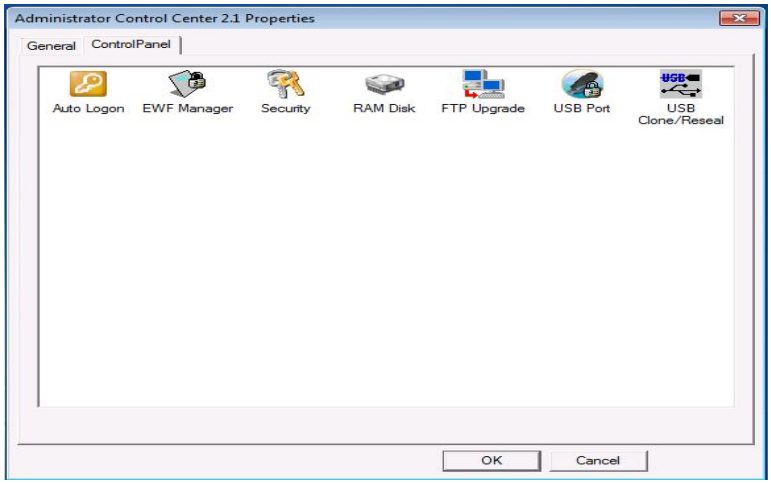
Administrator Control Center General Properties

Several of these general properties merit discussion.

- **Product ID**. The last twelve characters are a permutation of the MAC address.
- **Software Version**. This item identifies the specific image constructed by Affirmative and is useful when seeking technical support from Affirmative Technology Group.
- **OS Version**. This item is the number assigned by Microsoft for WES7. The leading numeral 6 identifies it as a version of W7; XP is identified by a 5.
- **RAM Size**. This is the remaining RAM after the Z drive has been allocated. See Control Panel|RAM Disk for more information..
- **ROM Size**. This is the approximate size of the flash memory. In the above example, the installed CompactFlash is 4096 MB.
- **Client Name**. This is the “friendly” network name seen by remote central management software and any network administration software. Even though this is a WES7 OS, Microsoft assigns an XPe default name. Enter a name that is meaningful to your network administrator.

ControlPanel

You must be in the administrator group to access any of the utilities in ControlPanel. Several important configuration utilities are accessed from this window.



Administrator Control Center ControlPanel

These utilities are separate from the standard Control Panel because their significance typically calls for the extra security provided by the password login and restriction to administrators.

Note: If you **OK** out of this window, you will see the following information box even if you have not made any changes using any of these utilities,

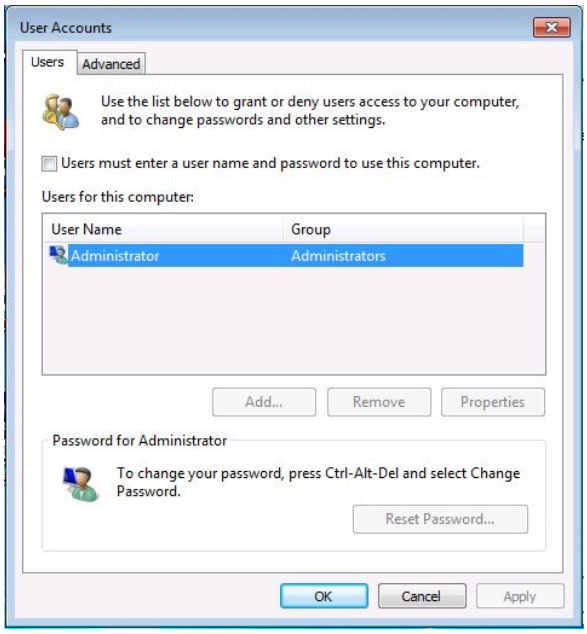
Commit Information Box

If you have made changes and want to save the changes into flash memory for use after the next reboot, be sure to click on **Yes**. See EWF Manager for more information on writing into flash.

Auto Login

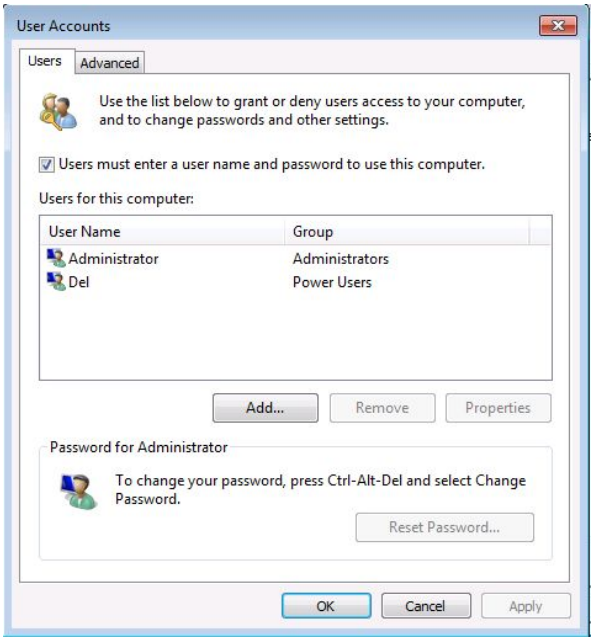
Despite the restrictive title, this utility also provides extended control of user accounts.

Users



Default User Accounts

New users can be added here or in **Control Panel>User Accounts**. **Guest** is not shown in the default panel, but it does exist, as you will discover if you try to add an account with that name. Several user properties can only be controlled from this utility. These properties are better illustrated if there are already multiple users, as shown in the following dialog box.



Additional User Account

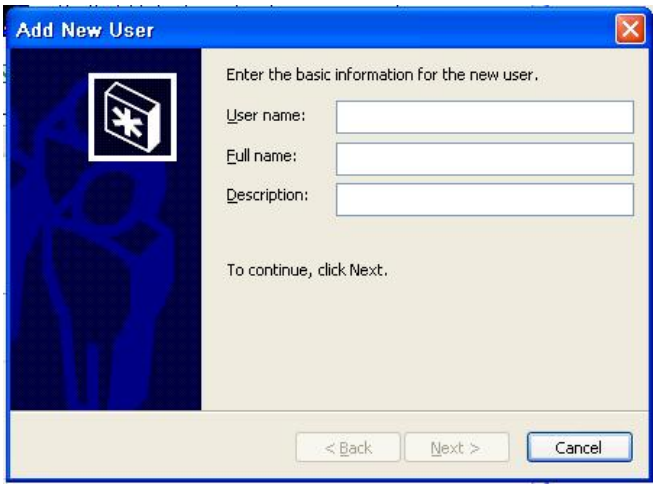
- **Users must enter…**. Check this box if you want user password control. But this control only exists for users that have been assigned passwords, and you can only assign passwords here in User Accounts. You can do this in one of two ways:
  - Add a new account here (click on **Add** and follow the Wizard) and define a password in the Wizard. You must check the **Users must enter…** box before you can add an account.

- Add password control to an existing user by highlighting that user in the user list, clicking on **Reset Password**, and entering the password in the resulting dialog box.

- **Users for this computer**. This box contains a list of all the defined users. **Administrator** is the default user; **Del** has been added.

Add.

Click on this button to launch the Add New User Wizard. You will be led through three dialog boxes.

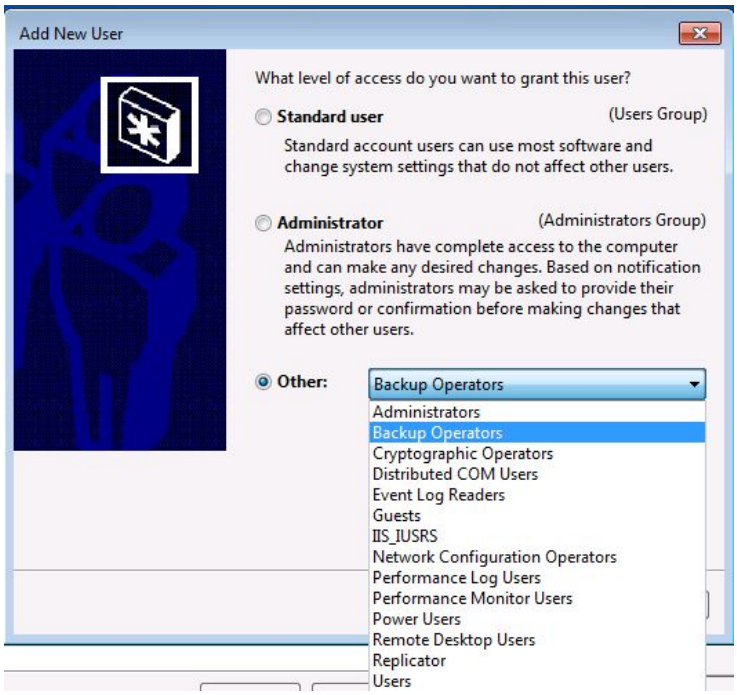


Add New User Dialog Box #1

Enter a **User Name**. The **Full Name** is the name you will see when you boot the terminal and arrive at the iconed Logon screen. If you want to enter some information about this user for future administrative clarification, enter it in the **Description** field.

Add New User Dialog Box #2

Enter and confirm a password if desired. If you want this user to auto logon (see Automatic Log On), you must enter a password.

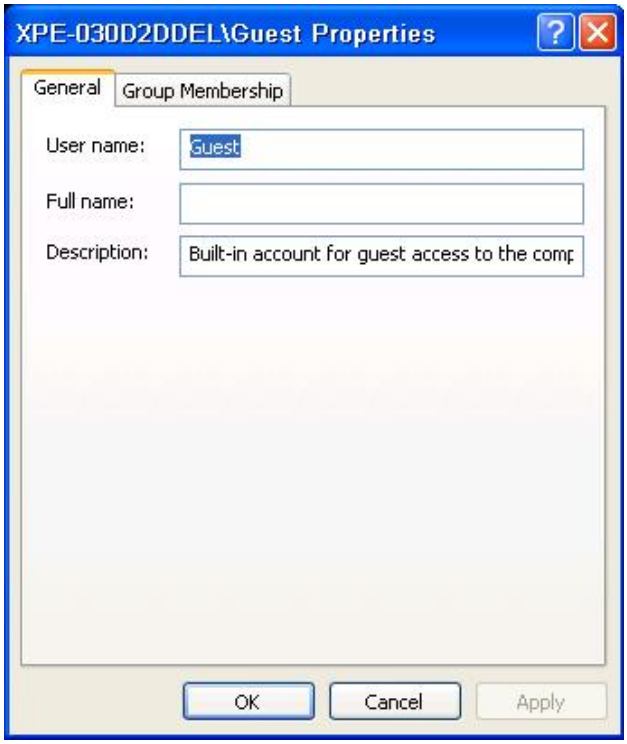


Add New User Dialog Box #3

Here is the interesting stuff. If you add a user through **Control Panel>User Accounts**, you have only two selections for the type of user, computer administrator (shown here as **Administrators**) and limited user (shown here as **Standard user** or **Users)**. But here you have additional options of **Guests** and **Power user**. You also see several other options if you select the **Other** radio button and access the drop-down list as shown in the above dialog box, but they have little or no use here.

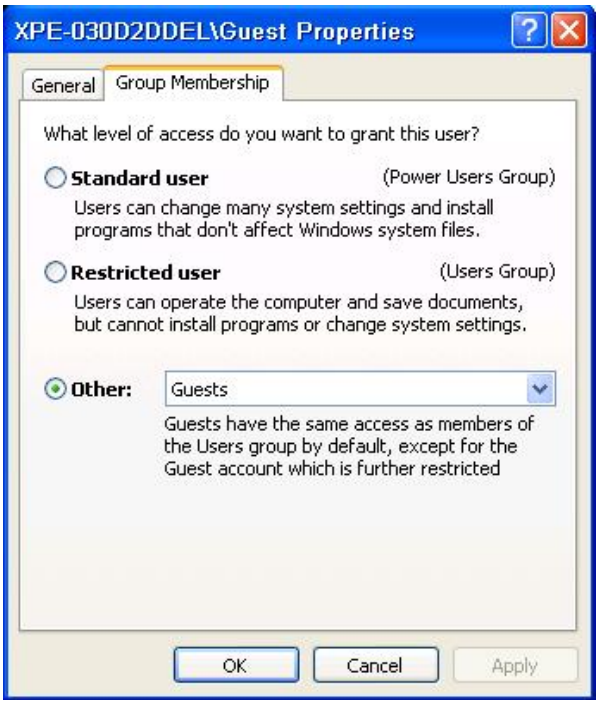
Properties

Click on this button to change the properties of an existing account. You can access two dialog boxes.



User General Properties Dialog Box

You can see that this dialog is a duplicate of the first dialog box encountered when adding a user.



User Group Membership Properties Dialog Box

This dialog is a duplicate of the final dialog box encountered when adding a user.

Reset Password

Click on this button to change the password for the highlighted user.

Reset User Password Dialog Box

This dialog is a duplicate of the second dialog box encountered when adding a user.

Automatic Log On

You can designate one user to be automatically logged on when you boot the terminal. To do this:

1. Highlight the desired user in the Users list.
2. De-select the **Users must enter…** box.
3. Click on **OK** or **Apply**. You will see the following dialog box.

Auto Logon Dialog Box

4. Enter the information for the user. You can change the user name here if you wish. **Note: You can enter a user name that is not in the User list, but the terminal will do strange, undesirable things on boot up.**
5. Click on **OK**.

EWF Manager

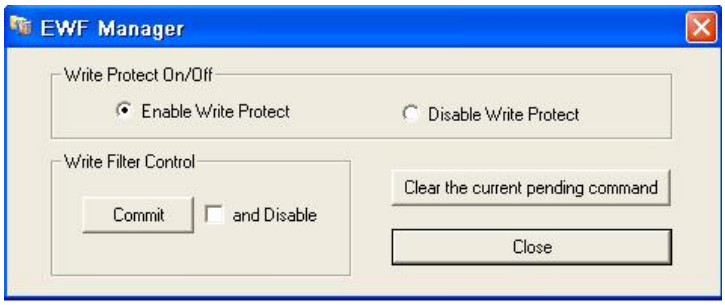
Enhanced Write Filter (EWF) may be the most visible difference between WES7 and W7, at least from an administrator's point of view. Flash memory (the c drive) is treated as a protected volume, and the protection must be disabled or a specific action must be taken in order to commit software, file, and configuration changes to flash. EWF is the utility that controls flash protection.

There are several reasons why you may want to write into flash memory.

- You have transferred files into your 2xx9 and want to save them for future use after a Power Off or reboot.
- You have made configuration changes, such as those made via Control Panel, and want to retain them after a reboot.
- You have installed new application programs or device drivers and want to save them for future use after a reboot.
- You have signed on to a Terminal Server for the first time and want to save the TSCAL information.
- You are participating in a Domain and want to save the Domain Secret Key.

When flash write protection is enabled, changes, new software, etc. are written into a RAM overlay. The contents of this overlay can be written into flash, as shown below. But if the contents are not written into flash, they are lost when the terminal is rebooted. If write protection is disabled, changes, new software, etc. are written immediately into flash and are still available after a reboot.

Click on the icon to open the following dialog box.



EWF Manager Dialog Box

- **Write Protect On/Off**. These two radio buttons show the current status of EWF.
  - **Enable Write Protect**. If this radio button is active, the flash memory is write protected (EWF is enabled). This is also an action button; if the **Disable Write Protect** button is active (EWF is disabled), you can switch to a protected state by clicking on **Enable Write Protect** and closing the dialog box.
  - **Disable Write Protect**. If this radio button is active, the flash memory is not write protected (EWF is disabled). You can switch from the protected state to an unprotected state by enabling this button and closing the dialog box.
- **Write Filter Control**. In addition to the enabling action provided by the **Enable Write Protect** button, you can initiate two other actions here.
  - **Commit**. Click on this button to commit the overlay contents to flash. You will see the following information box

EWF Commit Information Box

    This box is for information only. It is not asking for your approval, so the commit will take place regardless of whether you click on **OK** or **X**.
  - **and Disable**. If you make this selection and then close the dialog box without clicking **Commit**, there is no subsequent action. This option has no effect without clicking **Commit**.
  - **Commit and Disable**. Check the **and Disable** box and then click on **Commit** to commit the overlay contents to flash and disable the flash protection on the next boot up.
- **Clear the current…**. If you have a change of heart, click on this button and no action will be taken on bootup..
- **Hide**. If you click this button, the dialog box will disappear, but you can still access it by clicking on the icon in the System Tray.
- **Close**. Click here to close the EWF dialog box. If you took action to enable or disable write protect, that action will not actually take place until you reboot your terminal, as you will be reminded by the following information box.

Restart Information Box

There are two other ways to access the EWF utility.

- Enter from **Start>All Programs>EWF**. You will have to enter the EWF password to gain access. Even a non-administrator can gain access this way and appear to make changes after going through all the boxes. However, after reboot you will see that the changes never occurred.
- Use the command line interface from **Start>Run>Cmd**. In this case, no EWF password is required. However, the EWF commands will be executed only for administrators. Here are the available commands.
  - **ewfmgr c:** This command gives you the current protection state, **DISABLED** or **ENABLED**, of the C drive.
  - **ewfmgr c: -enable** This command enables protection *after the next reboot*.
  - **ewfmgr c: -commit** This command commits, at this point in time, any new files, software, and configuration changes to flash without regard to the protection state.
  - **ewfmgr c: -commitanddisable** This command commits, at this point in time, any new files, software, and configuration changes to flash without regard to the protection state, and then disables protection *after the next reboot*.

Security

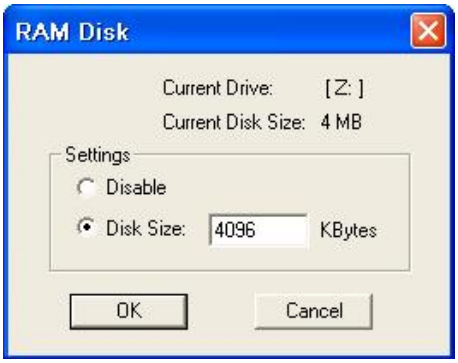
Click on this icon for another opportunity to change the Administrator Control and EWF Manager password. You will see the following dialog box.

Change Password Dialog Box

The entries are self-evident, but there is one eccentricity. Even if your only desire is to disable the password, this utility still demands a new, confirmed password before disabling.

RAM Disk

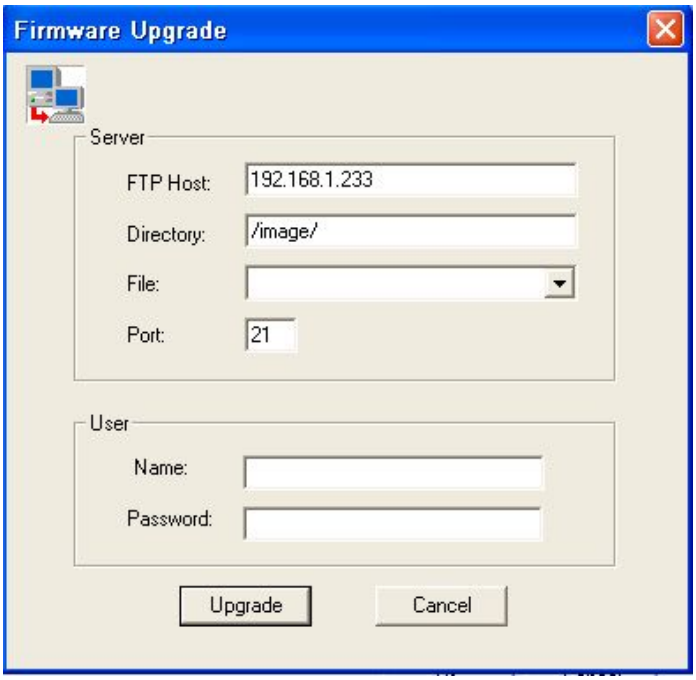
Click on this icon to adjust the size of the RAM disk.



RAM Disk Dialog Box

FTP Upgrade

Click on this icon to see the Firmware Upgrade dialog box. If you have an FTP host somewhere on your network, you can pull down and install a new image file from that host. This new file will replace the current contents of the terminal's flash memory, and *all configuration parameters will be replaced with those in the new image*.



Firmware Upgrade Dialog Box

1. Enter the parameters for your FTP server, as instructed by your network administrator.
2. Click on the **File** dropdown arrow to see the available image files at that server.
3. Highlight the desired image file.
4. Click on **Upgrade**. The image will now be upgraded without any further required interaction.

If you have Affirmative Technology Group' remote management software, eProManager, installed on your network, you can execute this same procedure from that management console, rather than having to be on site. Using that software, you can schedule the procedure to occur automatically at a convenient time, if you wish.

USB Port

This applet controls the use of USB storage. Click on this icon to see the USB Storage Control dialog box.

USB Storage Control Dialog Box

For security reasons, you may want to avoid files being removed from your unit by disabling USB storage. In that case, check the **Read-only USB Storage** box, and nothing can be copied into attached USB storage.

USB Clone/Restore

This applet allows you to clone the current image to a USB drive and restore that image to any WES7 thin client with the same hardware configuration. See Cloning a 2xx9 YES*tation* Image for cloning/restore details.

THIS PAGE INTENTIONALLY BLANK

Cloning a 2xx9 YES*tation* Image

The 2xx9 YES*tation* has the capability to clone firmware images to other 2xx9 YES*tations*. You can build your special Desktop configuration, add applications and peripheral drivers, and then exactly reproduce the resulting firmware image on other units. You can create as many unique images as you wish, with the images stored in local USB drives or network-share directories anywhere on your network. In this section, the two methods of clone/restore will be referred to as **local** and **network**.

Requirements

First, two definitions:

- The **benchmark** YES*tation* is the unit on which the desired configuration, applications, and drivers are first assembled.
- The **target** YES*tation* is the unit which is to be made identical to the benchmark unit.

YES*tations* are based on several different hardware platforms, and cloning across different platforms is usually not exact. Applications and peripheral drivers should present no problem, but configuration parameters that depend upon internal hardware may not be cloned. This is often the case with display parameters, for example. For the best and most reliable results, use identical benchmark and target hardware platforms.

Network cloning requires the following elements:

- eProManager remote central management software, version 3.4a or above, installed on a management console on the network. This software can be downloaded from the Affirmative Technology Group web site; contact Affirmative Technology Group Technical Support for instructions.
- Benchmark and target units installed on the same network as eProManager.
- The network must have a DHCP server.
- Benchmark and target units to have flash memory of the same size.
- At least one shared directory on the network that can be used to store the clone images.
- The YES*tation* must have a wired connection to the network. Cloning and restoration will not work with a wireless YES*tation* connection.

Local cloning requires the following elements:

- Benchmark and target units to have flash memory of the same size.
- USB drive with free space equal to or larger than the flash memory in the units. **Note:** This is *not* the size of the image, but the total size of the flash—typically 4 GB.
- Benchmark and target units with older images must be connected to a network with a DHCP server. Yes, this is a strange requirement for local storage, but it is due to using legacy code borrowed from the network procedures. Newer images do not have this restriction, but we can't provide a cutoff point here. Contact Affirmative Technology Group Tech Support if you have questions about your particular image.

Network Cloning

Cloning consists of two major operations: Capture and Restoration.

- Capture involves the extraction and storage of the benchmark image.
- Restoration involves moving the benchmark image to the target unit and loading the image into the flash memory of the target unit.

eProManager

ePro is the central element in network cloning. This remote central management software must be installed on a computer on the same network as the benchmark and target YES*tations*. The installation requirements are:

- Windows 2000 Professional/Server/Advanced Server with Service Pack 3 or higher, Windows XP Professional, Windows 2003 Server, Windows 7 PC, or Windows 2008 Server.
- 13MB-20MB disk space.

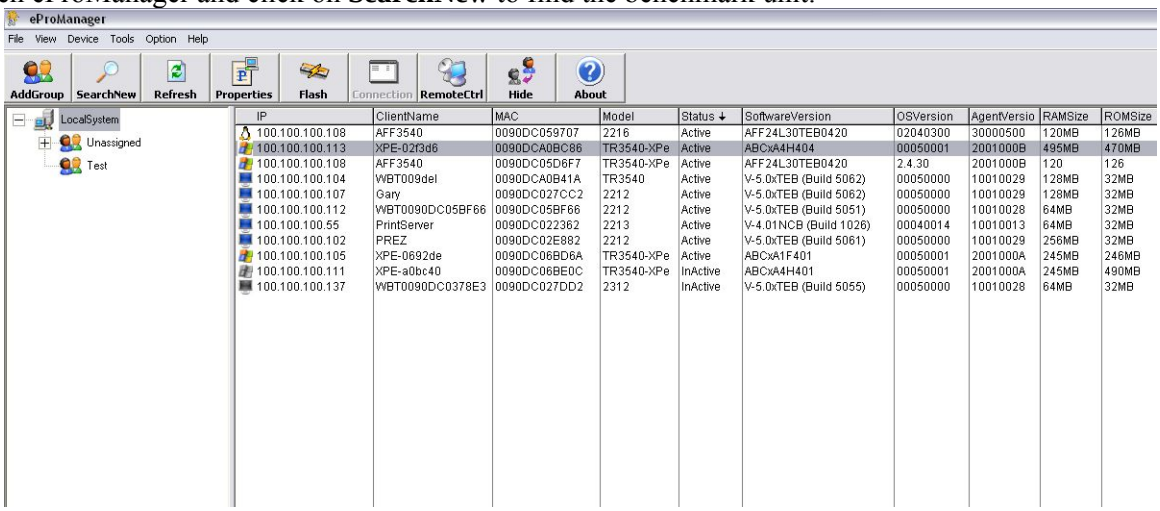
This document only discusses the particular aspects of ePro that apply to cloning. Complete details on the installation and operation can be found in the eProManager User Guide at http://www.affirmative.net/pub/eProManagerUserGuide.pdf.

You can download an installation package of the latest version of ePro from http://www.affirmative.net/EPROMANAGERV4.8.ZIP. Installation instructions are included in the zip file and in the User Guide.

Capture

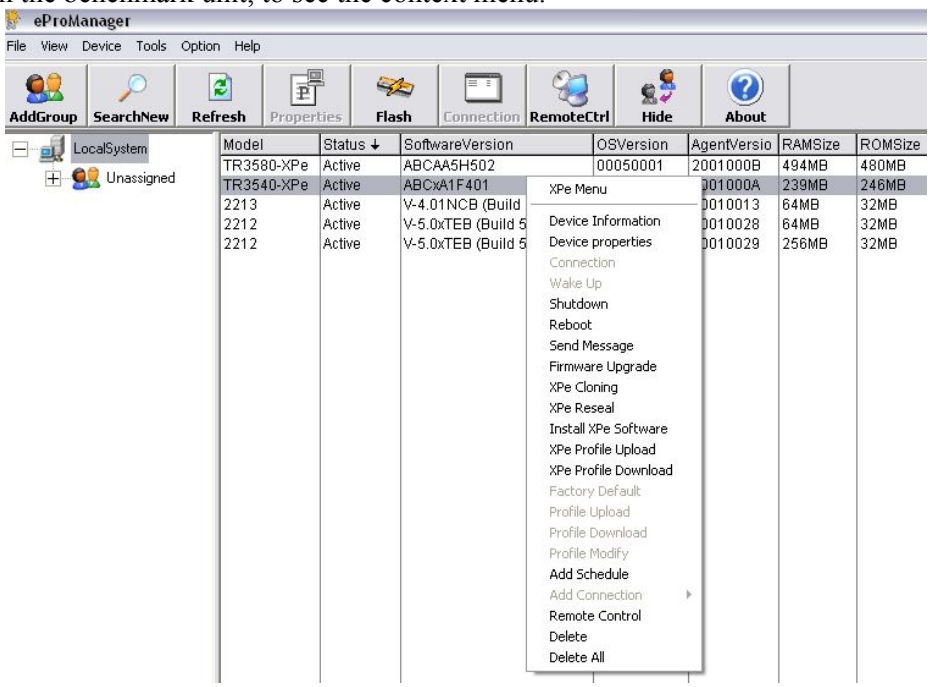
The capture procedure is:

1. Set up a base benchmark unit with a WES7 image..
2. Configure the benchmark unit per your Desktop needs and with all the desired applications and peripheral drivers.
3. Connect the benchmark unit to the same network as your eProManager management console.
4. Open eProManager and click on **SearchNew** to find the benchmark unit.



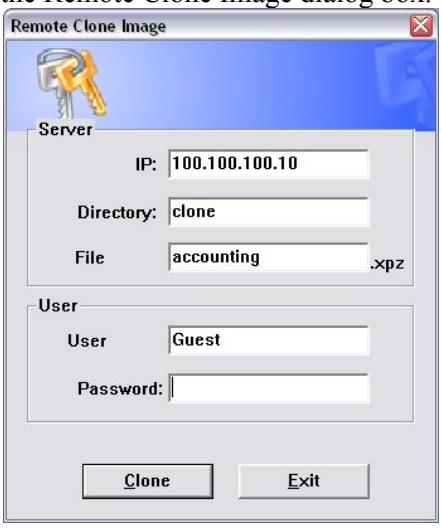
ePro Local System Terminal List

5. Right click on the benchmark unit, to see the context menu.



XPe Context Menu

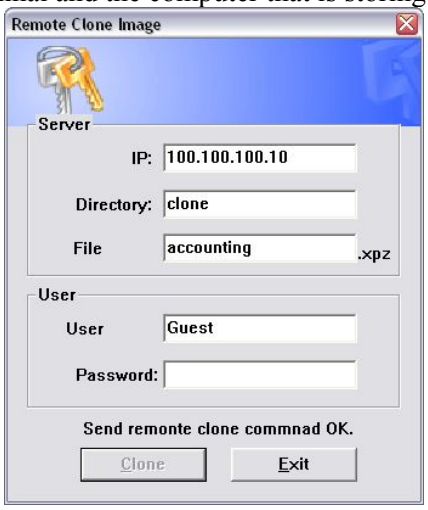
6. Left click on **XPe Cloning** to see the Remote Clone Image dialog box.



Remote Clone Image Dialog Box

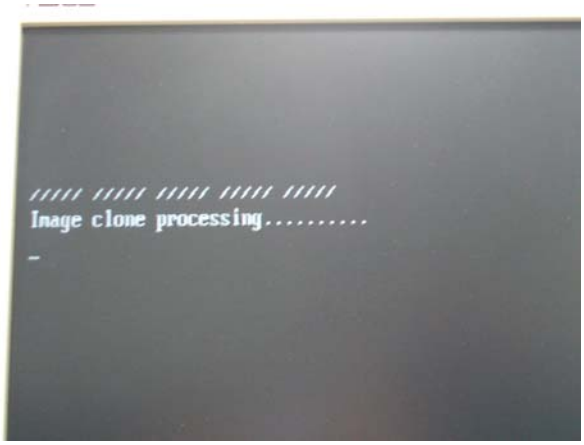
7. Enter the information:
   - **IP**. This is the IP address of the computer on the network that contains the shared directory that will contain the captured images. You can use your management console as the server, or you can use any Windows computer on the network that allows shared directories.
   - **Directory**. This is the share name of the directory that will contain the captured images. Do not enter the complete path; only enter the share name.
   - **File**. This will be the name of the captured image file. The extension, **.xpz**, will be added automatically.
   - **User/Password**. This is the *local* user name and password that allows access to the shared directory. **Note: If the shared directory is in a domain environment, you must use the local User/Password, not the domain credentials.**

8. Click on **Clone**. You should see a confirmation that the remote clone command has been sent. You can now close this dialog box if you wish. ePro is now out of the capture loop, with all subsequent interaction taking place between the benchmark terminal and the computer that is storing the image files.



Remote Clone Image Dialog Box with Confirmation

9. If you look at the benchmark unit display, you will see the unit shut off and then reboot with a lengthy Linux boot dialog. At the end of the dialog, you will see the processing message.



10. The image capture is a relatively slow process, occurring at about 9MB-50MB per minute, depending upon your hardware platform. At the end of this process, the benchmark unit will reboot and you should see three new files in your share directory, the desired **.xpz** image file and two information files (a **.res** and a **.txt** file). You won't get much information out of the information files, and they are not subsequently necessary for any image processing, so you can safely delete them. You will be using the **.xpz** file for subsequent restoration.

Restoration

Your **.xpz** images can be restored to any target YES*tation*, subject to the afore-mentioned requirements (see Requirements). But there are two different methods for restoration, FTP Update or Reseal.

FTP Update

You can execute a pull from the terminal or a push from eProManager. In either case, you must have an FTP server, configured to access your shared directory of image files, running somewhere on your network. Most network administrators use the FTP server that is a standard feature of Windows servers, but any FTP server will work if it is properly configured. FTP server configuration is not covered here.

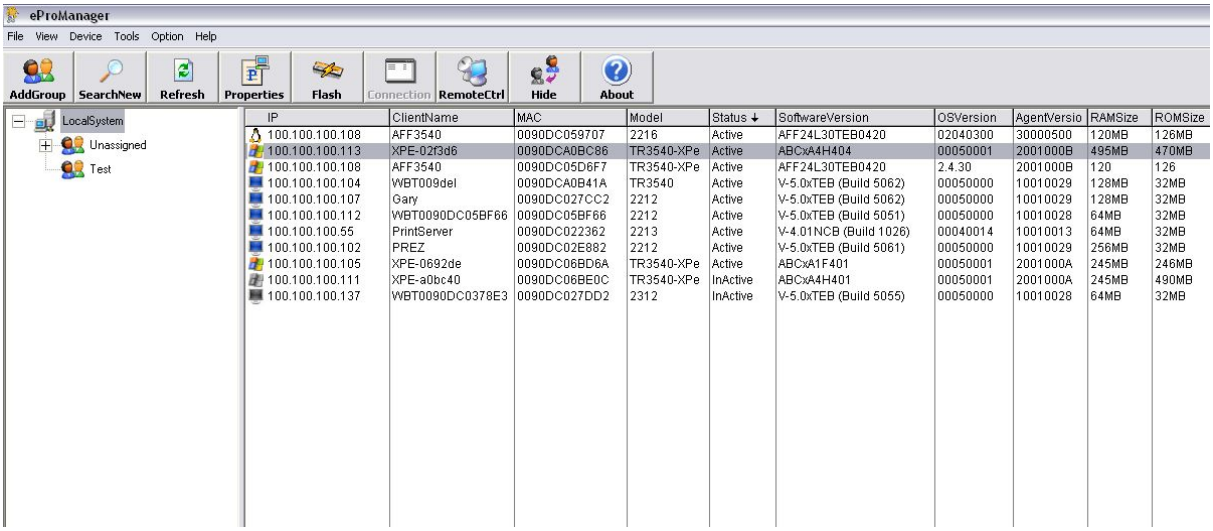
Only the pull procedure will be covered here, since a push is more conveniently done using resealing rather than FTP. The procedure is:

1. Make a copy of your desired benchmark image file and rename it with a **.xpe** extension. The FTP method for WES7 terminals only works with **.xpe** files, but **.xpe** and **.xpz** files are identical except for the name.
2. Place this **.xpe** file in a folder that is accessible to your FTP server.
3. Now follow the FTP procedure described in Configuring Terminal Properties|Administrator Control Center|Control Panel|FTP Upgrade.

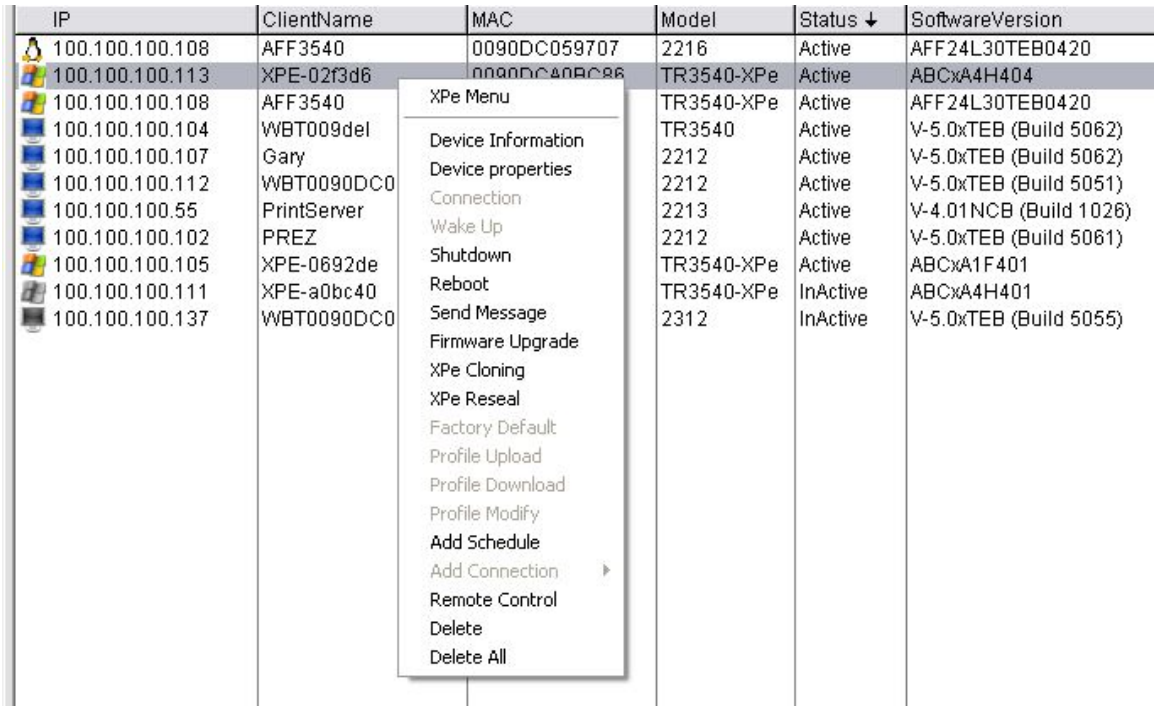
Reseal

The procedure is:

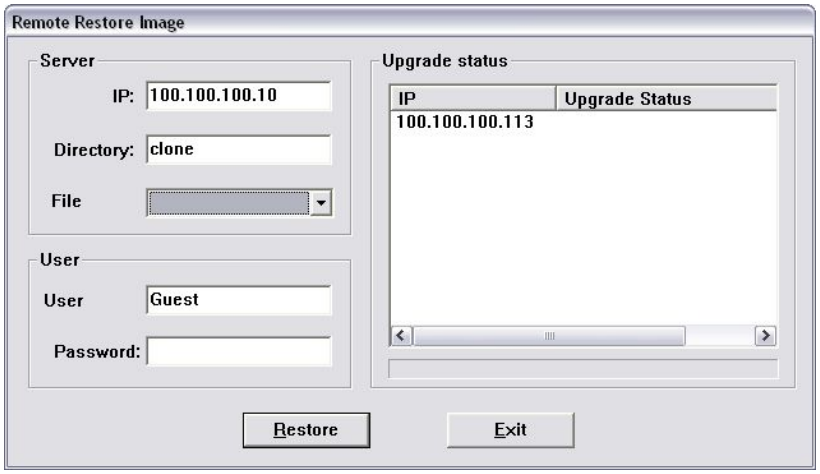
1. Make sure that your desired benchmark image file has a **.xpz** extension. If that file has a **.xpe** extension, rename it with a **.xpz** extension. The Reseal method for only works with **.xpz** files, but **.xpe** and **.xpz** files are identical except for the extension label.
2. Open eProManager and click on **SearchNew** if your target unit is not seen in the terminal list.



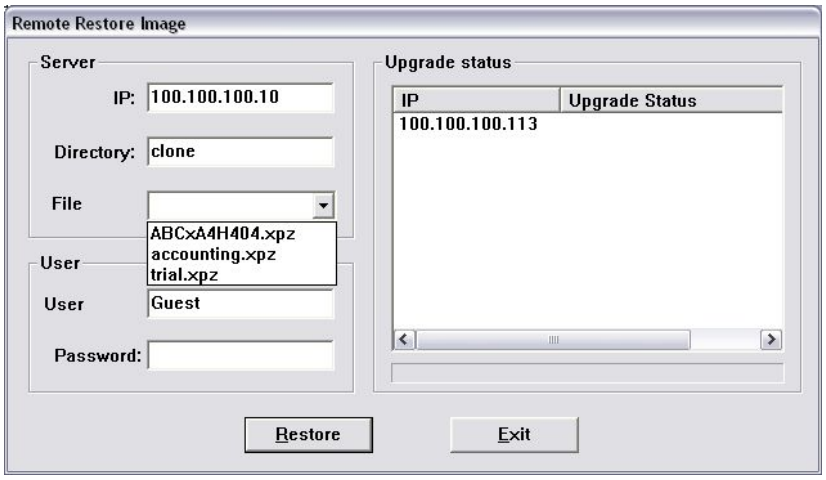
3. Right click on the target unit, to see the context menu.



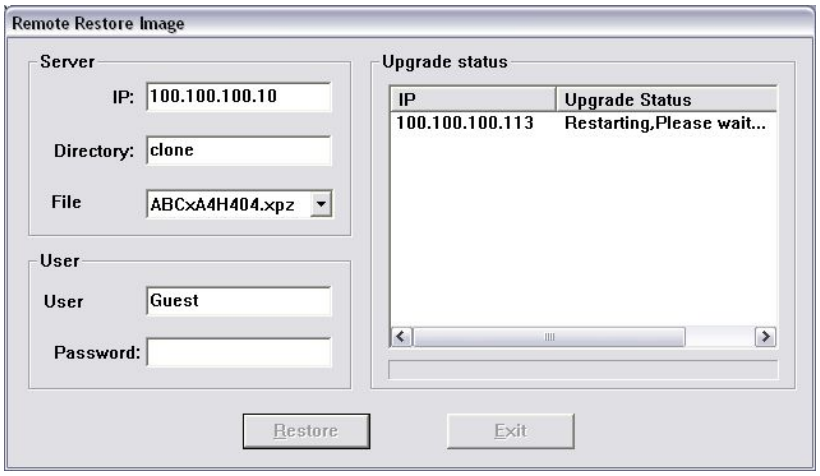
4. Left click on **XPe Reseal** to see the Remote Restore Image dialog box.



5. Enter the information:
   - **IP**. This is the IP address of the computer on the network that contains the shared directory with the images to be restored. You can use your management console as the server, or you can use any Windows computer on the network that allows shared directories.
   - **Directory**. This is the share name of the directory that will contain the restore images. Do not enter the complete path; only enter the share name.
   - **File**. You cannot enter anything into this field.
   - **User/Password**. This is the *local* user name and password that allows access to the shared directory. You *must* enter something in the Password field. If your password is blank, enter a character and then delete it. **Note: If the shared directory is in a domain environment, you must use the local User/Password, not the domain credentials.**
6. Click on the drop-down arrow of the **File** field to see a list of all the **.xpz** files in the image directory.



7. Highlight the desired file and click on **Restore**. You will see a "Restarting…" message.



8. If you look at the target unit display, you will see the unit shut off and then reboot with a lengthy Linux boot dialog. At the end of the dialog, you will see an **"Image restore processing"** message.
9. The image restore is a relatively fast process, occurring at about 80MB-100MB per minute. At the end of this process, the target unit will reboot and you should see the Desktop results of the new image.

Local Cloning

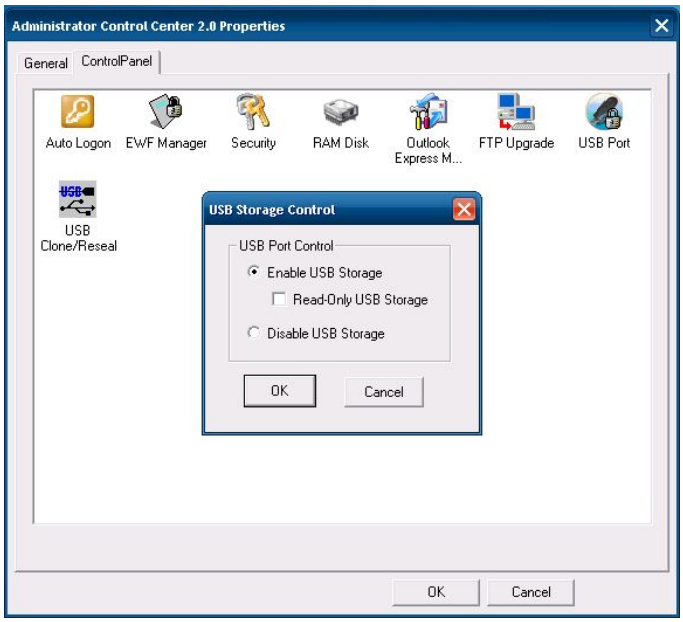
Cloning consists of two major operations: Capture and Restoration.

- Capture involves the creating, extracting, and storing of the benchmark image.
- Restoration involves moving the benchmark image to the target unit and loading the image into the flash memory of the target unit.

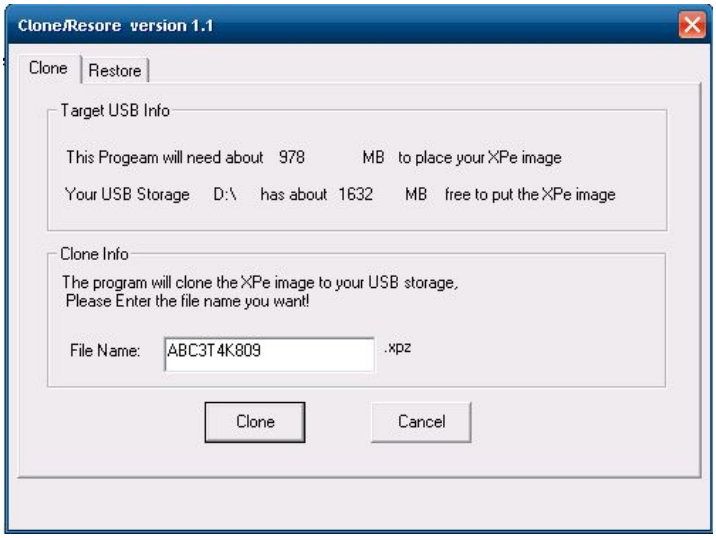
Capture

1. Make sure that your USB drive has enough free space. The cloned image itself probably does not occupy the entire flash memory, but the USB Clone/Reseal applet assumes that all of the internal flash will be cloned and requires that much free space.

2. Open the Administrator Control Center Control Panel and make sure that the USB Port applet has USB Storage enabled.



3. Insert your USB drive.
4. Open the USB Clone/Reseal applet, click on the **Clone** tab, and enter a file name in the File Name field. The **.xpz** will automatically be added to the file name when the file is stored.

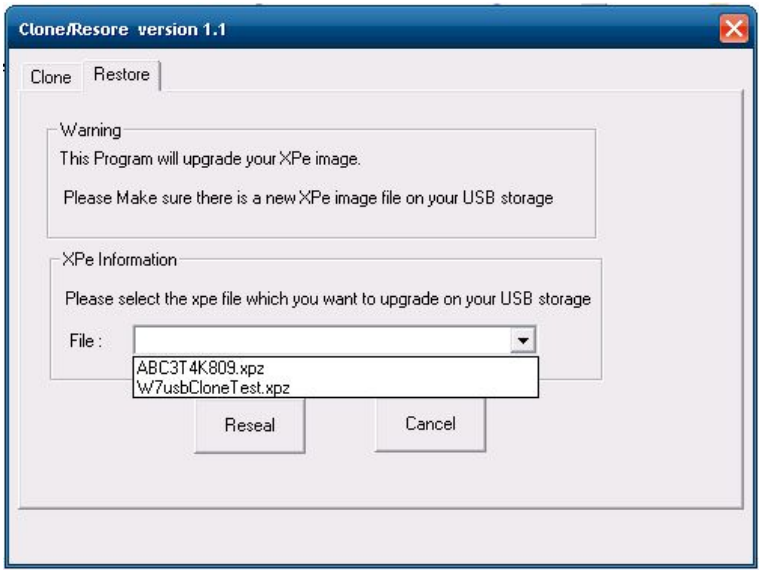


5. Click on **Clone** and watch the action, although that can get quite boring.
6. The unit will automatically restart, go through a Linux bootup process, and start cloning. This is where it gets boring, since all you will see for 10-15 minutes are dancing diagonal lines.
7. When cloning is complete, the unit will reboot back to the XPe desktop.

Note that the image file obtained this way is exactly the same as the image file that can be obtained over the LAN via the cloning process in eProManager. Therefore, you can use this file for Resealing over the network, and vice-versa.

Restoring

1. Make sure that the boot order in your BIOS puts the internal HDD ahead of the USB drive. Access the BIOS by toggling **F2** at the start of boot-up.
2. Open the Administrator Control Center Control Panel and make sure that the USB Port applet has USB Storage enabled.
3. Insert your USB drive.
4. Open the USB Clone/Reseal applet, click on the **Restore** tab, and choose the appropriate **.xpz**; file from the drop-down list.



5. Click on **Reseal** and watch the action, although that can get quite boring.
6. The unit will automatically restart, go through a Linux bootup process, and start copying the **.xpz** file into the flash memory. This is where it gets boring, since all you will see for several minutes are dancing diagonal lines.
7. When copying is complete, the unit will reboot back to the WES7 desktop.

Note that you can also use this same **.xpz** file to reseal over the network as described in **Network Cloning|Restoration|Reseal**.

THIS PAGE INTENTIONALLY BLANK

Supporting Your YES*tation*

Affirmative Technology Group offers Technical Support services for all the Affirmative products. You can access Affirmative Technical Support in one of the following ways:

- via Phone
  - 602-437-1220
  - 855-437-1220
- via Fax
  - 602-437-1320
- via E-mail
  - support@affirmativetg.com