

Microsoft® Windows Embedded Standard 2009
(WES) and Windows® XP Embedded (XPe)
Quick Reference Guide
HP thin clients



© Copyright 2008, 2009 Hewlett-Packard Development Company, L.P.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. Win32, Windows Internet Explorer, and Windows Media Player are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Acrobat are trademarks or registered trademarks of Adobe Systems Incorporated.

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

This document contains proprietary information that is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company.

Microsoft Windows Embedded Standard 2009 (WES) and Windows XP Embedded (XPe) Quick Reference Guide

HP thin clients

Second Edition (April 2009)

First Edition (September 2008)

Document Part Number: 502961–002

About This Book

This guide supplements the standard XPe documents supplied by Microsoft Corporation. This document highlights the differences, enhancements, and additional features provided by the latest image with this terminal.

- △ **WARNING!** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.
- △ **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.
- 📝 **NOTE:** Text set off in this manner provides important supplemental information.

Table of contents

1 For More Information and Updates

2 Introduction

The Desktop	3
User Desktop	3
Administrator Desktop	3
Server Environment Requirements	4
Session Services	4
Citrix ICA	4
Microsoft RDP	5
Terminal Emulation Support	5
Support Services	5
Altiris Deployment Server	5
HP Device Manager	5

3 Configuration

Logging On	6
Automatic Logon	6
Manual Logon	7
Administrator Logon Access	7
Logging Off, Restarting, and Shutting Down the Thin Client	8
Enhanced Write Filter	8
Power Management	9
System Time	9
Local Drives	10
Drive Z	10
Drive C and Flash	10
Saving Files	11
Mapping Network Drives	11
Roaming Profiles	11
User Accounts	11
Creating a New User Account	11
User Manager	11
User Profiles	12

Regional and Language Options	14
Administrative Tools	15

4 Applications

Symantec Endpoint Protection Firewall	17
About the Agent	17
New Features and Functionality	18
Microsoft Windows Firewall	18
On-by-Default	18
Configuring Microsoft Windows Firewall	18
Gathering Configuration Information	21
Troubleshooting Applications	21
Failure Symptoms	21
Resolution	22
Adding a Program	22
Adding a Port	22
Citrix Program Neighborhood and PN Agent	24
Remote Desktop Connection	25
HP Remote Desktop Protocol (RDP) Multimedia and USB Enhancements	27
HP Remote Graphics Software (RGS) Receiver	27
HP Session Allocation Manager (SAM) Client	28
Teemtalk Terminal Emulation	29
VMWare View Manager	29
Altiris Client Agent	30
HP Management Agent	32
HP Client Automation Registration and Agent Loading Facility (RALF)	32
Microsoft Internet Explorer	33
Windows Media Player 11	33

5 Control Panel Extended Selections

Enhanced Write Filter Manager	36
Benefits of the Enhanced Write Filter	36
Enhanced Write Filter Status Service	36
Enhanced Write Filter GUI	37
EWF GUI Buttons	38
DOS Command-line Tool Boot Commands	39
Using Boot Commands	39
HP RAMDisk	39
HP DHCP Settings Update Client	41
HP ThinState Capture	42
HP ThinState Deploy	45
HP FTP Image Update	46
Server Requirements	46

DHCP Server	46
FTP Server	46
Description	46
Host Settings	47
Select Image to Update	47

6 Administration and Image Upgrades

Altiris Deployment Solution Software	49
HP Device Manager	49
Add-on Upgrades	49
Image Upgrades	49
HP FTP Image Update	50
HP ThinState Capture and Deploy	50
HP Compaq Thin Client Imaging Tool	50
HP Client Automation	50

7 Peripherals

Printers	51
Adding Printers Using Generic Text-only Print Driver	51
Using Manufacturer Print Drivers	52
HP Universal Print Driver for Thin Clients Add-on	52
Audio	52

Index	53
--------------------	-----------

1 For More Information and Updates

HP provides add-ons, Microsoft® Quick Fix Engineering updates (QFEs), and periodic updates for thin client images. Check the HP support site for these updates or for important documentation that provides specific information for the image version at <http://www.hp.com/support>. Select the country from the map, then select **See support and troubleshooting information** or **Download drivers and software (and firmware)**. Type the thin client model in the field and click [Enter](#).

2 Introduction

HP WES-based thin client models use the Windows Embedded Standard 2009 (WES) operating system. HP XPe-based thin client models use the Windows XP Embedded (XPe) operating system. This guide provides information pertaining to the latest shipping WES and XPe Service Pack 3 (SP3) images. These thin clients provide the flexibility, connectivity, security, multimedia, and peripheral capabilities that make them ideal for most mainstream business use:

- Flexible
 - Win32[®]-based application support
 - Extensive peripheral device support
- Connectivity
 - Citrix XenApp Plugin for Hosted Apps, Microsoft Remote Desktop Protocol (RDP), VMware View Client, HP Session Allocation Client, HP Remote Graphics, and HP TeamTalk
- User interface similar to familiar Windows XP Professional
- Improved security
 - Symantec EndPoint Protection Firewall
 - Microsoft Firewall (Add-on)
 - Locked down protected Flash drive
- Multimedia
 - Windows Media[®] Player
 - Windows Musical Instrument Device Interface (MIDI) (Add-on)
- Internet browsing
 - Windows Internet Explorer[®]
 - Adobe Acrobat[®] (Add-on)
- Extensive MUI support: English, French, German, Spanish, Dutch, Norwegian, Traditional Chinese, Simplified Chinese, Korean, and Japanese

HP provides this client “ready to go” out of the box to meet most common customer requirements. You may want to add/remove features using the Add or Remove programs control panel applet or the add-ons provided on the HP support site, and customize it to specific needs.

This guide will introduce you to the features of this client that are not found in the standard Microsoft Windows XP operating system.


Typically, a terminal is configured locally then used as a template for other terminals, which are then configured using local or remote administration tools.

The Desktop

This section provides a general overview of WES and XPe user and administrator desktop features and functions.

User Desktop


The desktop that displays when you are logged on as a user is a standard WES or XPe desktop, with the exception that the only icons displayed are for the Citrix Program Neighborhood, Microsoft RDP, and Internet Explorer. These selections are also available from the Start menu. You can open the terminal emulator application (HP TeemTalk) from **Start > Programs > Hewlett-Packard**.

 **NOTE:** Links to remote Citrix published applications may also be configured to be listed on the Start menu and/or displayed as icons on the desktop. Refer to the Citrix documentation for information and instructions.

For information about the functionality of the standard WES or XPe desktop and Start menu items, refer to the applicable Microsoft documentation: .

- WES—<http://msdn.microsoft.com/en-us/embedded/bb981920.aspx0.aspx>
- XPe—<http://msdn2.microsoft.com/en-us/embedded/aa731409.aspx>

For information on the Citrix Program Neighborhood or Citrix XenApp, please visit <http://www.citrix.com>.

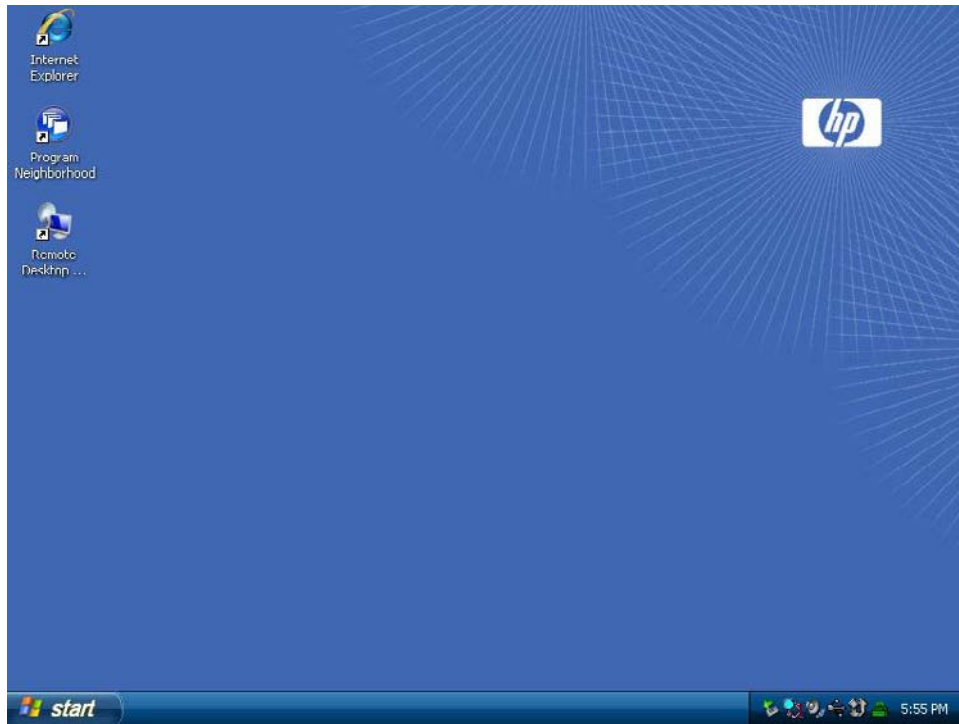
 **NOTE:** The Control Panel, available by clicking **Start > Control Panel**, provides access to a limited set of resources for changing WES or XPe user preferences. You must log on as Administrator to access the extended set of Control Panel options and utilities.


Right-clicking the mouse when the pointer is on a user's desktop background does not open a pop-up menu.

Administrator Desktop

The desktop that displays when you are logged on as an administrator is a standard Windows XP desktop. Icons present on the default administrator desktop Start menu include:

- Citrix Program Neighborhood
- Microsoft RDP
- Internet Explorer



 **NOTE:** Right-clicking the mouse when the pointer is on the administrator's desktop background opens a pop-up menu.

Server Environment Requirements

HP thin clients use a variety of services accessed through a network. These services include session and product support services as well as standard network services such as DHCP and DNS. Thin clients require the following

- Session services
- Support services

Session Services

The network to which the thin client is connected requires any of the following session services:

- Citrix ICA
- Microsoft RDP
- Terminal emulation support


Citrix ICA

You can make Citrix Independent Computing Architecture (ICA) available on the network using Presentation Server and/or XenApp for Microsoft Windows 2000/2003/2008 Server family.

Microsoft RDP

The Terminal Services Client application on the thin client accesses Microsoft Terminal Services. You can make Microsoft RDP available on the network using any of the following services:

- Microsoft Windows 2000/2003/2008 Server with Terminal Services installed
- Microsoft Windows Server 2000/2003/2008

 **NOTE:** If a Windows 2000/2003/2008 Server is used for both of these session services (ICA and RDP), a Terminal Services Client Access Licenses (TSCAL) server must also reside somewhere on the network. Client Access licenses permit clients to use the terminal, file, print, and other network services provided by Windows 2000/2003/2008 Server. The server grants temporary licenses (on an individual device basis) that are good for 90 days. Beyond that, you must purchase TSCALs and install them in the TSCAL server. You cannot make a connection without a temporary or permanent license.

For additional information about Microsoft Terminal Services, see the Microsoft Web site at <http://www.microsoft.com/windows2000/technologies/terminal/default.asp000/technologies/terminal/default.asp>.

Terminal Emulation Support

All WES- or XPe-based thin client models include terminal emulation software to support computing on legacy platforms. The terminal emulation software uses the Telnet protocol to communicate with the computing platform.

Support Services

Altiris Deployment Server

The Altiris Deployment Solution™ support service is available for the thin client network. This service provides an easy-to-use, integrated tool that allows remote management of thin clients throughout their life cycle, including initial deployment, ongoing management, and software deployment.

You must install the Altiris Deployment Solution on a Windows 2000/2003/2008 Server, or a workstation capable of logging on as administrator to a domain that provides specified network services which can access a software repository for the thin client. The Altiris Deployment Solutions software uses a Preboot Execution Environment (PXE) session and protocol to reimagine or recover the thin client. PXE upgrade services are built into the Altiris Deployment Solution.

For additional information about the Altiris Deployment Solution, refer to the Altiris Web site at <http://www.altiris.com/Support/Documentation.aspx> and review the *Altiris Deployment Solution User Guide*.

HP Device Manager

HP Device Manager is a thin client focused management tool that is easy to install and use. HP Device Manager is similar to Altiris and offers many of the same capabilities for managing thin clients. HP Device Manager, along with Altiris is a key part to HP overall manageability offering, which focuses on allowing the customer to choose the management tool that is most applicable to their environment.

3 Configuration


Logging On

You can log on to the thin client either automatically or manually.

Automatic Logon

The default for the WES- or XPe-based thin client is automatic logon. The administrator can use the HP Windows Logon Configuration Manager in the Control Panel to enable/disable auto logon and change the auto logon user name, password, and domain. Only the administrator account can change auto logon properties.



 **NOTE:** To save changes, be sure to disable the write filter cache or right-click on the green write filter icon and choose **commit** anytime during the current boot session. See [Enhanced Write Filter Manager on page 36](#) for information about and instructions for disabling the write filter. Enable the write filter when you no longer want permanent changes.

Enabling automatic logon bypasses the Log On to Windows dialog box. To log on as a different user while auto logon is enabled, press and hold **Shift** while clicking **Start > Shut Down > Log Off**. This displays the Log On to Windows dialog box and allows you to type in the logon information.

Manual Logon

When automatic logon is disabled, thin client startup displays the Log On to Windows dialog box. Type the logon information in the **User Name** and **Password** text boxes. Note the following:


- For a user account, the factory-default user name and password are both **User**.
- For an administrator account, the factory-default user name and password are both **Administrator**.
- For security purposes, HP recommends that you change the passwords from their default values. An administrator can change passwords by pressing **Ctrl+Alt+Del** to open the **Windows Security** dialog box, and then selecting **Change Password**. You cannot change the password when logged on as a user.
- Passwords are case-sensitive, but user names are not.
- The administrator may create additional user accounts using the **User Manager** utility available in the **Administrative Tools** option in Control Panel. However, due to local memory constraints, you should keep the number of additional users to a minimum. For more information, see [User Accounts on page 11](#).

Administrator Logon Access

To access Administrator logon regardless of the state of the thin client user mode:

- ▲ While holding down **Shift**, click **Start > Shut Down**. Still holding down **Shift**, from the **Shut Down** dialog box, select **Log Off**, and then click **OK**.

The screen for Administrator logon is displayed.

 **NOTE:** The default username and password for the Administrator account is **Administrator**. The default user name and password for the User account is **User**.

You can use the HP Windows Logon Configuration Manager to permanently modify the default login user. Located in the Control Panel, only the Administrator can access this application.

Logging Off, Restarting, and Shutting Down the Thin Client

To restart, shut down, or log off from the thin client, click **Start > Shut Down**. From the **Shut Down** dialog box, select the desired action, and then click **OK**.



NOTE: You may also log off or shut down using the Windows Security dialog box. Press **Ctrl+Alt+Del** to open the dialog box.

If automatic logon is enabled, when you log off (without shutting down), the thin client immediately logs on the default user set up in Windows Login Configuration. For instructions for logging on as a different user, see [Logging On on page 6](#).

The following utilities are affected by logging off, restarting, or shutting down the thin client:

- Enhanced Writer Filter
- Power Management
- System Time

Enhanced Write Filter

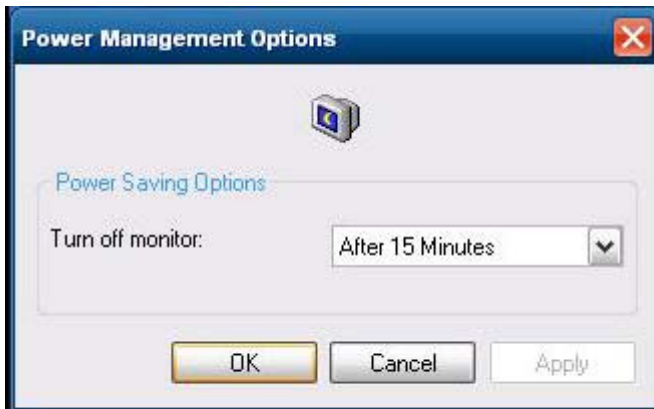
For detailed information about the Enhanced Write Filter, see [Enhanced Write Filter Manager on page 36](#). If you want to save changes to system configuration settings, you must disable the write filter cache or issue the `-commit` command during the current boot session. Otherwise, the new settings will be lost when the thin client is shut down or restarted. Enable the write filter when you no longer want to make permanent changes

The write filter cache contents are not lost when you log off and on again (as the same or different user). You may disable the write filter cache after the new logon and still retain the changes.

Only the administrator has write filter disabling privileges.

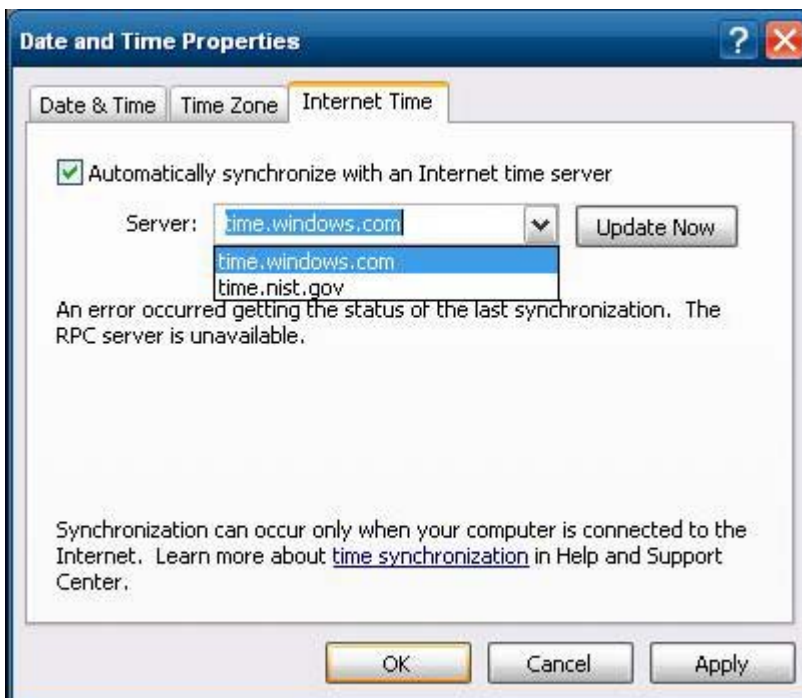
Power Management


A “Monitor Saver” turns off the video signal to the monitor after a designated idle time, allowing the monitor to enter a power-saving mode. To set power saving options for the monitor, right-click the desktop background and select **Properties** > **Screen Saver** > **Power**.



System Time

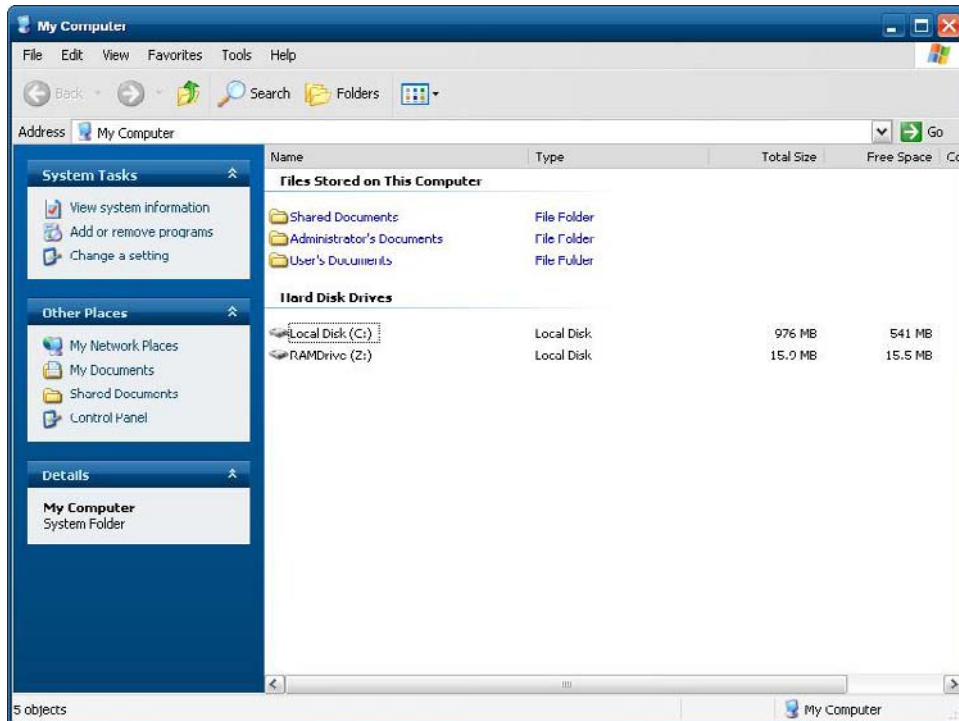
After power off, clock time is not lost as long as the power source remains plugged in. You can manually set the local time, or you can automatically set the local time utility to synchronize the thin client clock to a time server at a designated time.



 **NOTE:** The Windows Time service is Stopped by default. You can Start the service via the administrative tools control panel applet. You may want to Start the service and maintain correct time because some applications may require access to the local thin client time. To open the Date and Time Properties dialog, click on the time area in the task bar or double-click the **Date and Time** icon in the Control Panel.

Local Drives

The following sections describe the local drives located on the thin client.




Drive Z

Drive Z is the onboard volatile memory (MS-RAMDRIVE) on the logic board of the thin client. Because drive Z is volatile memory, HP recommends that you do not use this drive to save data that you want to retain. For RAMDisk configuration instructions, see [HP RAMDisk on page 39](#). For information about using the Z drive for roaming profiles, see [Roaming Profiles on page 11](#).

Drive C and Flash

Drive C is in the onboard flash drive. HP recommends that you do not write to drive C, as writing to drive C reduces the free space on the flash.

 **CAUTION:** If the available free space on the flash drive is reduced to below 10 MB, the thin client becomes unstable.

A write filter is used by the thin client for security and to prevent excessive flash write activity. Changes to the thin client configuration are lost when the thin client is restarted unless the write filter cache is disabled or a `-commit` command is issued during the current boot session. See the write filter topics in [Enhanced Write Filter Manager on page 36](#) for instructions to disable the cache. Enable the write filter when you no longer want permanent changes.

Saving Files

- △ **CAUTION:** The thin client uses an embedded operating system with a fixed amount of flash memory. HP recommends that you save files that you want to retain on a server rather than on the thin client. Be careful of application settings that write to the C drive, which resides in flash memory (in particular, many applications by default write cache files to the C drive on the local system). If you must write to a local drive, change the application settings to use the Z drive. To minimize writing to the C drive, update configuration settings as described in [User Accountson page 11](#).

Mapping Network Drives

You can map network drives if you log on as Administrator.

To keep the mappings after the thin client is rebooted:


1. Disable the write filter cache during the current boot session or issue the `-commit` command.
2. Select **Reconnect at Logon**.

Because a user logon cannot disable the write filter cache, you can retain the mappings by logging off the user (do not shut down or restart) and logging back on as Administrator, and then disabling the write filter.

You can also assign the remote home directory by using a user manager utility.

Roaming Profiles

Write roaming profiles to the C drive. The profiles need to be limited in size and will not be retained when the thin client is rebooted.

-  **NOTE:** For roaming profiles to work and be downloaded, there must be sufficient flash space available. In some cases it may be necessary to remove software components to free up space for roaming profiles.

User Accounts

This section describes how to create a new user account and user profile

Creating a New User Account

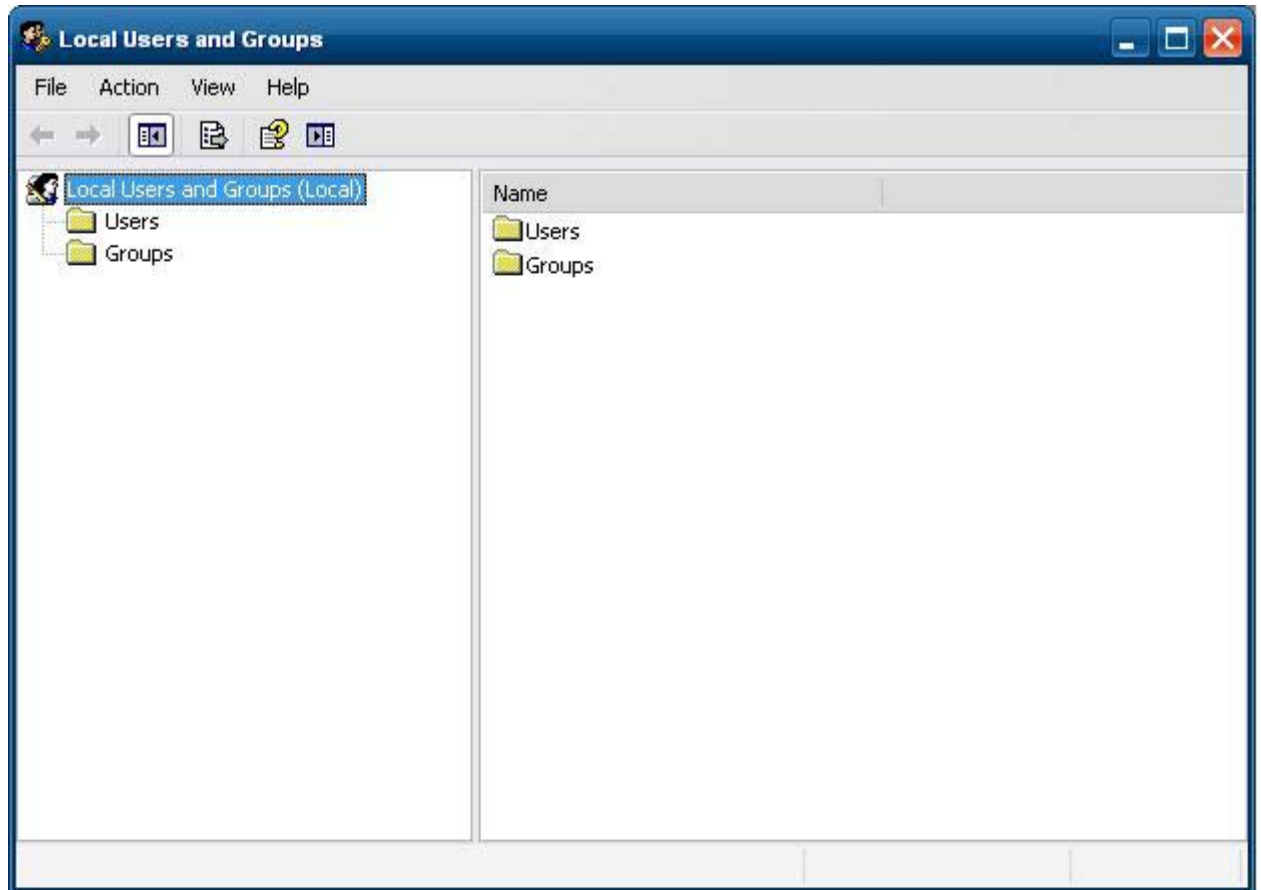
- △ **CAUTION:** Make sure to disable the write filter cache during the boot session in which a new account is created. Remember to enable the write filter after saving all of the permanent changes to flash.

You must log on as Administrator to create user accounts locally or remotely. Due to local flash/disk space constraints, you should keep the number of additional users to a minimum.

Use the User Manager utility to create new user accounts. To access this utility, click **Control Panel > Administrative Tools**.

User Manager

User Manager is a utility that allows the administrator to create, delete, and maintain user accounts.



User Profiles

A new user's profile is based on the Default User profile template, which includes policies similar to the factory-defined User account. This new account will default to membership within the local Users group. If the Default User profile settings are changed from those set at the factory, the changed settings are automatically applied to any newly user profile—local or domain. Any local accounts created or cached domain accounts logged into this device prior to changes made to the Default User profile are unaffected by these changes—only accounts logged in or cached after the changes.

For a new user to match the characteristics of the pre-defined User account, the Administrator must add the new user to the Power Users group; otherwise the new user will not be able to add a local printer. The user's actions are still limited while the user is in the Power Users group.

To create the user:

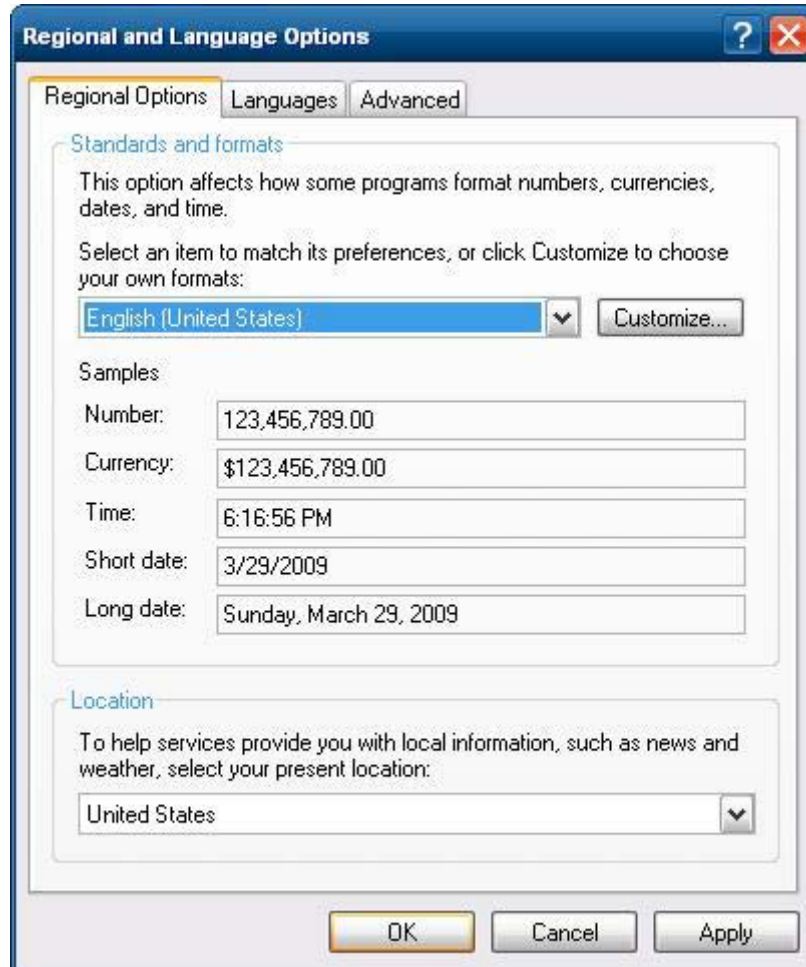
△ **CAUTION:** Because of the limited size of flash memory, HP strongly recommends that you configure other applications available to the new and existing users to prevent writing to the local file system. For the same reason, HP also recommends that you exercise extreme care when changing configuration settings of the factory-installed applications.

1. Log in as Administrator.
2. Open the **Administrative Tools** window by clicking **Start > Control Panel > Administrative Tools**.
3. Double-click **User Manager** to open the **Local Users and Groups** window.
4. Double-click the **Users** folder to view the contents in the right pane.
5. Click **Action** in the menu bar, and then select **New User**. This opens the **New User** dialog box.
6. Type in the user name and password, and then select the attributes you want.
7. Click **Create**, and then click **Close**.
8. In the **Local Users and Groups** window, select the **Users** folder in the left pane.
9. In the right pane, double-click the name of the user just created. This opens the **[user name] Properties** tabbed dialog box.
10. Open the **Member Of** tab dialog.
11. Click **Add**. This opens the **Select Groups** dialog box.
12. Type `Power Users` in the **Enter the Object Names to Select** field. This enables the **Check Names** command button.
13. Click **Check Names**, and then click **OK**.

The newly created user is now a member of both the Power Users and Users groups and should match the privileges of the default user account.

Regional and Language Options

The keyboard language options are preset at the factory. Should you need to make a change, the keyboard language selection is made through the Regional and Language Options selection in the Control Panel. From this program you can select the type of keyboard you are using as well as the layout/IME settings.



Administrative Tools

Click the **Administrative Tools** icon in the **Control Panel** to gain access to the available administrative tools:



4 Applications

The latest WES and XPe images have the following preinstalled applications:

- [Symantec Endpoint Protection Firewall on page 17](#)
- [Microsoft Windows Firewall on page 18](#)
- [Citrix Program Neighborhood and PN Agent on page 24](#)
- [Remote Desktop Connection on page 25](#)
- [HP Remote Desktop Protocol \(RDP\) Multimedia and USB Enhancements on page 27](#)
- [HP Remote Graphics Software \(RGS\) Receiver on page 27](#)
- [HP Session Allocation Manager \(SAM\) Client on page 28](#)
- [Teemtalk Terminal Emulation on page 29](#)
- [VMWare View Manager on page 29](#)
- [Altiris Client Agent on page 30](#)
- [HP Management Agent on page 32](#)
- [HP Client Automation Registration and Agent Loading Facility \(RALF\) on page 32](#)
- [Microsoft Internet Explorer on page 33](#)
- [Windows Media Player 11 on page 33](#)

Access to the following applications is available to all users logon accounts:

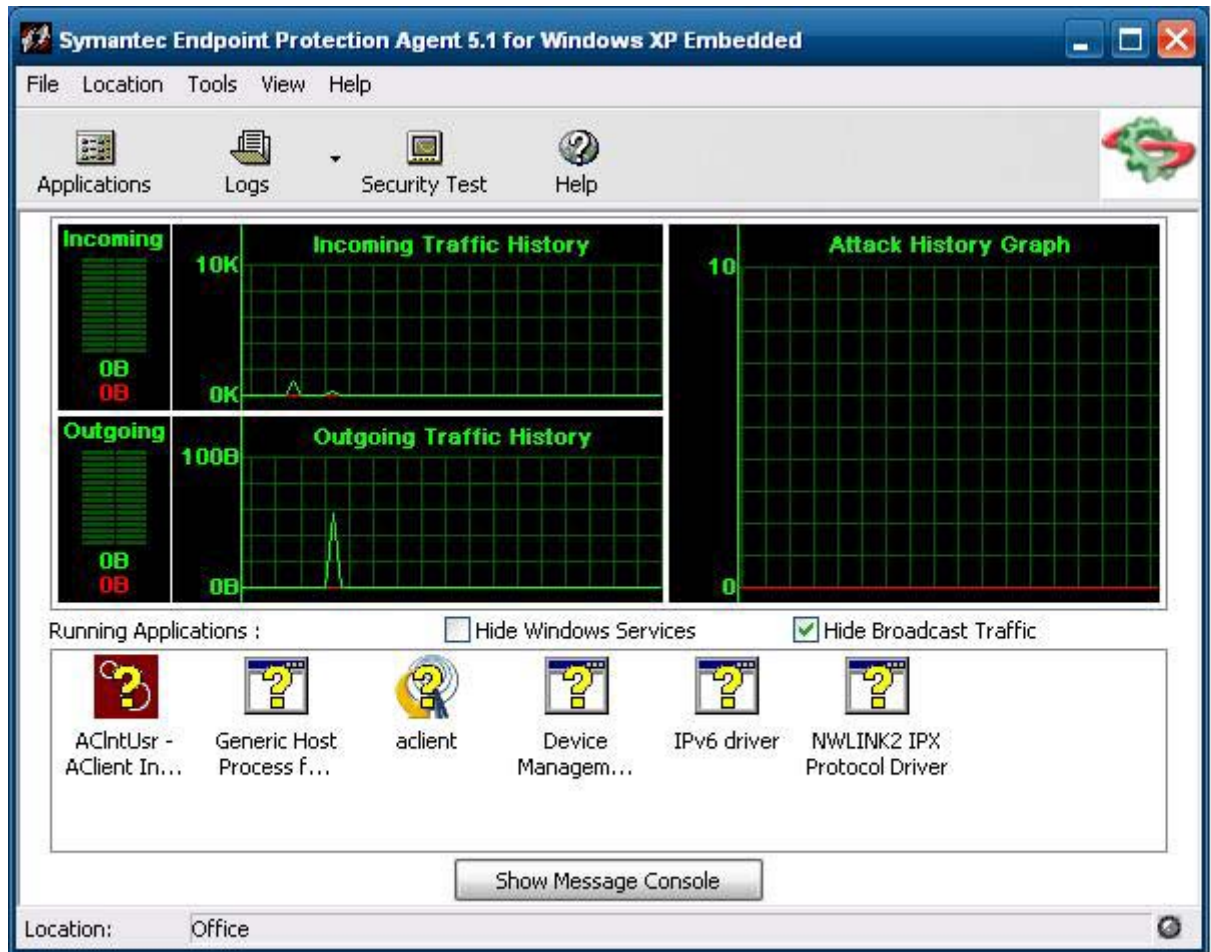
- [Symantec Endpoint Protection Firewall on page 17](#)
- [Altiris Client Agent on page 30](#)

Additional applications in the form of add-ons are provided and can be downloaded from the HP Web site.

Check the HP support site for these applications or for other important updates or documentation: <http://www.hp.com/support>. Select the country from the map, then select **See support and troubleshooting information** or **Download drivers and software (and firmware)**. Type the thin client model in the field and click [Enter](#).

Symantec Endpoint Protection Firewall

The HP image includes a Symantec Endpoint Protection Agent Firewall.



About the Agent

The Symantec Endpoint Protection for Windows XPe Agent is security software that is installed on embedded endpoints, such as HP thin clients, that run the WES or XPe operating system.

The agent provides a customizable firewall that protects the endpoint from intrusion and misuse, whether malicious or unintentional. It detects and identifies known Trojan horses, port scans, and other common attacks. In response, it selectively allows or blocks traffic, or various networking services, applications, ports, and components.

The agent uses security policies, which include firewall rules, as well as security settings. These policies protect an individual endpoint from network traffic and the viruses that can cause harm. Firewall rules determine whether the endpoint allows or blocks an incoming or outgoing application or service from gaining access through the network connection. Firewall rules allow the agent to systematically allow or block incoming or outgoing applications and traffic from or to specific IP addresses and ports. Security settings detect and identify common attacks, send e-mail messages after an attack, display customizable messages, and accomplish other related security tasks. Security policies, advanced rules,

security settings, as well as IPS engine settings have been customized by HP to provide both optimal performance as well as a secure computing environment.

New Features and Functionality

- All user accounts can now modify SEP Agent options and settings. Previously the Sygate Agent only granted the Administrator account this ability. User access to firewall settings may now be restricted by configuring an agent password.
- Updated command line management options and rules interface replace the legacy Sygate Policy Editor. Rules and policy changes that would have previously required a stand-alone policy editor may now be made within the agent interface then exported/imported using new command line options. A stand-alone policy editor will not be made available for SEP.

Additional information about the Symantec SEP Firewall is available in the *Symantec™ Endpoint Protection for Windows® Embedded Standard 2009 (WES) and Windows XP Embedded (XPe) User Guide* at: <http://www.hp.com/support>. Select the country from the map, then click **See support and troubleshooting information**. Type the thin client model in the field and click **Enter**.

Microsoft Windows Firewall

An improved Microsoft Windows Firewall (previously known as Internet Connection Firewall, or ICF) is available from HP as an add-on. The firewall is enabled by default after you install the add-on.

On-by-Default

After you install the add-on, Windows Firewall is turned on by default for all network interfaces. On-by-default also protects new network connections as they are added to the system. This could break application compatibility if the application by default does not work with stateful filtering.


Configuring Microsoft Windows Firewall

To provide the best security and usability, Windows Firewall provides the ability to add exceptions for applications and services so that they can receive inbound traffic.

To configure Windows Firewall, open the firewall from **Control Panel**. You can also access the firewall configuration from the **Advanced** tab in **Network Connection** properties.

Security Center is not in the image. Once you apply the Windows Firewall, the FIREWALL.CPL control panel applet is only available for the Administrator account.



 **NOTE:** After you launch the Windows Firewall add-on, the Control Panel applet is only available to the Administrator account.

- **General Tab:** The **General** tab provides access to the main three configuration options as shown below.
 - On (Recommended)
 - Don't allow exceptions
 - Off (Not Recommended)

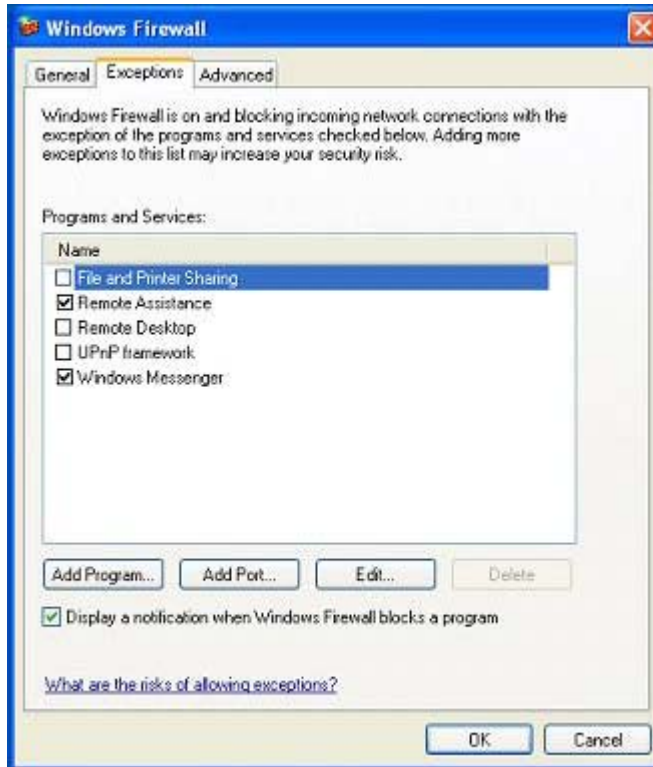
When you select **Don't allow exceptions**, Windows Firewall blocks all requests to connect to the computer, including those from programs or services on the **Exceptions** tab. The firewall also blocks file and printer sharing and discovery of network devices

Using Windows Firewall with no exceptions is useful when connecting to a public network. This setting can help to protect the computer by blocking all attempts to connect to the computer. When you use Windows Firewall with no exceptions, you can still view Web pages, send and receive e-mail, or use an instant messaging program.

- **Exceptions Tab:** Provides the ability to add program and port exceptions to permit certain types of inbound traffic. The exception settings specify the set of computers for which this port/program is open.

You can specify three different modes of access:

- Any computer (including those on the Internet)
- My network (subnet) only
- Custom list



Display a notification when the Windows Firewall blocks a program is selected by default.

You can set a scope for each exception. For home and small office networks, it is recommended that you set the scope to the local network only where possible. This will enable computers on the same subnet to connect to the program on the machine, but drops traffic originating from a remote network.

- **Advanced Tab:** Enables you to configure the following functions.
 - **Network Connection Settings:** Select connection-specific rules which apply per network interface.
 - **Security Logging:** Create a log file for troubleshooting.
 - **ICMP:** With Global Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.
 - **Default Settings:** Restore Windows Firewall to a default configuration.



Gathering Configuration Information

To examine the current policy configuration for Windows Firewall, you can use the following command: **netsh firewall show configuration**.

Troubleshooting Applications


Modifying an application to work with a stateful filtering firewall is the ideal way to resolve issues. This is not always possible, so the firewall provides an interface for configuring exceptions for ports and applications.

Failure Symptoms

Failures related to the default configuration will manifest in two ways:


- Client applications may fail to receive data from a server. Examples include an FTP client, multimedia streaming software, and new mail notifications in some e-mail applications.
- Server applications running on the WES- or XPe-based computer may not respond to client requests. Examples include a Web server such as Internet Information Services (IIS), Remote Desktop, and File Sharing.



 **NOTE:** Failures in network applications are not limited to firewall issues. RPC or DCOM security changes can cause failures. It is important to note whether the failure is accompanied by a Windows Firewall Security Alert indicating that an application is being blocked.

Resolution

With either of the failures mentioned above, you can add exceptions to the configuration for Windows Firewall. Exceptions configure the firewall to permit specific inbound connections to the computer.

 **NOTE:** HP recommends adding a program instead of adding a port. Adding a program is easier and safer than adding a port because you do not have to know which port numbers to use, and the port is only open when the program is waiting to receive a connection. Only the specified application can use the port, whereas opening a port allows any application to use it.

Adding a Program

The recommended configuration involves adding a program to the exception list. This solution provides the easiest configuration, as well as enables the firewall to open ranges of ports that can change each time the program runs.

To add a program exception:

1. Open **Windows Firewall** and select the **Exceptions** tab.
2. If the program is in the list, click to enable the setting. If the program is not in the list, click **Add Program** to display the **Add a Program** dialog box.
3. Click **Browse** to choose the program you wish to add as an exception, and then click **OK**.
4. Click **Change Scope** to view or set the scope for the program, and then click **OK**.
5. Click **OK** to close the **Add a Program** dialog box.
6. Click the check box to enable the program. By default, the program is not enabled in the list.

Adding a Port

If adding the program to the exception list does not resolve the application issue, you can add ports manually. You must first identify the ports used by the application. The most reliable method for determining port usage is consulting with the application vendor.

If the port number(s) for the process are less than 1024, it is likely that the port numbers will not change. If the port numbers used greater than 1024, the application may be using a range of ports, so opening individual ports may not resolve the issue reliably.

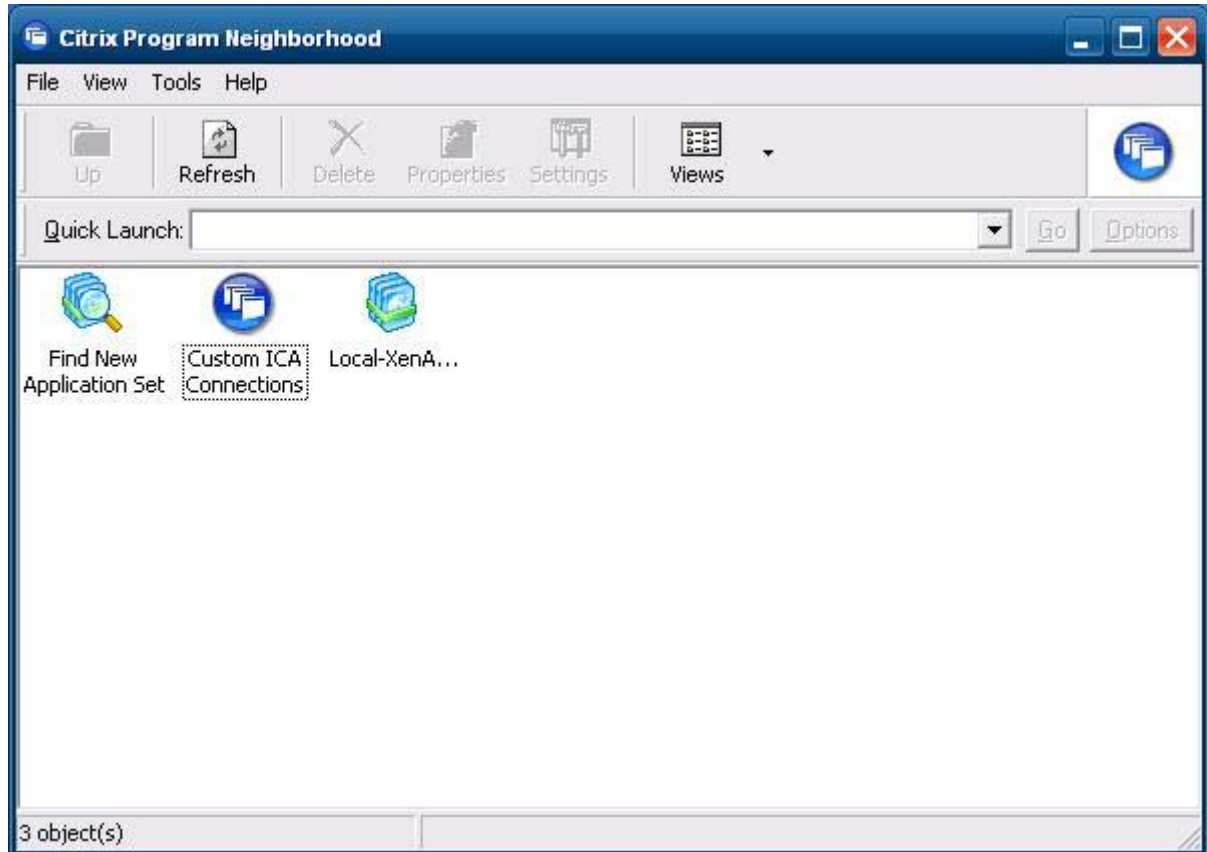
Once you have the port number and protocol, add an exception for that port.

To add a port exception:

1. Open **Windows Firewall** and click the **Exceptions** tab.
2. Click **Add Port** to display the **Add a Port** dialog box.
 - a. Type the **Port Number**.
 - b. Choose **TCP** or **UDP** protocol.
 - c. Give the port exception a descriptive name in the **Name** field.
3. Click **Change Scope** to view or set the scope for the port exception, and then click **OK**.
4. Click **OK** to close the **Add a Port** dialog box.
5. Click to enable the port.

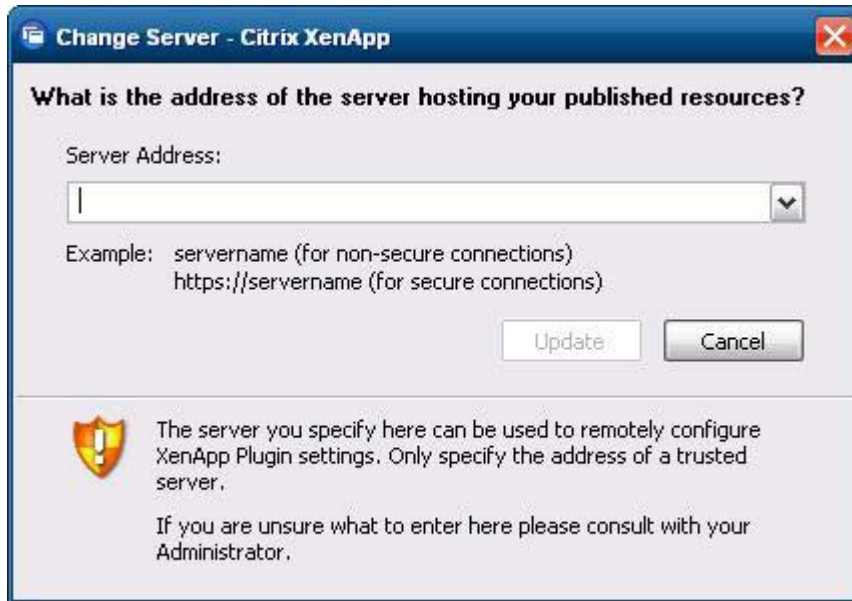
Citrix Program Neighborhood and PN Agent

Citrix Program Neighborhood is a feature of ICA introduced with MetaFrame 1.8 that enables users to connect to MetaFrame and WinFrame servers and published applications. Program Neighborhood allows complete administrative control over application access and delivers an even greater level of seamless desktop integration.



Alternatively, use PN Agent where Citrix Presentation Server or XenApp is deployed with Web Interface. PN Agent relies on a central configuration file on the Web Interface server. This client enables placing icons on the desktop or Start menu of the thin client for seamless integration of published applications.

PN Agent can be accessed and started through the Citrix folder in the Start menu.

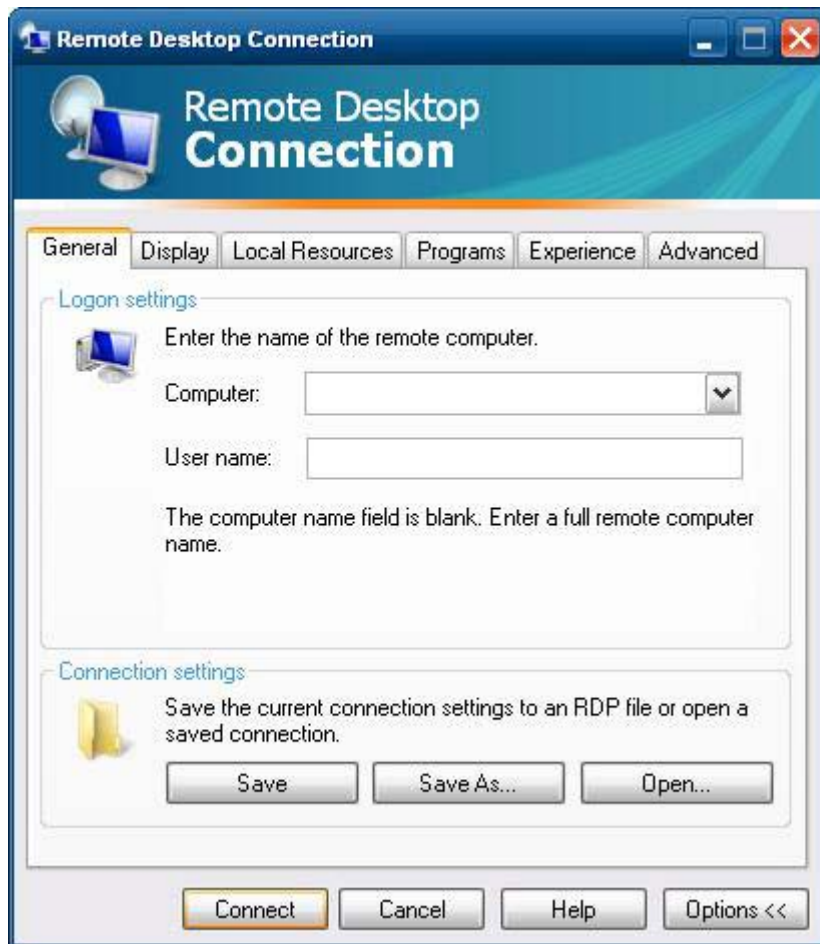


Documentation for the ICA client application is available from the Citrix Corporation Web site at www.citrix.com.

Remote Desktop Connection

Use the Remote Desktop Connection dialog box to establish connections to a Windows Terminal Server or to access remote applications using Microsoft RDP.

Refer to the Microsoft Web site for documentation that offers a detailed explanation and instructions on how to use the Microsoft RDC dialog box.



HP Remote Desktop Protocol (RDP) Multimedia and USB Enhancements

HP Remote Desktop Protocol (RDP) Multimedia and USB Enhancements software enhances your users' Microsoft Remote Desktop Protocol virtualization experience. HP Remote Desktop Protocol Enhancements provide users with a single-logon initiated, full-screen virtual desktop experience (including stereo audio). The client-side software, which is included in the latest WES and XPe images, works seamlessly. Users simply log in on the thin client to take advantage of its multimedia features, such as training videos, and USB device support. For additional information, visit <http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c01705352/c01705352.pdf/c01705352.pdf>.

HP Remote Graphics Software (RGS) Receiver

HP Remote Graphics Software (RGS) is a high-performance remote desktop connection protocol that delivers an exceptional remote desktop user experience for rich user environments that include video, web flash animations and graphics intensive applications. All applications run natively on the remote system and take full advantage of the compute and hardware graphics resources of the sending system.

HP RGS captures the desktop of the remote system and transmits it over a standard network to a window on a local client (a receiver) using advanced image compression technology specifically designed for text, digital imagery and high frame rate video applications. The receiver uses their keyboard, mouse, and USB devices to interact with applications just as if they were physically interacting with the sender system providing an interactive, high performance, multi-display desktop experience.

The RGS Receiver is included in the latest HP thin client WES and XPe image. Visit <http://www.hp.com/go/rgs> for information on RGS Sender Licensing, installation, and use.

HP Session Allocation Manager (SAM) Client

The Consolidated Client Infrastructure (CCI) solution from HP centralizes desktop computing and storage resources into easily managed, highly secure data centers, while providing end users the convenience and familiarity of a traditional desktop environment. Additionally, companies have long used server-based computing (SBC) to create virtual instances of desktop applications on a server that multiple remote users can access. HP CCI offers a new alternative for virtualizing the desktop.

Part of the CCI solution is the HP Session Allocation Manager (HP SAM) and is an extension the HP SAM client. HP SAM client is included in the latest HP Thin Client WES and XPe image, and can be accessed from **Start > Programs**.

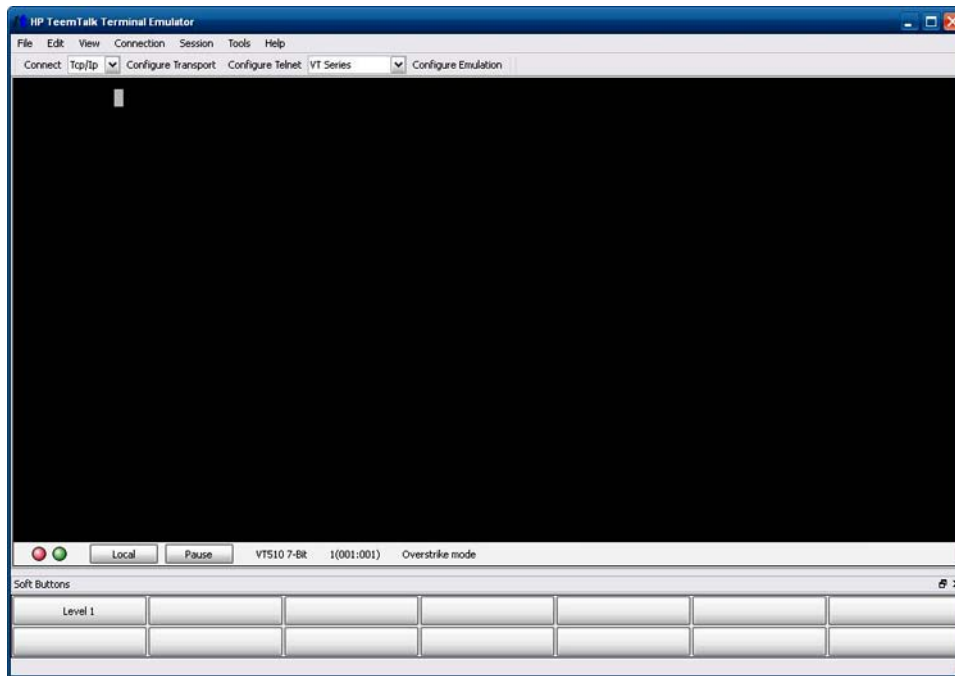


HP SAM becomes the control point in managing a CCI deployment. Specifically, it manages the assignment of Microsoft Remote Desktop connections from a user's access device (thin client) to Remote Desktop sessions (blade PCs). Whether the session resides on a dedicated physical blade or resides together with other sessions on a virtual hardware platform, the HP SAM system can make these desktop sessions available to users as they are needed.

For more information about HP SAM, see http://h71028.www7.hp.com/enterprise/cache/323204-0-0-225-121.html?jumpid=reg_R1002_USEN3204-0-0-225-121.html.

Teemtalk Terminal Emulation

All WES- or XPe-based thin client models include terminal emulation software to support computing on legacy platforms. The software uses the Telnet protocol to communicate with the computing platform. Refer to the terminal emulation documentation (supplied separately) for instructions. By default, you can access the Teemtalk Connection Wizard and the Teemtalk Emulator from **Start > All Programs**.



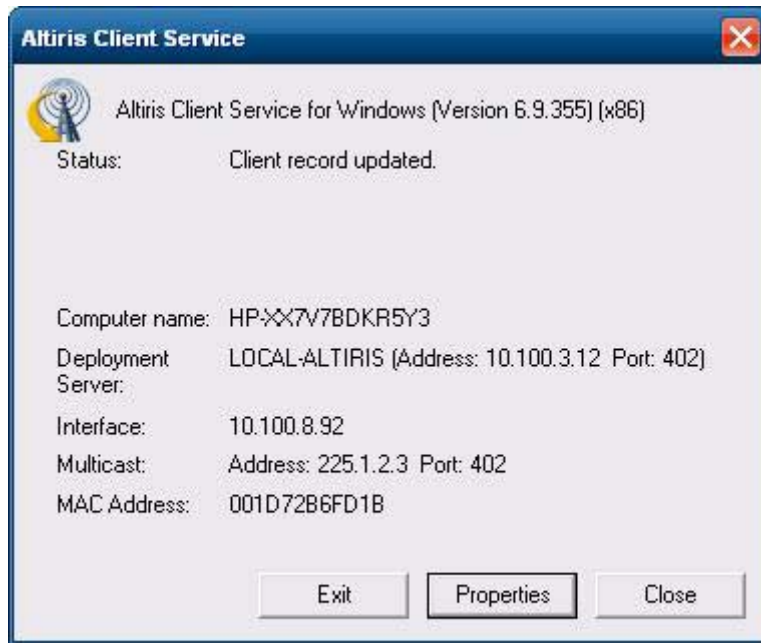
VMWare View Manager

View Manager, a key component of VMWare View, is an enterprise class desktop management solution, which streamlines the management, provisioning and deployment of virtual desktops. Users securely and easily access virtual desktops hosted on VMWare Infrastructure, terminal servers, blade PCs or even remote physical PCs through View Manager.

For additional information about VMWare View, see <http://www.vmware.com/products/view>.


Altiris Client Agent

The Altiris Client Agent allows the Altiris server to discover valid clients that are added to the network. The agent carries out assignments and reports the status of individual thin clients to the Altiris server.



Altiris Client Service Properties [X]

Server Connection | Access | Security | Log File | Proxy | Startup/Shutdown

 Connect directly to this Deployment Server

Address/Hostname: Port:

Enable key-based authentication to Deployment Server

Key file:

Deployment Agent will require a key file in order to connect to Deployment Server.

Discover Deployment Server using TCP/IP multicast

If no Deployment Server is specified, the Deployment Agent will connect to the first Deployment Server it finds.

Server Name: Port:

Multicast Address: TTL:

Refresh connection after idle

Abort file transfers if rate is slower than Kbps

OK Cancel

HP Management Agent

The HP Management Agent is a software component installed on thin client devices so that HP Device Manager can interact with them. The agent is embedded in the standard thin client WES and XPe image to enable Device Manager to manage devices out-of-the-box (agents on older devices, however, may need to be upgraded).

For additional information concerning the HP Device Manager and the HP Management Agent please check the HP support site for these applications or for other important updates or documentation: <http://www.hp.com/support>. Select the country from the map, then select **See support and troubleshooting information** or **Download drivers and software (and firmware)**. Type the thin client model in the field and click **Enter**.



HP Client Automation Registration and Agent Loading Facility (RALF)

RALF configuration and operation

RALF is shipped pre-installed on the latest HP thin client images (except those running ThinConnect). It is used to register with an HP Client Automation Server (HPCA) so that the full HPCA agent can be pushed down and therefore the thin client be managed by the HP Client Automation console. RALF is configured using a default HPCA Server hostname defined as 'hpcaserver.' While the HPCA server can be installed to match this name, it is more common to use this name as a DNS alias in defining the actual HPCA server host name. The HP Client Automation Standard, Starter, and Enterprise version 7.5 or greater have additional documentation on how RALF can also be re-configured to define a different hostname using the command line options. More information on HP Client Automation can be found at https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-271-272%5e9783_4000_100_&jumpid=go/clientautomation.

When RALF is installed, it runs as a Windows service or Linux daemon that periodically probes for the HPCA server. This probing continues for 24 hours, and then RALF will shut down. It starts this 24-hour

probe again upon reboot. Once the server is contacted, RALF registers the device with the HPCA infrastructure and waits to accept the request to install the HPCA agent. Once the HPDA agent is installed, RALF periodically contacts the server and verifies device registration attributes.

Microsoft Internet Explorer

Version 7.0 of the Microsoft Internet Explorer browser is installed locally on the thin client. The Internet options settings for the browser have been preselected at the factory to limit writing to the flash memory. These settings prevent exhaustion of the limited amount of flash memory available and should not be modified. You may access another browser through an ICA or RDP account if you need more browser resources.

Microsoft Internet Explorer 7.0 is much more secure. Internet Explorer has more control over the execution of all content, including a built-in facility to manage pop-up windows. Furthermore, Internet Explorer now prevents scripts from moving or resizing windows and status bars to hide them from view or obscure other windows.

A block unsafe file transfers feature is available with Internet Explorer 7. For a list of files generally considered unsafe, see *Information About the Unsafe File List in Internet Explorer 6* on the Microsoft Web site at <http://support.microsoft.com/kb/29136991369>.

Windows Media Player 11

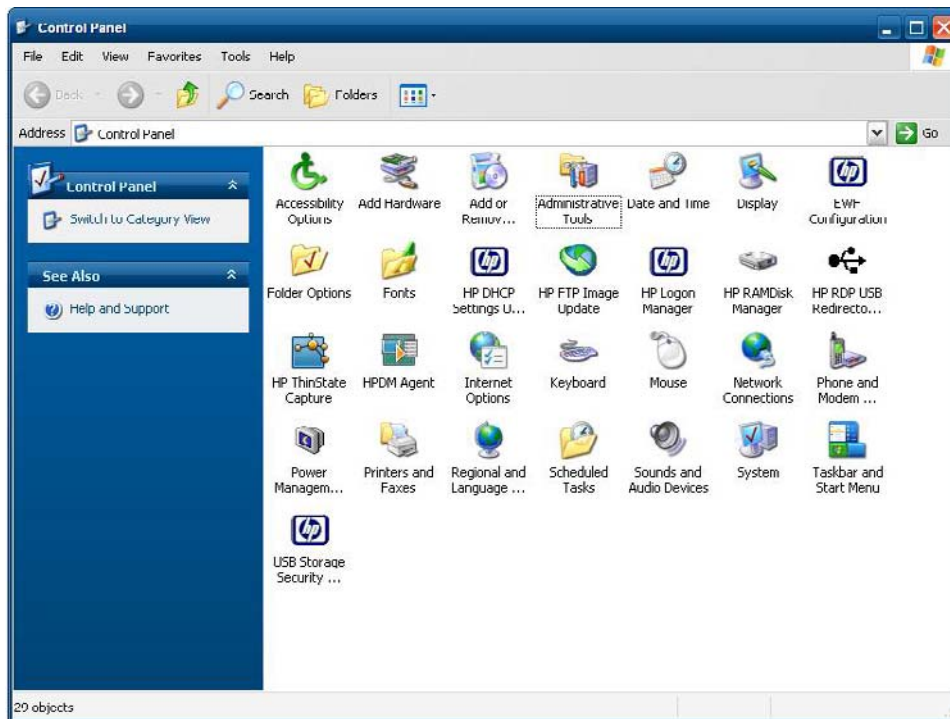
Version 11 of the Windows Media Player contains security, performance, and functionality improvements. For more information about improvements to Windows Media Player, refer to the Windows Media Player home page at <http://www.microsoft.com/windows/windowsmedia/player/11/default.aspx>.



5 Control Panel Extended Selections

The Control Panel is accessed by selecting **Start > Control Panel**.

Some of the extended selections available on the Control Panel are discussed in the following sections.



Enhanced Write Filter Manager

WES and XPe include the Enhanced Write Filter (EWF) console application command-line tool, Ewfmgr.exe. In addition to the DOS command-line tool, the WES and XPe images include an Enhanced Write Filter GUI. The EWF allows the operating system (OS) to boot from a disk volume residing on any read-only media or write-protected hard drive while appearing to have read/write access to the OS. The EWF saves all writes to another storage location called an overlay. Changes made to the overlay will not be committed to the flash memory unless the EWF has been disabled or the user performs an intentional commit.

The EWF manager console application can be used to issue a set of commands to the EWF driver, report the status of each protected volume overlay and report the format of the overall EWF configurations.

By including the EWF manager console application component in the configuration and building it into the run-time image, you enable the use of Ewfmgr.exe and the corresponding commands.

Benefits of the Enhanced Write Filter

The EWF provides a secure environment for thin client computing. It does this by protecting the thin client from undesired flash memory writes (flash memory is where the operating system and functional software components reside). The write filter also extends the life of the thin client by preventing excessive flash write activity. It gives the appearance of read-write access to the flash by employing a cache to intercept all flash writes and returning success to the process that requested the I/O.

The intercepted flash writes stored in cache are available as long as the thin client remains active, but will be lost when the thin client is rebooted or shut down. To preserve the results of writes to the registry, favorites, cookies, and so forth, the contents of the cache can be transferred to the flash on demand by the Altiris Deployment Solution software or manually using the Enhanced Write Filter Manager.




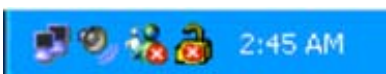
After the write filter has been disabled, all future writes during the current boot session are written to the flash, with no further caching until a reboot occurs. The write filter may also be enabled/disabled through the command line. Always enable the writer filter after all of the permanent changes have been successfully made.


The EWF is a powerful tool for any thin client environment in which multiple users have access to the device. The EWF prevents unauthorized users from altering or damaging the image.

Enhanced Write Filter Status Service


This service creates an icon in the System Tray that shows the status of EWF. The EWF Status icon will appear as a red 'lock' when disabled, a green 'lock' when enabled, and a yellow 'lock' when the state is set to change on the next boot.



Status	Description	Example
Red	Disabled	
Green	Enabled	
Yellow	Commit Mode	
Yellow with Red 'X'	Write Filter Corrupted	

 **NOTE:** In the event of a corrupted EWF state, you will need to re-flash the thin client unit with the standard shipping image provided on the web.

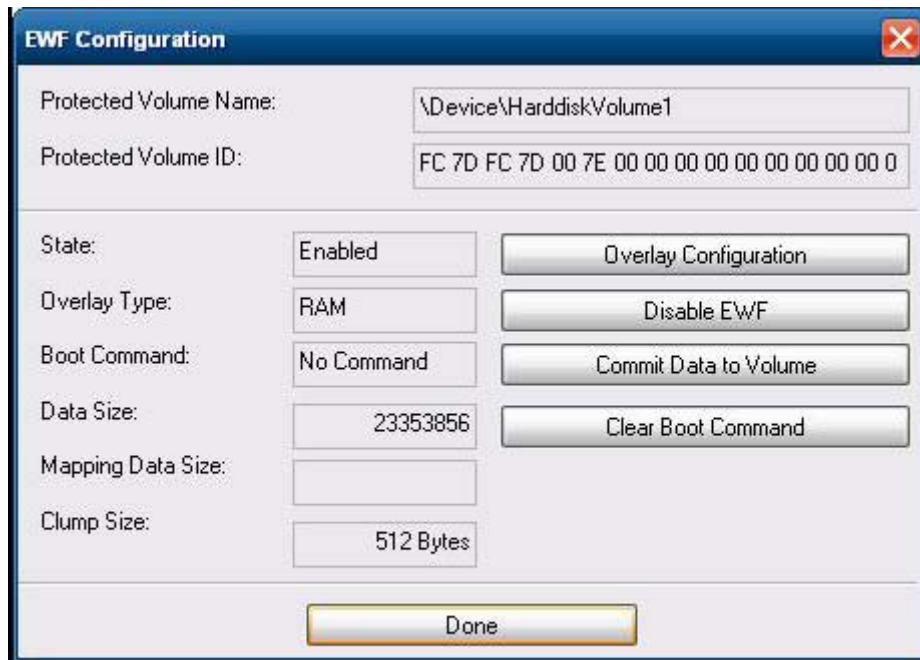
If you are logged-on as Administrator, you can change the status of EWF by right-clicking on the icon and selecting the desired EWF state.

 **NOTE:** Since EWF Manager console utility (ewfmgr.exe) and the EWF status service execute separate code, any status changes by ewfmgr.exe will not be automatically reflected by the EWF status icon.

To refresh the status icon after modifying EWF through ewfmgr.exe, you must right-click on the icon (you can then click anywhere on the screen to close the context menu). However, any operations made through the EWF status icon menu will be visible through the EWF Manager console application. Status and changes to the Enhanced Write Filter will be synchronized between the EWF status icon and the EWF Manager Control Panel applet.

Enhanced Write Filter GUI

The EWF GUI can be accessed through the Control Panel or the Administrative Tools option for the administrator.




To access the EWF GUI, perform the following steps:

1. Log in as an administrator.
2. Select **Start > Control Panel > Other Control Panel Options** or **Start > Control Panel > Administrative Tools**.
3. Click the **EWF Manager** icon.
4. Use the EWF GUI to select the Write Filter options.

EWF GUI Buttons

The current version of the EWF GUI includes the following buttons:


Button	Description
Enable EWF	This button is the same as executing ewfmgr.exe c: -Enable from the DOS prompt.
Disable EWF	This button is the same as executing ewfmgr.exe c: -Disable from the DOS prompt.
Overlay Configuration	This button simply displays the Overlay information and is a combination of the information supplied when executing ewfmgr.exe c: -Description and ewfmgr.exe c: -Gauge from the DOS prompt.
Clear Boot Command	This button is the same as executing ewfmgr.exe c: -NoCmd from the DOS prompt.
Commit Data to Volume	This button is the same as executing ewfmgr.exe c: -Commit from the DOS prompt.

 **NOTE:** When using the Commit boot command, all the temporary contents will be permanently written to the flash memory. In addition, all content accessed (and changes made) after running Commit, but before rebooting the system, will be written to the flash memory as well. This includes changes made during any number of login/logout sessions before the next reboot.

DOS Command-line Tool Boot Commands

The following table lists the EWF boot commands that are supported.


Boot Command	Description
All	Displays information about all protected volumes and performs a command, such as disable , enable , and commit , on each volume if specified.
Commit	Commits all current level data in the overlay to the protected volume, and resets the current overlay level to 1 upon shutdown.
Disable	Allows user to write to the image after the next reboot.
Enable	Prevents the user from writing to the image after the next reboot.
Commitanddisable	Combination of the Commit and Disable commands. This command will commit data in the overlay upon shutdown. Additionally, EWF will be disabled after the system reboots.

 **NOTE:** When using the Commit boot command, all the temporary contents will be permanently written to the flash memory. In addition, all content accessed (and changes made) after running Commit, but before rebooting the system, will be written to the flash memory as well. This includes changes made during any number of login/logout sessions before the next reboot.

Using Boot Commands

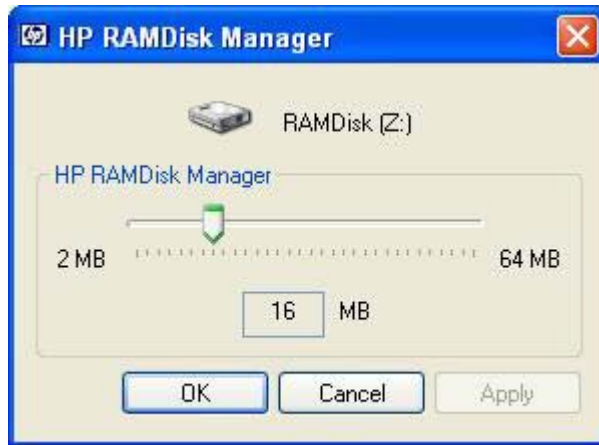
To use the EWF manager boot commands, type the following syntax in a command prompt:

```
EWMGR <drive-letter> -[boot command].
```

 **NOTE:** Because the EWF manager commands are executed on the next boot, you must reboot the system for the command to take effect.

HP RAMDisk

The RAMDisk is volatile memory space set aside for temporary data storage. It is the Z drive shown in the My Computer window.




The following items are stored on the RAMDisk:

- Browser Web page cache
- Browser history
- Browser cookies
- Browser cache
- Temporary Internet files
- Print spooling
- User/system temporary files

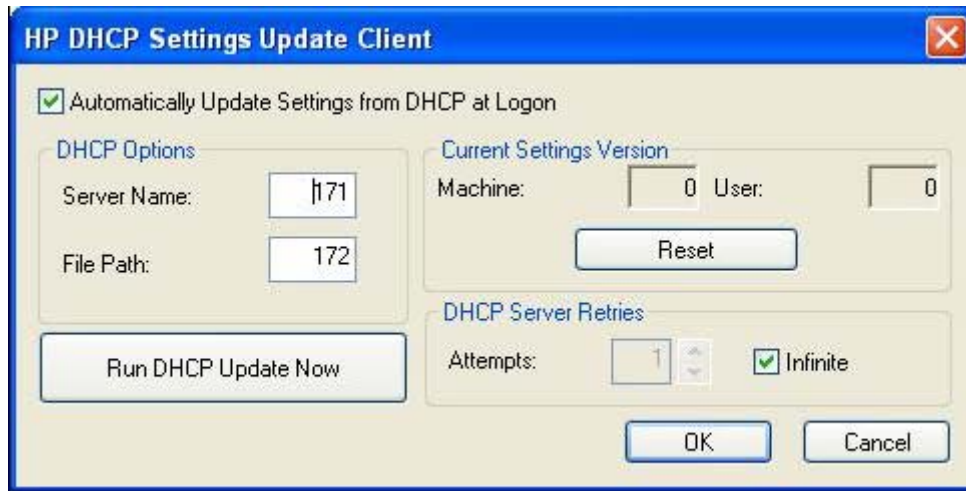
You can also use the RAMDisk for temporary storage of other data (such as roaming profiles) at the administrator's discretion (see [Local Drives on page 10](#)).

Use the RAMDisk Configuration dialog box to configure the RAMDisk size. If you change the size of the RAMDisk, you will be prompted to restart for changes to take effect. To permanently save the change, make sure to disable the write filter cache or to issue the `-commit` command during the current boot session before restarting.

 **NOTE:** The default optimal RAMDisk size is set to 16 MB. The maximum RAMDisk size that you can set is 64 MB. The minimum is 2 MB.

HP DHCP Settings Update Client

The HP DHCP Settings Update Client is a utility found in the Control Panel that allows an IT Administrator to apply some settings to an HP WES or XPe operating system.



The settings are applied through an .INI file that uses a subset of parameters from Microsoft's sysprep.inf as well as several XPe/HP-specific keys. XPePrep can run by specifying a local .INI file to be processed, or it can be used in conjunction with DHCP and FTP servers to automatically apply settings across multiple clients on a network.

For detailed information, please review the *Using the HP DHCP Settings Update Client* document on the HP support site at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01444724/c01444724.pdf?jumpid=reg_R1002_USEN4/c01444724.pdf.

HP ThinState Capture

The HP ThinState Capture tool is a very simple wizard-based tool that you can use to capture an HP thin client WES or XPe image, which you can then deploy to another HP thin client of identical model and hardware.

What do you need to have?

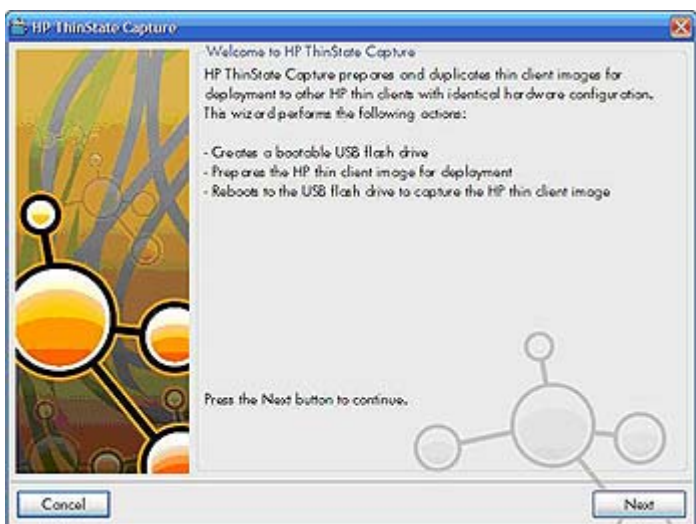
- An HP WES- or XPe-based thin client that contains the latest HP provided image
- An HP-approved USB flash drive (Disk-On-Key). Consult the t5630 quick specs for the latest approved USB flash drives.

WARNING! By default, the First Boot Device in the F10 System BIOS is first set to USB, then ATA Flash, and finally to Network boot. If the default Boot order settings have been changed, it is critical before using the HP ThinState Capture tool that you first set the First Boot Device in the Advanced BIOS Features section of the F10 System BIOS to USB.

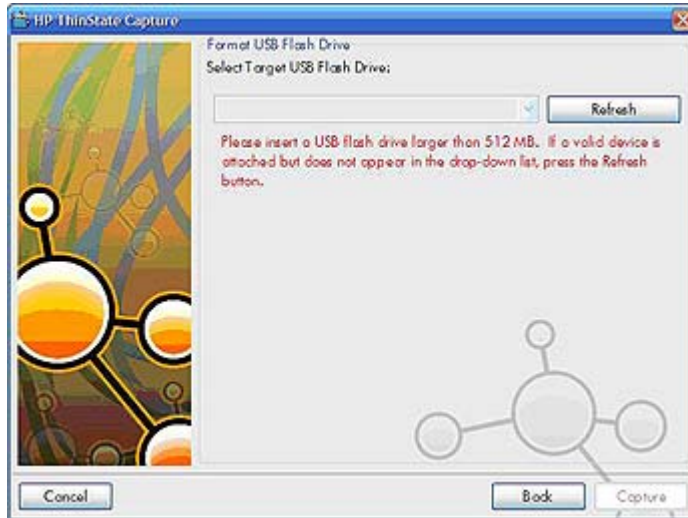
NOTE: The HP ThinState Capture tool is not a standalone tool and can only be accessed by the administrator from within the thin client image.

Save all data on the USB flash drive prior to performing this procedure.

1. Once you launch the HP ThinState Capture tool from within the Control Panel, you are presented with the following screen.



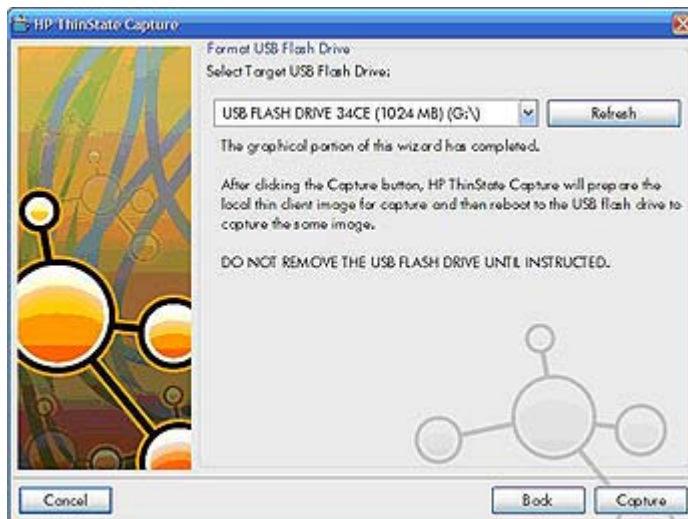
2. Click **Next**.



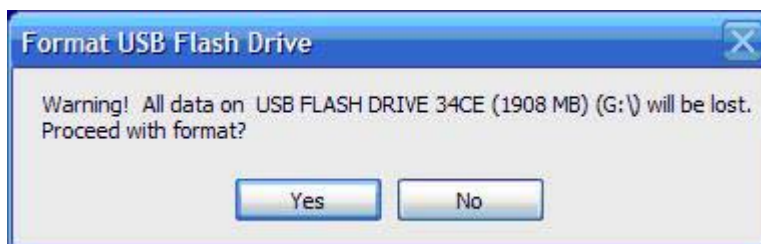
At this point, attach a disk on key (DOK) to the unit. The DOK drive letter and size are displayed.

The DOK must be greater in size than the onboard flash disk. As a result, if the thin client has 512 MB Flash, then the USB flash drive must be 1 GB.

Once the right DOK size is attached, the following screen displays.



3. Click **Capture**. The following warning displays.



4. Click **Yes**. The HP ThinState Capture tool formats and makes the USB flash drive bootable. HP ThinState Capture will now reboot the system.

- After you perform these actions, the HP ThinState Capture tool displays the following screen. Please follow the on-screen instructions.



You can now use the USB flash drive to deploy the captured image to another HP thin client of the exact same model and hardware with equal or greater flash size capacity.

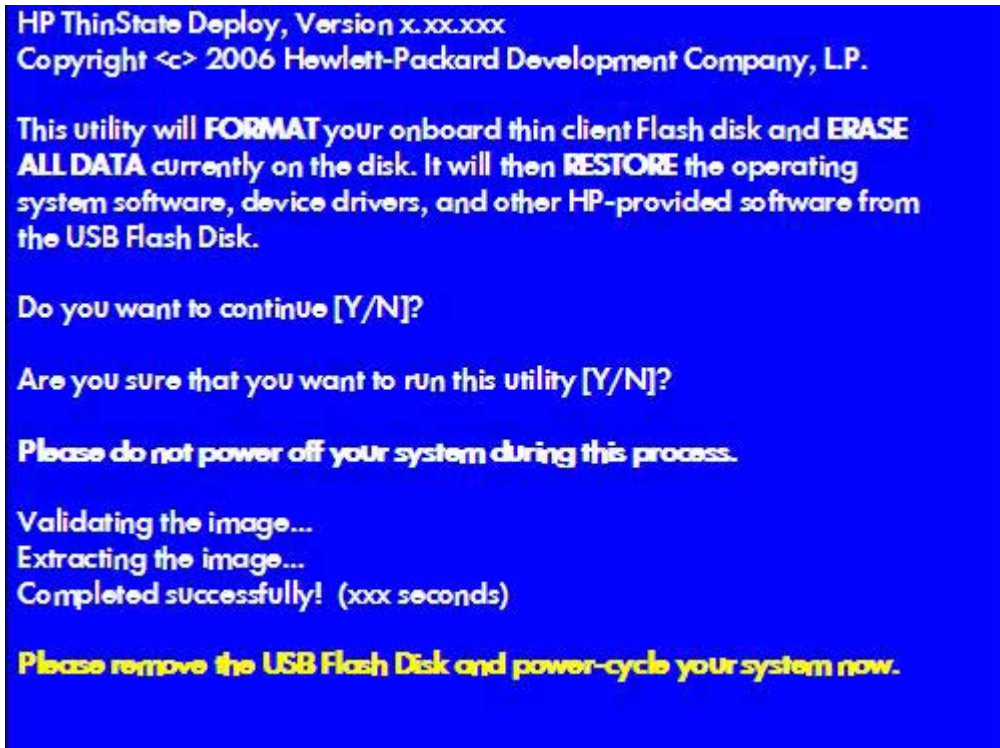
The following table lists the supported capture and deploy scenarios:

	Deploy To:		
	2GB Flash	1GB Flash	512MB Flash
Capture From:			
2GB Flash	X		
1GB Flash	X	X	
512MB Flash	X	X	X

HP ThinState Deploy


To perform an HP ThinState deployment:

1. Set the boot order in the F10 System BIOS to **USB boot**.
2. Attach the USB flash drive to the thin client unit you wish to deploy the captured image to, and then power on the unit.
3. Follow the on-screen instructions.



After you remove the USB flash drive and cycle power to the system, the image will unbundle. This process can take between 10-12 minutes. Do not interrupt or cycle power to the unit during this process.

You may use the captured image (flash.ibr) found in the USB flash drive in combination with Altiris Deployment or HP Device Manager Solution to remotely image multiple thin client units.

 **NOTE:** You must use flash.ibr in conjunction with the HP ThinState Deploy utility (e.g., ibr.exe). Flash.ibr is not compatible with the Altiris rdeploy.exe or rdeploy.exe utilities. Please consult the *HP Compaq Thin Client Imaging Tool* white paper at <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00485307/c00485307.pdf>.

For more information about Altiris, see <http://www.altiris.com/>.

HP FTP Image Update

HP FTP Image Update Client is a utility that allows image update from an FTP share to an HP thin client system running WES or XPe operating system.

Server Requirements

DHCP Server

Option 137 should contain a string value specifying an FTP share where the WES or XPe images and WinPE image are stored.

For example, if the XPe images and WinPE image are stored in ftp://ftpserver/ftpfolder, then the option DHCP option 137 should contain the following string:

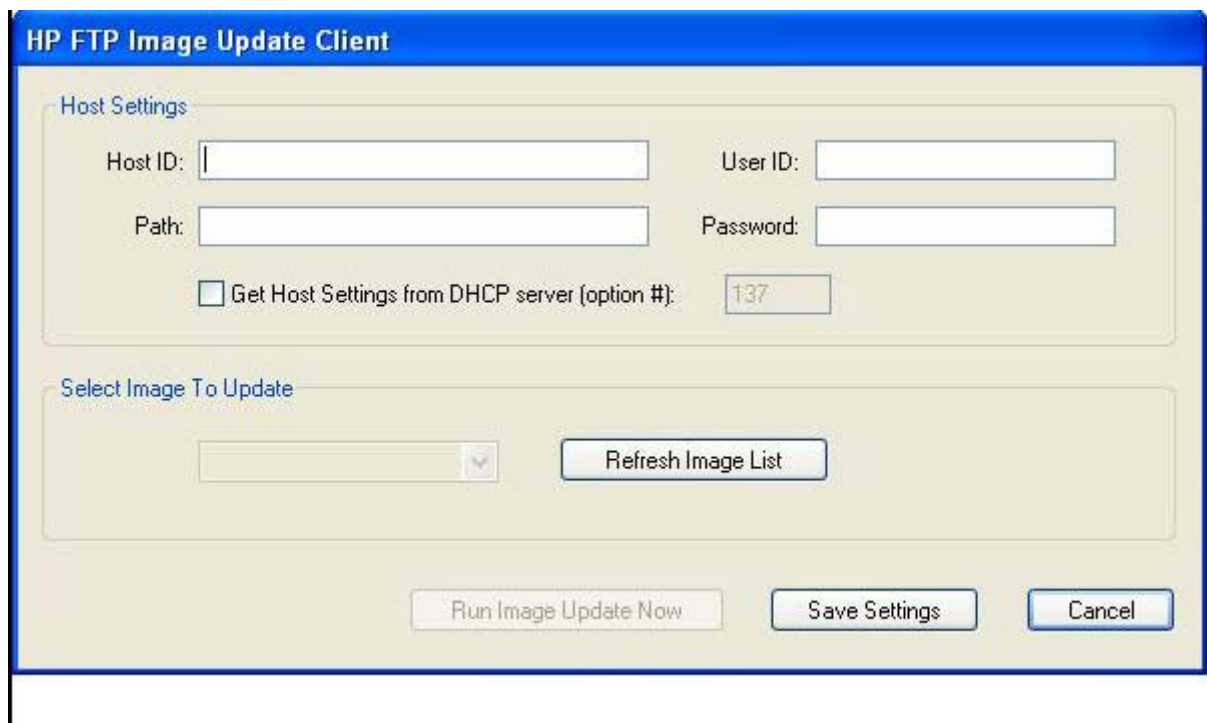
- ftp://username:password@ftpserver/ftpfolder, if the FTP share is protected
- or –
- ftp://ftpserver/ftpfolder, if the FTP share allows anonymous access


FTP Server

The WES and XPe images (in .IBR format) and the WinPE image provided by HP must reside in the same folder on the FTP server.

Description

The HP FTP Image Update Client can only be run by an administrator on an HP thin client system which has a license to run the WES or XPe operating system.



 **NOTE:** FTP Image Update is only provided on the t5630, t5630w, t5730, t5730w, gt7720, and vc4820T thin clients with the latest HP XPe image (5.1.606 or greater). For FTP Image Update to function properly, it requires the following available free space on the client: ~200MB of flash and ~250MB of RAM. FTP Image Update over wireless is not supported. For greater usage flexibility and to take advantage of this and all features provided in the latest image, HP recommends at least 1 GB of flash and 1 GB of RAM.

Host Settings

There are two ways to specify host settings:

1. You can manually enter settings by clearing the **Get Host Settings from DHCP server** check box and typing the appropriate information in the **Host ID**, **Path**, **User ID**, and **Password** fields.

If the FTP share allows anonymous read access, then you can leave the **User ID** and **Password** fields empty.

If the WES or XPe images and WinPE image are stored in the default (root) folder on the FTP server, then you can leave the **Path** field empty or type */* in the field.

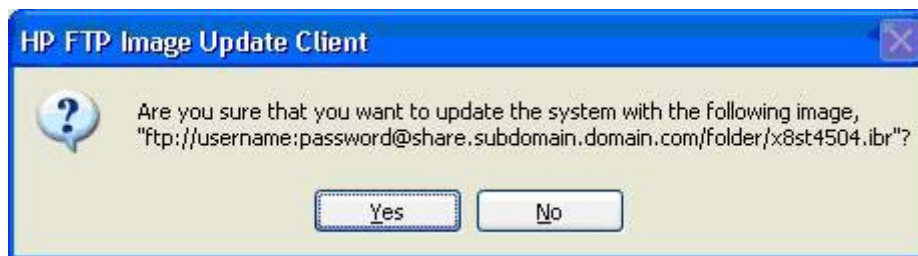
2. Automatically through a DHCP option by selecting the **Get Host Settings from DHCP server** check box.

These host settings can be saved and committed by clicking on the **Save Settings** button. When the applet is invoked again, the settings will be retrieved and the corresponding controls are automatically populated.

Select Image to Update

Once the host settings are entered, either manually or automatically through DHCP, then click the **Refresh Image List** button to make the applet query the FTP share for all XPe images whose targeted BIOS families match the one of the current thin client system, and fill in the drop-list combo box to the left of the button. You can choose any of the listed images to update/image the system.

When ready, you can click the **Run Image Update Now** button to proceed with the image update using the selected image. A confirmation dialog similar to the following is displayed.



Click **No** to abort the operation. If you click **Yes**, the HP FTP Image Update Client confirms that the flash drive has at least 200MB free to host the WinPE image. If the flash drive does not, the following error message is displayed.



If the flash device has enough memory, the update client starts the download of the WinPE image, modifies the boot loader to boot to WinPE in the next system restart, and then restarts the system to continue to the WinPE phase.



Once WinPE is loaded, IBRPE is spawned to image the system's flash drive using the selected image from the FTP share. When the imaging completes, IBRPE automatically restarts the system to enter the FBA phase.



6 Administration and Image Upgrades

This section highlights and discusses the Remote Administration capabilities and firmware upgrade methods applicable to the thin client.

Altiris Deployment Solution Software

The Altiris Deployment Solution software is a full-featured remote administration tool set. It accesses the thin client through the Altiris remote Agent and PXE server utilities installed on the thin client. Altiris allows you to perform the thin client administration functions (including firmware upgrades) without requiring an administrator to visit the individual thin client sites.

For more information about Altiris, see <http://www.altiris.com>.

HP Device Manager

HP Device Manager is a server-based application that provides centralized administration capabilities for HP thin client devices. It accesses the thin client through the HP Management Agent which is embedded in the standard thin client WES or XPe image to enable Device Manager to manage devices out-of-the-box (agents on older devices, however, may need to be upgraded).

For additional information concerning the HP Device Manager and the HP Management Agent please check the HP support site for these applications or for other important updates or documentation: <http://www.hp.com/support>. Select the country from the map, then select **See support and troubleshooting information** or **Download drivers and software (and firmware)**. Type the thin client model in the field and click [Enter](#).

Add-on Upgrades

If you want to install an add-on module, you can use the Altiris Deployment Solution or HP Device Manager to administer the thin client. Disable/enable the write filter as needed to save the changes.


△ **CAUTION:** If the available free space on the flash memory is reduced to less than 10MB and/or the available system memory is reduced to less than 15MB, the thin client becomes unstable.

📄 **NOTE:** For add-on modules to work and be downloaded, there must be sufficient flash space available. In some cases it may be necessary to remove software components to free up space for add-on modules.

Image Upgrades

The Intel Preboot Execution Environment (PXE) is a protocol that defines interaction between TCP/IP, DHCP and TFTP to enable a client to download a preboot environment from a server. PXE allows a

client to boot from a server on a network prior to booting the embedded operating system or the operating system from the local flash module. PXE allows a network administrator to remotely wake up a thin client and perform various management tasks, including loading the operating system and other software onto the thin client from a server over the network. The PXE client is installed on the thin client and the PXE server component is part of the Altiris Deployment Solution suite.

 **NOTE:** Citrix ICA auto update does not function for the ICA client installed on the thin client; updates are implemented through the standard firmware upgrade process.

HP FTP Image Update

HP FTP Image Update Client is a control panel utility that allows image update from an FTP share to an HP thin client system running WES or XPe operating system. For additional information please go to [HP FTP Image Update on page 46](#).

HP ThinState Capture and Deploy

The HP ThinState Capture tool is a very simple wizard based tool that can be used to capture an HP thin client WES or XPe image, which can then be deployed to another HP thin client of identical model and hardware. For more information about the HP ThinState Capture tool, see [HP ThinState Capture on page 42](#).

HP Compaq Thin Client Imaging Tool

The HP Compaq Thin Client Imaging Tool is part of the SoftPaq deliverable that contains the original factory image for the HP thin client. You can use this utility to restore the original factory image to the thin client.

This utility allows you to perform the following options:

- Create a bootable flash image on a USB flash device (such as on a disk on key).
- Unbundle the image to a directory for use in a custom deployment scenario or PXE image.

For additional information about this utility and its uses, visit the HP Web site at <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00485307/c00485307.pdf>.

HP Client Automation

HP Client Automation is an enterprise-wide client management solution for both physical and virtual clients. In addition to being able to completely manage traditional desktop and notebook PCs, HPCA can also manage thin client devices and the back-end virtual infrastructures they connect to. It significantly reduces the management challenges and complexities of thin client devices and client virtualization technologies by providing automation tools for creating and deploying operating system images, software updates, and tracking hardware assets. By using the same management console and tools for all client devices, HPCA helps customers reduce costs and simplify operations.

For additional information concerning HP Client Automation, see <http://www.hp.com/go/easydeploy>.

7 Peripherals

Depending on the ports available, the thin client can provide services for USB, serial, parallel, and PCI devices, as long as the appropriate software is installed. Factory-installed software is described in the following section. As they become available, you can install add-ons for other services using the Altiris Deployment or HP Device Manager solution software. For more information, see [Altiris Client Agent on page 30](#) and [HP Management Agent on page 32](#).

For more information about available peripherals, see the model QuickSpecs at http://h10010.www1.hp.com/wwpc/us/en/sm/WF04a/12454-321959-89307-338927-89307.html?jumpid=re_R295_prodexp/busproduct/computing/thinclients454-321959-89307-338927-89307.html.

Select the model, select **Specifications**, and then click the **QuickSpec** link.

Printers

A generic universal print driver is installed on the thin client to support text-only printing to a locally connected printer. To print full text and graphics to a locally connected printer, install the driver provided by the manufacturer and follow the manufacturer's instructions. Be sure to disable the write filter cache or run the `-commit` command to save the installation. You can print to network printers from ICA and RDP applications through print drivers on the servers.

For additional information, please review the *Printing and Imaging Support on HP Compaq Thin Clients* white paper on the HP support site at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00739537/c00739537.pdf?jumpid=reg_R1002_USEN.

△ **CAUTION:** If the available free space on the flash memory is reduced to less than 10MB and/or the available system memory is reduced to less than 15MB, the thin client becomes unstable.

📄 **NOTE:** Downloading and using printers requires sufficient flash space. In some cases, you may have to remove software components to free up space for printers.

Printing to a locally-connected printer from an ICA or RDP session using the print drivers of the server produces full text and graphics functionality from the printer. To do this, you must install the print driver on the server and the text-only driver on the thin client (see the following section).

Adding Printers Using Generic Text-only Print Driver

Follow these steps to add a printer using the text-only print driver:

1. Connect the printer to the parallel port.
2. Choose **Printers and Faxes** from the **Start > Settings** menu.
3. Select **Add a Printer** to open the **Add Printer Wizard**.

4. Click **Next** in the first panel of the wizard.
5. Select **Local printer configured to this computer**.
6. Verify that the **Automatically Detect and Install my Plug and Play Printer** check box is not selected.
7. Click **Next**.
8. Select **Use the Following Port**.
9. Select the appropriate port from the list, and then click **Next**.
10. Choose the manufacturer and model of the printer, and then click **Next**.
11. Use the assigned default name or other name for the printer, and then click **Next**.
12. Select **Do Not Share this Printer**, and then click **Next**.
13. Choose whether to print a test page, and then click **Next**.
14. Click **Finish**.

Using Manufacturer Print Drivers

Install the driver provided by the manufacturer and follow the manufacturer's instructions. Be sure to disable the write filter or issue the -commit command to save the installation.

HP Universal Print Driver for Thin Clients Add-on

HP has developed a printing add-on for the WES- and XPe-based thin clients; this add-on is a re-packaging of the HP Universal Print Driver with changes to make it more suitable for the thin client software environment. For example, due to disk space limitations, the current version is available only in English and with no help files. Go to <http://www.hp.com/support>. Select the country from the map, then select **Download drivers and software (and firmware)**. Type the thin client model in the field and click **Enter**. Select the thin client model, then the operating system, and download this add-on.

For the detailed specification, other downloads, and documentation on the original UPD, go to <http://www.hp.com/go/upd>.

For more information on the HP Universal Print Driver, refer to *Thin Client Printing with the HP Universal Print Driver*, a white paper, at <http://bizsupport.austin.hp.com/bc/docs/support/SupportManual/c01237156/c01237156.pdf37156/c01237156.pdf>.

Audio

You can redirect audio from applications to the audio jacks on the thin client. You control the level externally (such as by a 600-ohm potentiometer control) and driving speakers requires a power booster. You can adjust the volume using the sound icon in the task bar system tray. You can single-click on this icon to open the master volume control or double-click to open the volume control application dialog box.

Index

A

- accounts
 - creating user 11
 - user 7
- add-on modules 49
- add-on upgrades 49
- adding ports, Microsoft Windows Firewall 22
- adding printers 51
- adding programs, Microsoft Windows Firewall 22
- administration 49
- Administrative Tools 15
- administrator
 - desktop 3
 - logon 7
- Altiris
 - Client Agent 16
 - deployment server 5
 - Deployment Solution 49
- Altiris Deployment Solution 5
- Altiris Web site 5, 45
- applications 16
- audio 52
- automatic logon 6

C

- changing the password 7
- Citrix 16
- Citrix ICA 4
- Citrix Web site 25
- client agent, Altiris 16
- Client Automation 16, 50
- configuring Windows Firewall 18
- Control Panel 35
- creating user account 11

D

- default passwords 7
- deployment server, Altiris 5

- deployment solution, Altiris 5
- desktop 3
- desktop administrator 3
- desktop, user 3
- Device Manager 5, 16, 49
- DHCP server 46
- DHCP Settings Update Client 41
- disk on key requirements 43
- drive C 10
- drive Z 10
- drives
 - drive C and flash 10
 - drive Z 10

E

- emulation
 - Teemtalk Terminal Emulation 16
 - terminal 5
- Enhanced Write Filter 8
- Enhanced Writer Filter Manager 6
- EWf 8
- extended selections, control panel 35

F

- failure resolution 22
- failure symptoms, Microsoft Windows Firewall 21
- features, thin client 2
- filter
 - Enhanced Write Filter 8
 - write 10
 - writer 6
- firewall
 - configuring 18

- Microsoft Windows Firewall 16
- Symantec Endpoint Protection 16
- flash drive 10
- FTP Image Update
 - host settings 47
 - image selection 47
 - server requirements 46
- FTP server 46

H

- host settings, FTP Image Update 47
- HP Client Automation 16, 50
- HP Compaq Thin Client Imaging Tool 50
- HP Device Manager 5, 16, 49
- HP DHCP Settings Update Client 41
- HP FTP Image Update
 - host settings 47
 - image selection 47
 - server requirements 46
- HP Management Agent 16
- HP RALF 16
- HP RAMDisk 10
- HP Registration and Agent Loading Facility 16
- HP SAM 16
- HP SAM Web site 28
- HP Session Allocation Manager 16
- HP support Web site, 16
- HP ThinState Capture 42, 50
- HP ThinState Deploy 45, 50
- HP Universal Print Driver 52

I

- ICA 4

- image capture 42
- image deployment 45
- image selection, FTP Image Update 47
- image upgrades 49
- imaging tool 50
- information, Web sites 1
- internet 2
- Internet Explorer 16
- Internet Explorer unsafe file list 33

L

- language options 14
- local drives 10
- log on as Administrator 7
- logging off 8
- logon
 - automatic 6
 - manual 7
- Logon Configuration Manager 6

M

- Management Agent 16
- manual logon 7
- manufacturer print drivers 52
- mapping network drives 11
- Media Player 16
- memory, volatile 10
- Microsoft Internet Explorer 16
- Microsoft Internet Explorer unsafe file list 33
- Microsoft RDP 5, 16
- Microsoft Windows Firewall
 - adding ports 22
 - adding programs 22
 - configuring 18
 - failure symptoms 21
 - gathering configuration information 21
 - troubleshooting applications 21
- monitor saver 9
- multimedia 2

O

- on by default 18

P

- password 7
- password, changing 7

- peripherals 51
- peripherals, QuickSpecs Web site 51
- PN Agent 16
- power management 9
- preinstalled applications 16
- print driver 52
- print drivers 52
- printers 51
- printers, adding 51
- profiles 12
- program neighborhood 16
- PXE 49

R

- RALF 16
- RAMDisk 10
- RDP 5
- receiver, RGS 16
- regional language options 14
- Registration and Agent Loading Facility 16
- Remote Desktop Connection 16
- Remote Desktop Protocol 16
- Remote Graphics Software receiver 16
- requirements
 - disk on key 43
 - server 4
- resolution, network application failure 22
- restarting 8
- RGS receiver 16
- roaming profiles 10

S

- SAM Web site 28
- saving files 11
- security
 - configuring Microsoft Windows Firewall 18
 - Microsoft 16
 - Microsoft Windows Firewall 16
 - Symantec Endpoint Protection firewall 16
- Security Center 18
- server
 - DHCP 46
 - FTP 46

- server requirements 4
- server requirements, FTP Image Update 46
- server, Altiris deployment 5
- services, session 4
- Session Allocation Manager (SAM) 16
- session services 4
- shutting down 8
- Symantec Endpoint Protection 16
- system time 9

T

- Teemtalk Terminal Emulation 16
- terminal emulation 5
- text-only print driver 51
- Thin Client Imaging Tool 50
- ThinState Capture 42, 50
- ThinState Deploy 45, 50
- time utility 9
- troubleshooting applications, Microsoft Windows Firewall 21

U

- Universal Print Driver 52
- unsafe file list for Internet Explorer 33
- upgrades 49
- upgrades, add-on 49
- upgrading images 49
- USB enhancements 16
- user
 - accounts 7
 - profiles 12
- user desktop 3
- User Manager 11
- utilities
 - Client Automation 50
 - DHCP Settings Update Client 41
 - system time 9
 - Thin Client Imaging Tool 50
 - Universal Print Driver 52

V

- VMWare View Manager 16
- volatile memory 10

W

Web site

Altiris 45

Citrix 25

HP SAM 28

HP support 16

HP Thin Client Imaging Tool

white paper 45

more information 1

peripheral QuickSpecs 51

WES 3

Windows Media Player 33

Windows XPe 3

WES Web site 3

Windows Firewall 16

Windows Media Player 16

Windows Media Player Web
site 33

Windows XPe Web site 3

write filter 10

writer filter 6

Z

Z drive 10