



Microsoft® Windows Embedded
Standard (WES) 2009 for HP Thin
Clients

Quick Reference Guide

© Copyright 2012 Hewlett-Packard
Development Company, L.P.

Microsoft and Windows are U.S. registered
trademarks of Microsoft Corporation.

Adobe and Acrobat are 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.


Third Edition: December 2012


First Edition: November 2009

Document Part Number: 597495-003

About this book

This guide supplements the standard WES 2009 documents supplied by Microsoft Corporation. This document highlights the differences, enhancements, and additional features of the latest image provided by HP.

 **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	1
2 Introduction	2
The Desktop	3
User Desktop	3
Administrator Desktop	4
Server Environment Requirements	4
Session Services	5
Citrix ICA	5
Microsoft RDP	5
Terminal Emulation Support	5
Thin Client Management Services	5
HP ThinState Capture	5
HP Device Manager	6
HP Client Automation	6
Altiris Deployment Server	6
3 Configuration	7
Logging On	7
Automatic Logon	7
Manual Logon	8
Administrator Logon Access	8
Logging Off, Restarting, and Shutting Down the Thin Client	9
Write Filters	9
Power Management	10
System Time	10
Local Drives	11
Drive Z	11
Drive C and Flash	11
Saving Files	12
Mapping Network Drives	12

Roaming Profiles	12
User Accounts	12
Creating a New User Account	12
User Manager	13
User Profiles	13
Regional and Language Options	15
Administrative Tools	16

4 Applications 17

Symantec Endpoint Protection Firewall (select models only)	18
About the Agent	18
New Features and Functionality	19
Citrix Program Neighborhood (PN) Agent	19
Remote Desktop Connection	20
HP Remote Desktop Protocol (RDP) Multimedia and USB Enhancements	20
Configuring USB Drives for Redirection	20
HP Remote Graphics Software (RGS) Receiver	22
TeamTalk Terminal Emulation	22
VMware View Manager	23
Altiris Client Agent	24
HP Management Agent	25
HP Client Automation Registration and Agent Loading Facility (RALF)	25
HP ThinState	26
HP ThinState Capture	26
HP ThinState Deploy	30
Microsoft Internet Explorer	30
Windows Media Player 11	31

5 Control Panel Extended Selections 32

Write Filters	33
Choosing the Write Filter	33
Enhanced Write Filter Manager	33
Benefits of the Enhanced Write Filter	33
Enhanced Write Filter Status Service	34
Enhanced Write Filter GUI	35
EWF GUI Buttons	35
DOS Command-line Tool Boot Commands	36
Using Boot Commands	36
File-Based Write Filter Manager	37
Benefits of the File-Based Write Filter	37
File-Based Write Filter Status Service	37

File-Based Write Filter GUI	38
HP RAMDisk	40
HP Easy Tools	41
6 Administration and Image Upgrades	42
HP Device Manager	42
HP Client Automation	42
HP ThinState Capture and Deploy	42
Altiris Deployment Solution Software	43
HP Compaq Thin Client Imaging Tool	43
Image Upgrades	43
Add-on Upgrades	44
7 Peripherals	45
Printers	45
Adding Printers Using Generic Text-only Print Driver	45
Using Manufacturer Print Drivers	46
HP Universal Print Driver for Thin Clients Add-on	46
Audio	47
Index	48

1 For More Information and Updates

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

For important documentation that provides specific information for your image version, check the HP support site at <http://www.hp.com/support>. Select the country/region from the map, and then select **See support and troubleshooting information**. Type the thin client model in the field and click [Enter](#).

2 Introduction

HP WES 2009-based thin client models use the Windows Embedded Standard (WES) 2009 operating system. This guide provides information pertaining to the latest shipping WES 2009 image. 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 Remote Graphics Software (RGS)
 - HP TeamTalk
- User interface similar to familiar Windows XP Professional
- Improved security
 - Symantec EndPoint Protection Firewall (select models only)
 - Microsoft Firewall (Add-on)
 - Locked down protected Flash drive
- Multimedia
 - Windows Media[®] Player
 - Musical Instrument Digital Interface (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, the HP Easy Tools control panel applet, or the add-ons provided on the HP support site, and customize it to your specific needs.

This guide will introduce you to the features of this client that are not found in the standard WES 2009 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 2009 user and administrator desktop features and functions.


User Desktop

The desktop that is displayed when you are logged on as a user is a standard WES 2009 desktop, with the exception that the only icons displayed are for 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 Citrix documentation for information and instructions.

For information about the functionality of the standard WES 2009 desktop and Start menu items, refer to the applicable Microsoft documentation.

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

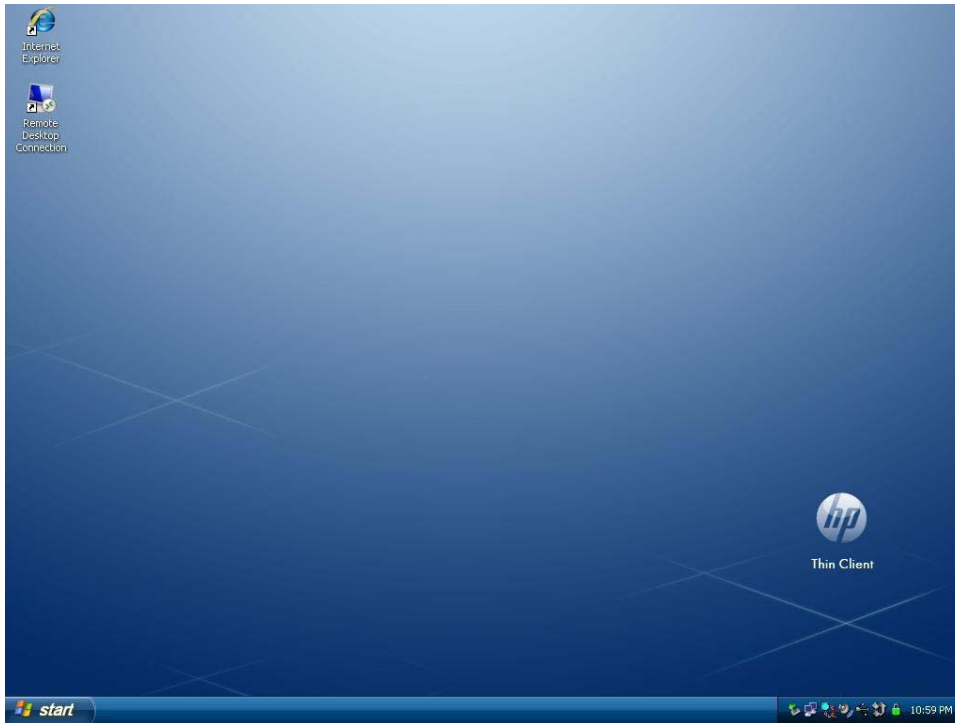
 **NOTE:** The Control Panel, available by clicking **Start > Control Panel**, provides access to a limited set of resources for changing user preferences. You must log on as Administrator to access the extended set of Control Panel options and utilities.

Right-clicking the mouse when the pointer is on a user’s desktop background does not open a pop-up menu in the default windows policies configuration.

Administrator Desktop

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

- Microsoft RDP
- Internet Explorer



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

Citrix Program Neighborhood and HP Easy Config were available on the desktop with older versions of the image.

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://technet.microsoft.com/en-us/windowsserver/default.aspx>.

Terminal Emulation Support

All WES 2009-based thin client models include TeemTalk terminal emulation software to support computing on legacy platforms. The terminal emulation software uses the Telnet protocol to communicate with the computing platform.

Thin Client Management Services

HP has a comprehensive suite of management solutions to fit your needs. This allows you to choose solutions that will work best in your environment.

HP ThinState Capture

HP ThinState Capture allows you to clone and deploy a software image from one thin client to another thin client of the same model, using a USB drive key.

HP Device Manager

HP Device Manager is an enterprise-class thin client management software application that allows customers to view their thin client assets remotely and to manipulate those thin clients to meet the required business need. It is robust, yet easy to install and use. HP Device Manager lets you track, configure, upgrade, clone, and manage thousands of individual devices from a centralized location. HP Device Manager agents are included in most HP thin clients.

HP Client Automation

HP Client Automation is an industry-leading device management product, which is part of a bigger Business Service Automation environment management solution. With HP Client Automation, you can manage simple thin client deployments or highly complex IT environments that contain a combination of thin clients, PCs, blades, servers and other common computer-based resources. HP Client Automation agents work with all HP thin clients. For more information on HP Client Automation, please visit the HP Web site at see <http://www.hp.com/go/easydeploy>.

Altiris Deployment Server

HP continues to partner with Altiris to manage HP thin clients. Altiris Deployment Solution is a leading tool for quick deployment and ongoing management of thin clients in your organization.

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*.

3 Configuration


Logging On

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

Automatic Logon

The default for the WES 2009-based thin client is automatic logon of the locked-down User account. 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, please perform the appropriate action depending on the write filter being used. Please consult [Write Filters on page 33](#) for detailed instructions.

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 opens 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 opens 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+Delete** 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 12](#).

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+Delete** to open the dialog box.

If automatic logon is enabled, when you log off (without shutting down), the thin client immediately logs on the pre-defined User account set up in Windows Login Configuration. For instructions for logging on as a different user, see [Logging On on page 7](#).

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

- [Write Filters on page 9](#)
- [Power Management on page 10](#)
- [System Time on page 10](#)

Write Filters

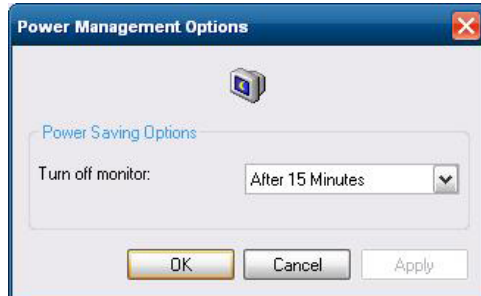
For detailed information, see [Enhanced Write Filter Manager on page 33](#) and [File-Based Write Filter Manager on page 37](#). If you want to save changes to system configuration settings, you must disable the write filter or issue the `-commit` command depending on the write filter being used. Otherwise, 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.

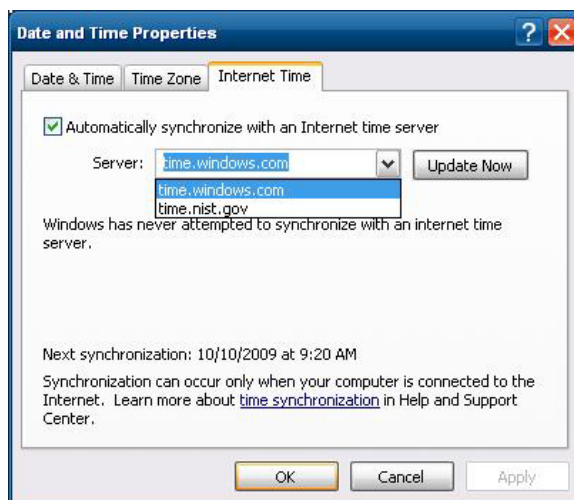
Power Management


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

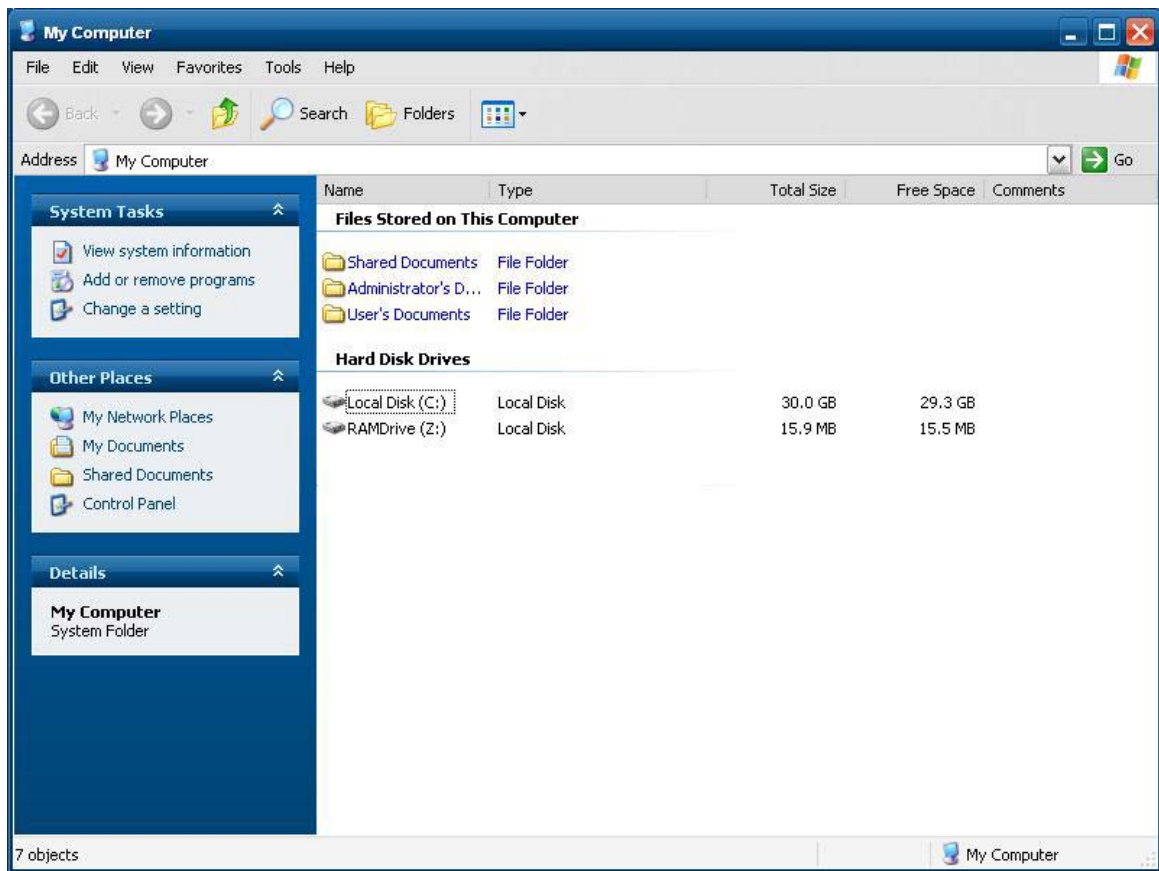
You can manually set the local time, or you can automatically set the local time utility to synchronize the thin client clock to a time server at a designated time.



 **NOTE:** On some older images, 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 40](#). For information about using the Z drive for roaming profiles, see [Roaming Profiles on page 12](#).

Drive C and Flash


Drive C is in the onboard flash drive. HP recommends that you do not allow the free space on Drive C to drop below 15MB.

CAUTION: If the available free space on the flash drive is reduced to below 15MB, 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 is disabled or a `-commit` command is issued, depending on the write filter being used. See the write filter topics in [Write Filters on page 33](#) for instructions to disable the cache. For detailed information see

[Enhanced Write Filter Manager on page 33](#) and [File-Based Write Filter Manager on page 37](#).
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 Accounts on page 12](#).

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.

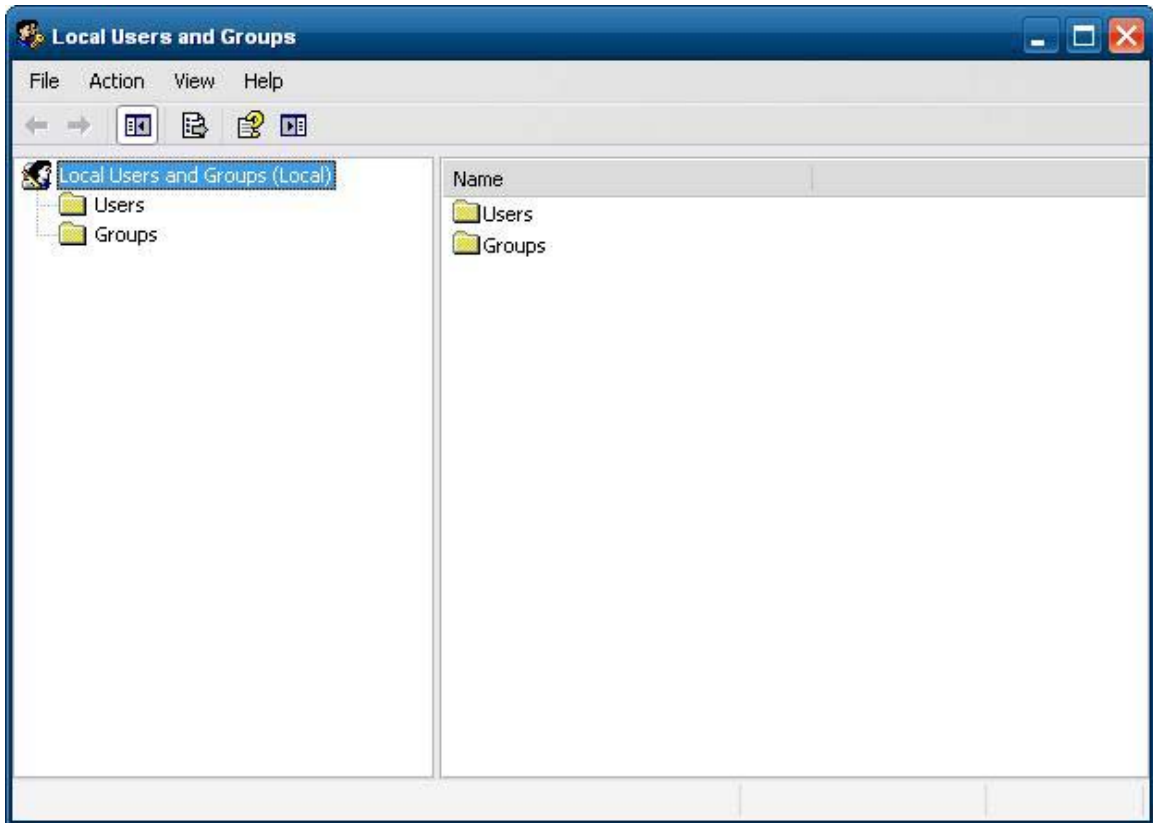
Creating a New User Account

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 Administrator 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 created 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. The Administrator may also want to apply specific Windows policies to the new account to restrict certain actions or behaviors.

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.

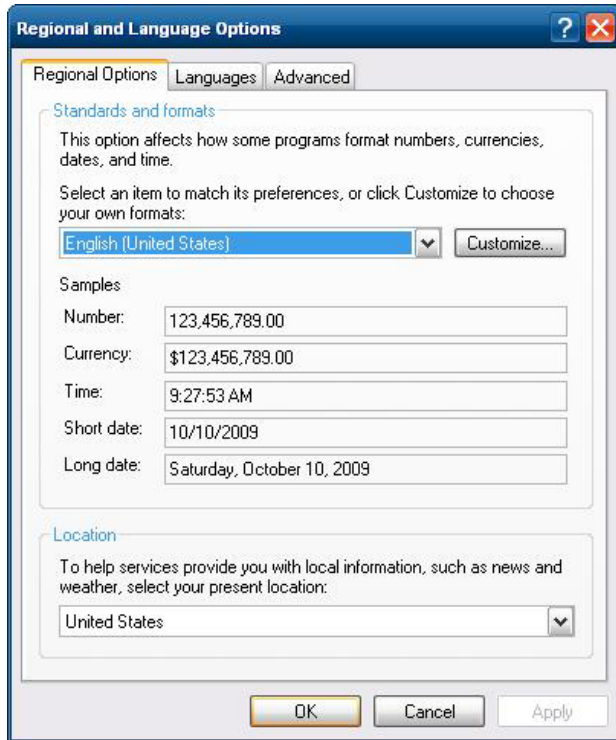
To create the user:

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 will have Windows policies applied similar to that of the Administrator account. It may be desirable to apply specific Windows policies to limit the capabilities of this new account.

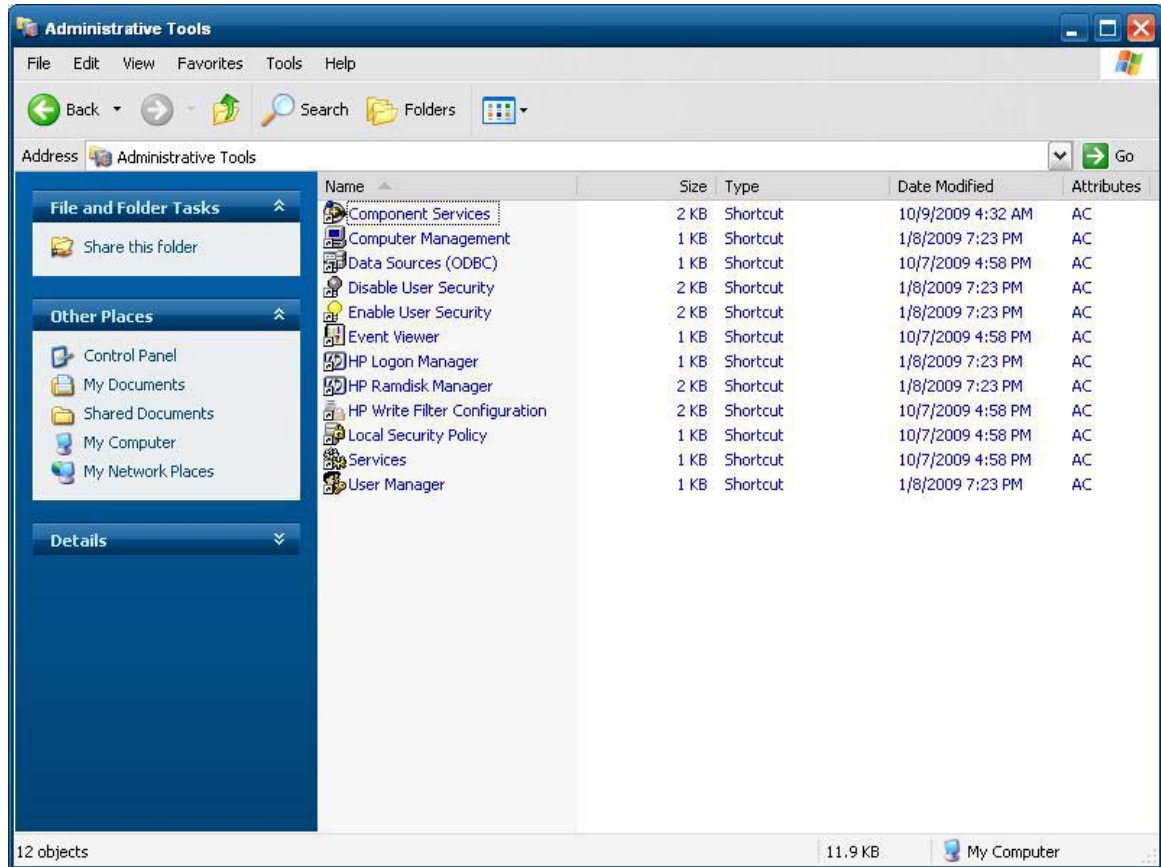
Regional and Language Options

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:



The administrative tools can also be accessed directly from the start menu:



4 Applications

The latest WES 2009 image has the following preinstalled applications:

- [Symantec Endpoint Protection Firewall \(select models only\) on page 18](#)
- [Citrix Program Neighborhood \(PN\) Agent on page 19](#)
- [Remote Desktop Connection on page 20](#)
- [HP Remote Desktop Protocol \(RDP\) Multimedia and USB Enhancements on page 20](#)
- [HP Remote Graphics Software \(RGS\) Receiver on page 22](#)
- [TeemTalk Terminal Emulation on page 22](#)
- [VMware View Manager on page 23](#)
- [Altiris Client Agent on page 24](#)
- [HP Management Agent on page 25](#)
- [HP Client Automation Registration and Agent Loading Facility \(RALF\) on page 25](#)
- [HP ThinState on page 26](#)
- [Microsoft Internet Explorer on page 30](#)
- [Windows Media Player 11 on page 31](#)

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

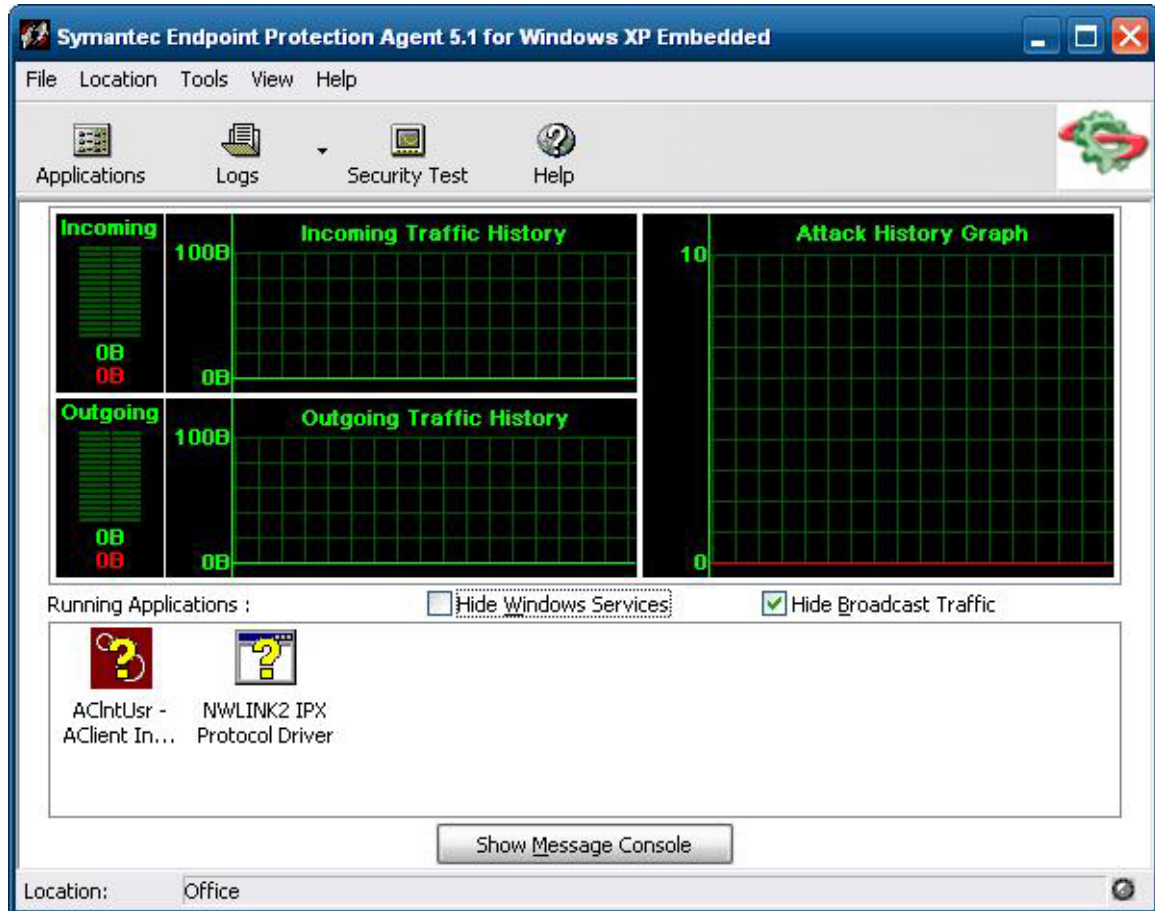
- [Symantec Endpoint Protection Firewall \(select models only\) on page 18](#)
- [Altiris Client Agent on page 24](#)

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/region 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 (select models only)

Select HP images include a Symantec Endpoint Protection Agent Firewall.



About the Agent

 **NOTE:** AV software and SEP management console are not included. Contact Symantec directly for software and licenses.

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 2009 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 Symantec (formerly 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.

Citrix Program Neighborhood (PN) Agent

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 2009 image, 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.

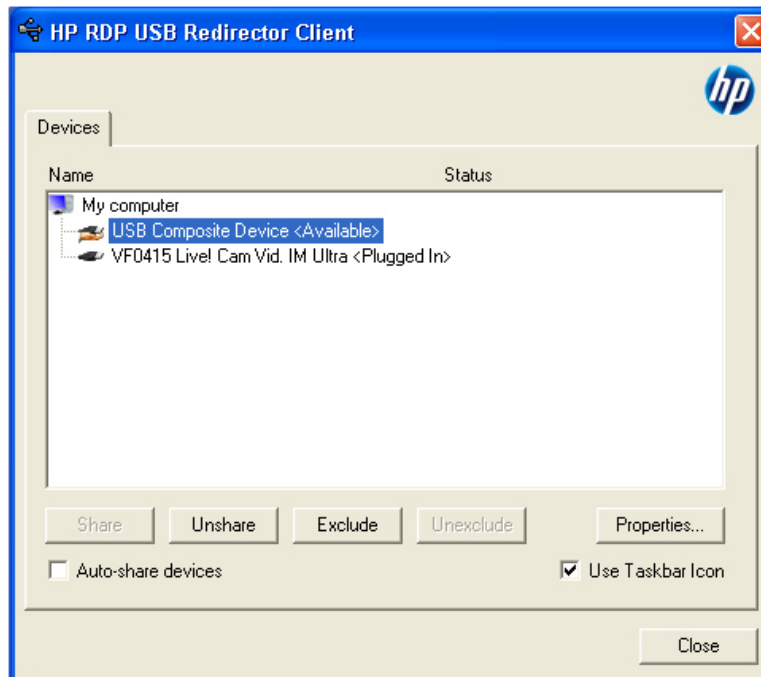
 **NOTE:** This functionality may not be preinstalled or offered on all platforms.

Configuring USB Drives for Redirection

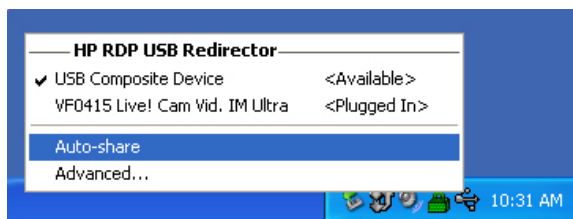
 **NOTE:** A shared device is a device that behaves as if it is connected to the remote desktop. An unshared or excluded device is only available locally. An excluded device will not be automatically shared, even if Auto-share is checked.

To share USB devices, complete the following steps:

1. On the thin client, open the Control Panel and select **HP RDP USB Redirector Client**.



NOTE: If Use Taskbar Icon is checked, you can right-click the icon in the task bar to open the HP RDP USB Redirector status. This lists the devices that are currently available or plugged in. Click **Advanced** to open the HP RDP USB Redirector Client dialog box.



2. Select the USB devices you want to redirect.
 - To automatically redirect all USB devices, check **Auto-share devices** (Auto-share is off by default).

NOTE: Auto-share automatically shares devices when they are plugged in. Most USB keyboards and mice are automatically excluded from Auto-share, because when a device is shared, it is disconnected from the local system. However, some multi-interface (composite USB) keyboards might not be automatically excluded from Auto-share. These types of devices should be manually excluded before enabling Auto-share.

- To selectively redirect USB devices, select each device individually from the list displayed, then click **Share**, **Unshare**, or **Exclude**.
- To prevent a device from being automatically redirected for use with the remote desktop, select the device and click **Exclude**. This disables both **Share** and **Unshare**. In order to share the device manually or automatically, you must click **Unexclude**.

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.

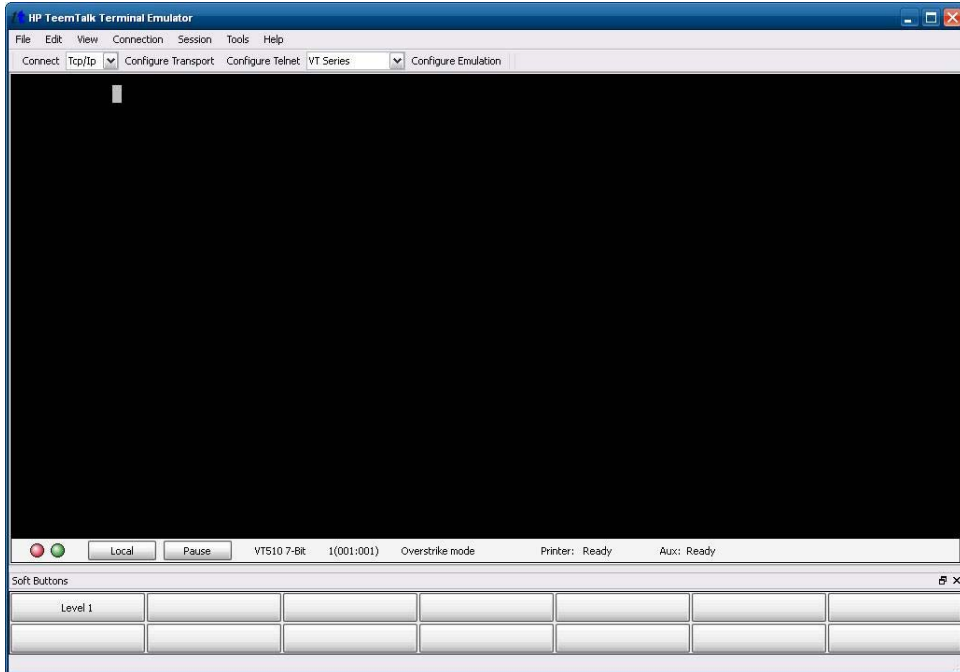
The RGS Receiver is included in the latest HP thin client WES 2009 image. Visit <http://www.hp.com/go/rgs> for information on RGS Sender Licensing, installation, and use.



TeemTalk Terminal Emulation

All WES 2009-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 > Hewlett Packard**.



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.

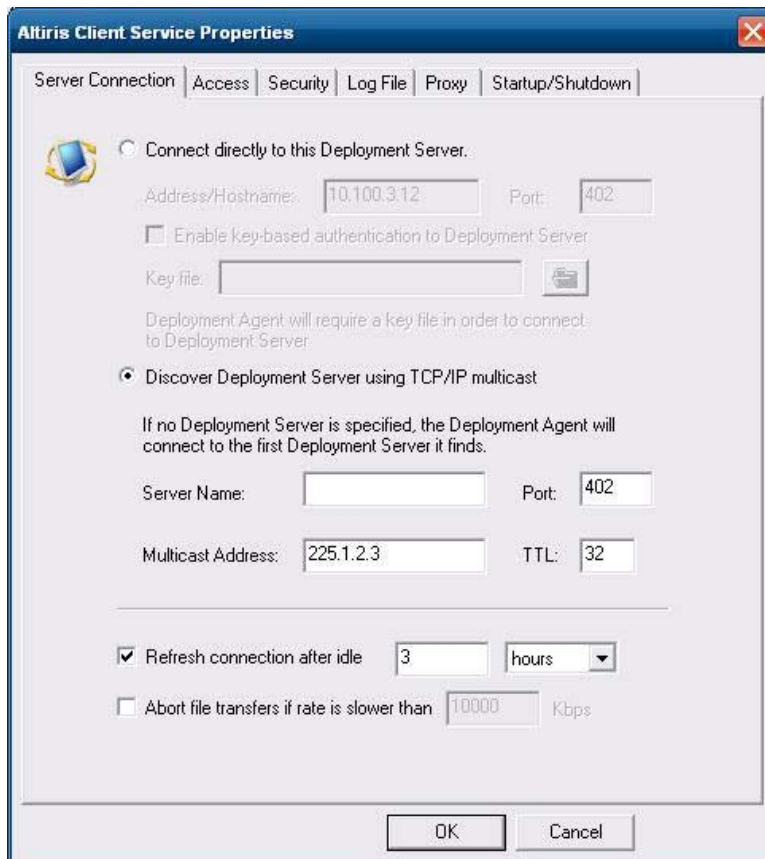
For additional information and to obtain the latest VMware View client, contact VMware or see <http://www.vmware.com/products/view>.




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.

 **NOTE:** Although the Altiris Client agent is preinstalled, a free license is no longer included on the HP t5740 Series and all new HP thin clients going forward. To purchase a license, contact Altiris at <http://www.altiris.com>.



 **NOTE:** This functionality may not be preinstalled or offered on all platforms.

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 2009 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/region 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 see <http://www.hp.com/go/easydeploy>.

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.

HP ThinState

The HP ThinState Capture tool is a very simple wizard-based tool that you can use to capture an HP thin client WES 2009 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 2009-based thin client that contains the latest HP-provided image
- An HP-qualified USB flash drive (Disk-On-Key). Consult the thin client 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: ThinState Capture now uses `ibrpe.exe` for imaging. Any flash drives previously created containing `ibr.exe` can no longer be used.

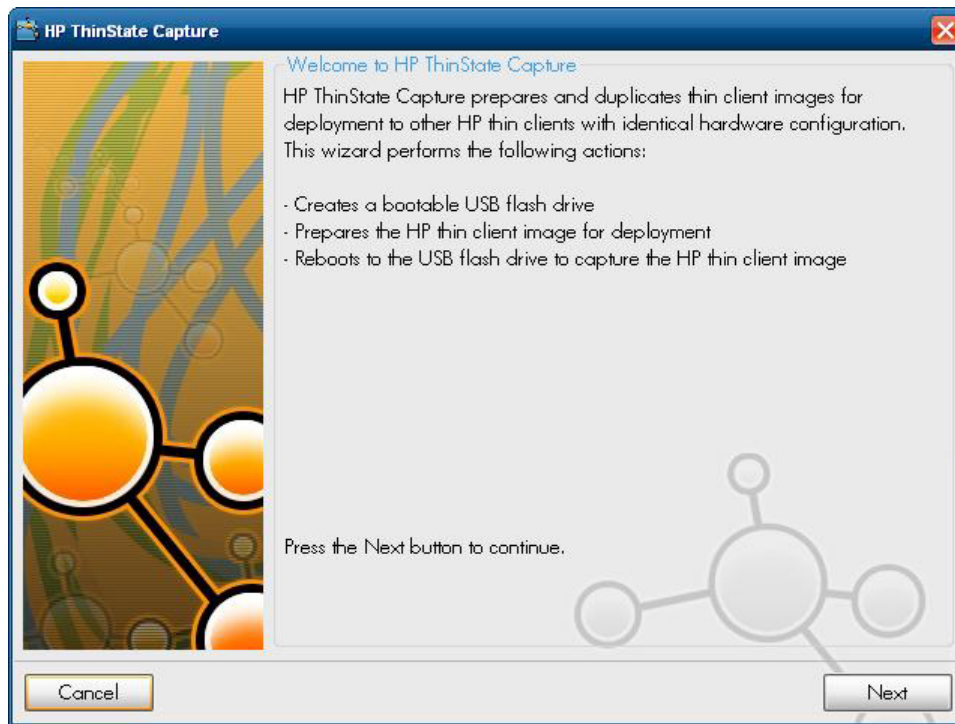
HP ThinState Capture

To perform an HP ThinState capture:

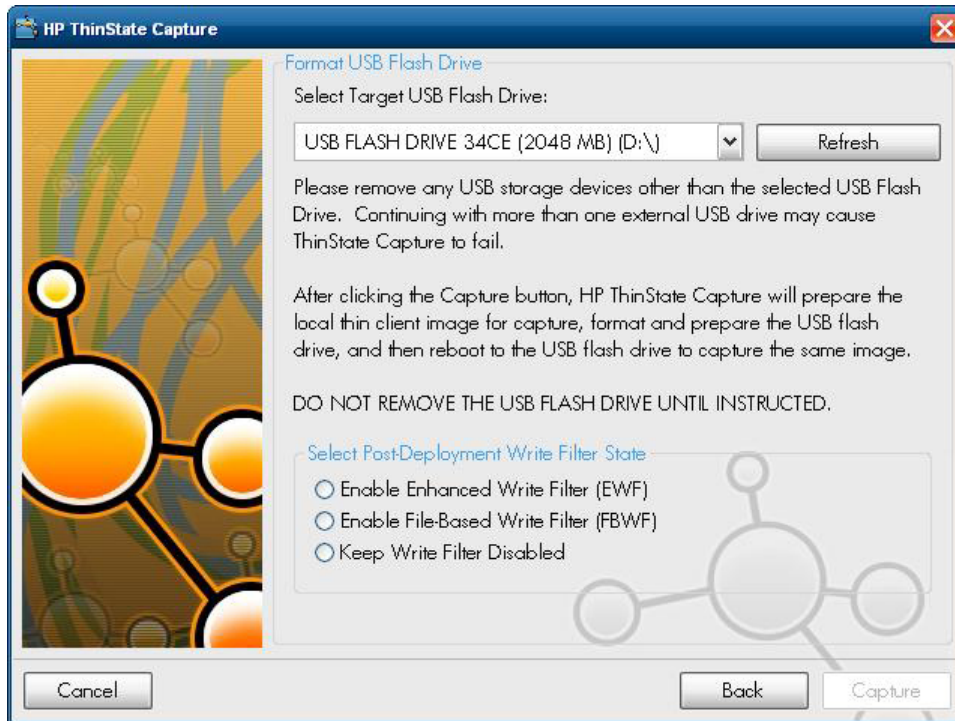
1. Disable the write filter prior to launching the Thinstate Capture tool. If you do not, you will be presented with the following warning:




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



3. Click **Next**.

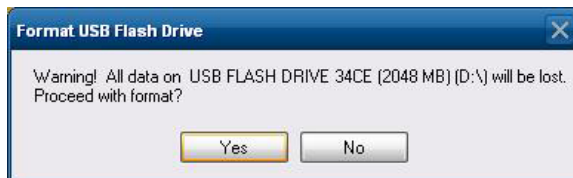


At this point, attach a disk on key (DOK) to the unit. The DOK drive letter and size are displayed.

 **NOTE:** Be sure that the DOK has enough storage capacity to hold the captured image.

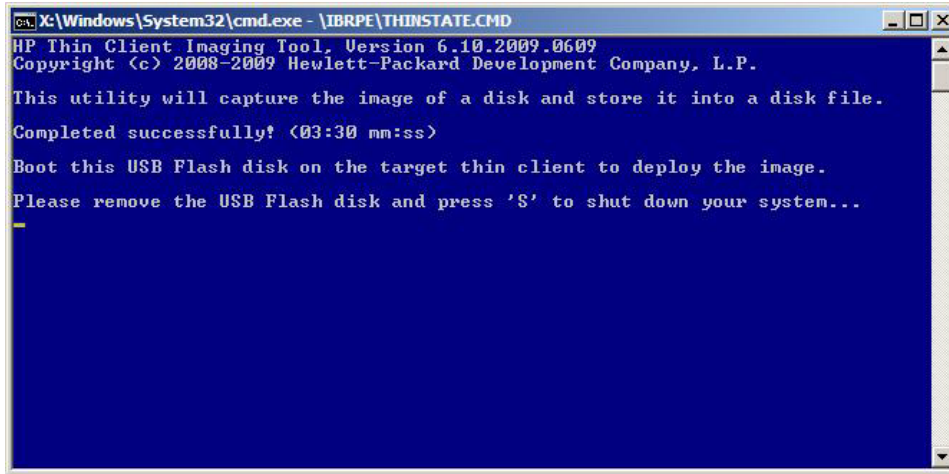
Once the DOK is attached, the following screen is displayed.

4. Click **Capture**. The following warning is displayed.



5. 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 opens 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.

NOTE: In this new version of ThinState Capture, you may be able to capture the image from a greater sized flash and deploy it to a lesser sized flash, depending on the size of the captured image.

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 prior images, the target unit would need to have had an equal or greater flash size capacity than the source unit. The following table lists examples of capture and deploy scenarios using images prior to 5.1.810:

		Deploy To (Target):	
		4GB Flash	2GB Flash
Capture From (Source):			
4GB Flash		X	
2GB Flash		X	X

With the new Thinstate Capture (starting with image 5.1.810), you may be able to capture the image from a greater sized flash and deploy it to a lesser sized flash. The following table lists examples of capture and deploy scenarios using image 5.1.810 or newer:

		Deploy To (Target):	
		4GB Flash	2GB Flash
Capture From (Source):			
4GB Flash		X	X*
2GB Flash		X	X

*Assuming the actual size of the image is less than the size of the flash.

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.

```
cmd: X:\Windows\System32\cmd.exe - \IBRPE\THINSTATE.CMD
HP Thin Client Imaging Tool, Version 6.10.2009.0609
Copyright (c) 2008-2009 Hewlett-Packard Development Company, L.P.

This utility will FORMAT your flash disk and ERASE ALL DATA currently on the
disk. It will then RESTORE the original operating system software, device
drivers, and other HP-provided software that came with the computer.

Do you want to continue [Y/N]?
Are you sure that you want to run this utility [Y/N]?

Please do not power off your system during this process.

Completed successfully! (03:57 mm:ss)

Please remove the USB Flash disk and press 'S' to shut down your system...
```

After you remove the USB flash drive and cycle power to the system, the image will unbundle. This process can take 3–5 minutes, depending on flash drive speed and internal flash size. Do not interrupt or cycle power to the unit during this process.

Microsoft Internet Explorer

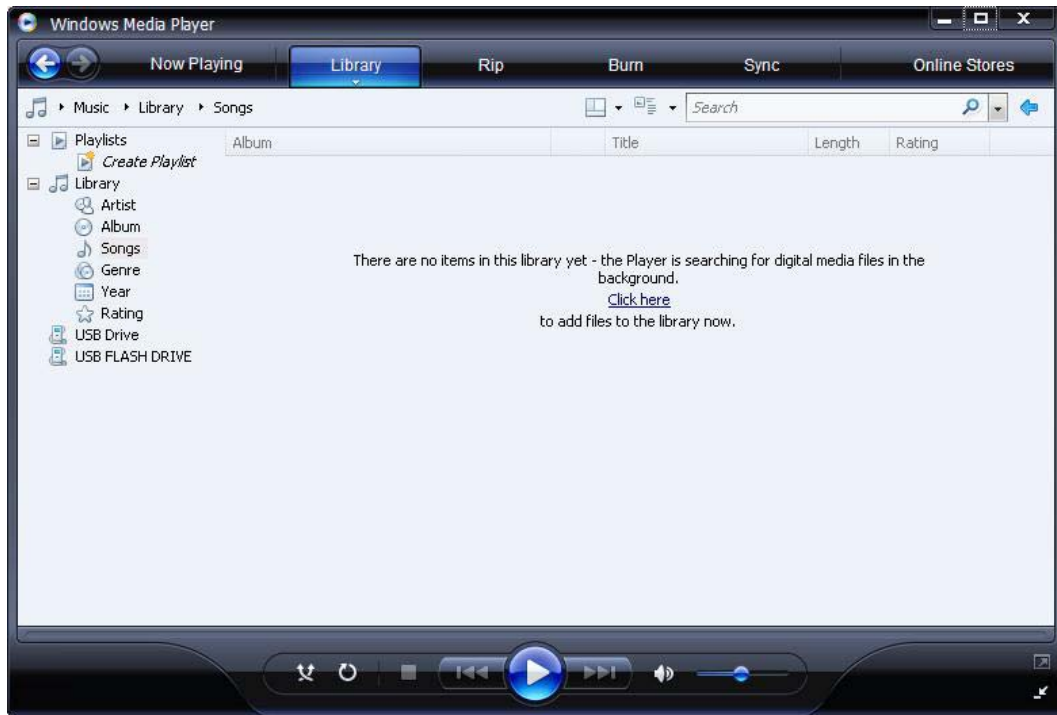
Version 7.0 of the Microsoft Internet Explorer browser is installed locally on the thin client. The Internet options settings for the browser have been preselected at the factory to limit writing to the flash memory. These settings prevent exhaustion of the limited amount of flash memory available and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

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/291369>.

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>.

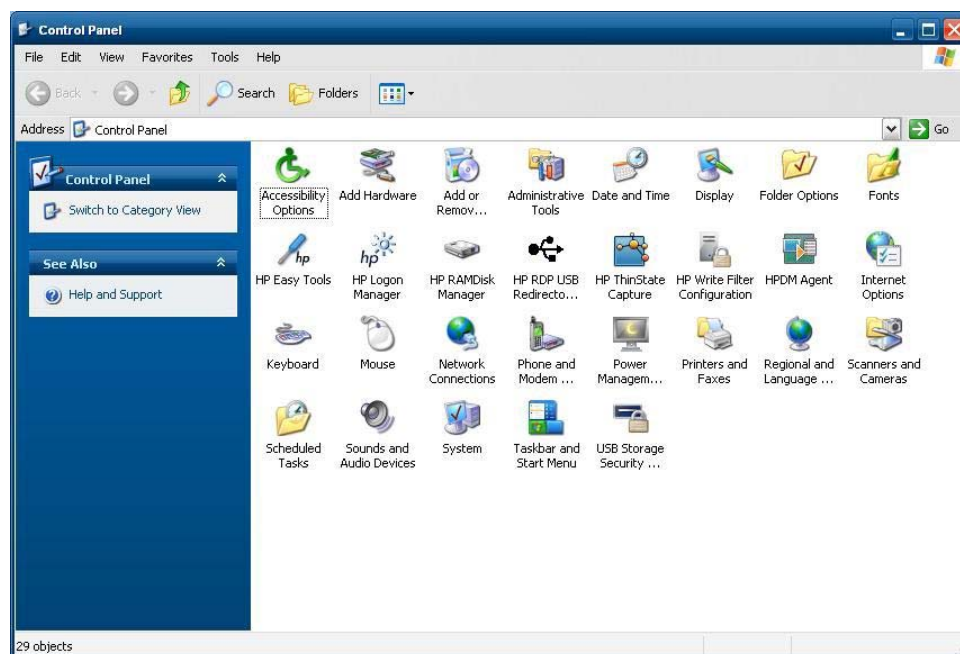


5 Control Panel Extended Selections

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:


- [Write Filters on page 33](#)
- [HP RAMDisk on page 40](#)
- [HP Easy Tools on page 41](#)



Write Filters

Choosing the Write Filter

HP Windows Embedded Standard Thin clients include both the Enhanced Write Filter (EWF) and the File-based Write Filter (FBWF) to protect the operating system. The Enhanced Write Filter is the factory default.

 **TIP:** Choose the Enhanced Write Filter to protect the entire flash from writes, or choose the File-based Write Filter to allow specific local applications and files to be updated dynamically.

To select the EWF or FBWF, perform the following steps:

1. Log in as an Administrator.
2. Select **Start > Control Panel > HP Write Filter Configuration**.
3. Select and configure the desired write filter.
4. Reboot the system for the chosen write filter selection and configuration to take effect.

Enhanced Write Filter Manager

WES 2009 includes the Enhanced Write Filter (EWF) console application command-line tool, `ewfmgr.exe`. In addition to the DOS command-line tool, the WES 2009 image includes 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.

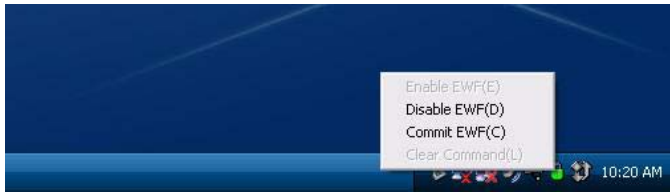
The intercepted flash writes stored in cache are available as long as the thin client remains active, but will be lost when the thin client is rebooted or shut down. To preserve the results of writes to the registry, favorites, cookies, and so forth, the contents of the cache can be transferred to the 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 may be able to correct this by issuing the command `'rundll32 c:\windows\system32\ewfdll.dll,ConfigureEwf'` from an Administrator's command prompt (type the command exactly as shown without the quotes) and reboot. If this is unsuccessful, you will need to re-flash the thin client unit with the standard factory image provided on the Web.

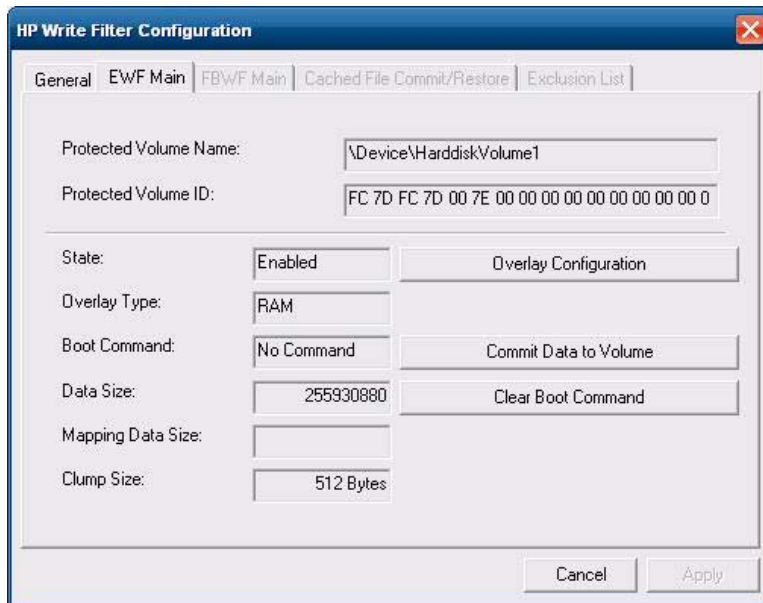
If you are logged-on as Administrator, you can change the status of EWF by right-clicking on the icon and selecting the desired EWF state.

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 (part of the HP Write Filter Configuration) can be accessed through the Control Panel or the Administrative Tools option only by 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
Overlay Configuration	This button simply brings to view 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:

```
EWFMGR <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.

File-Based Write Filter Manager

WES 2009 includes the File-Based Write Filter (FBWF) console application command-line tool, `fbwfmgr.exe`. In addition to the DOS command-line tool, the WES 2009 image includes a Write filter GUI. FBWF maintains the appearance of read and write access to write-sensitive or read-only storage to the operating system, making read and write access transparent to applications.





Benefits of the File-Based Write Filter

The FBWF 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 maintains the appearance of read and write access to write-sensitive or read-only storage to the operating system, making read and write access transparent to applications. File and/or folder exclusions can be configured to allow certain changes to persist, while preventing others from writing to disk.

File-Based Write Filter Status Service

This service creates an icon in the System Tray that shows the status of FBWF. The FBWF Status icon will appear as a red 'lock' when disabled and a green 'lock' when enabled.

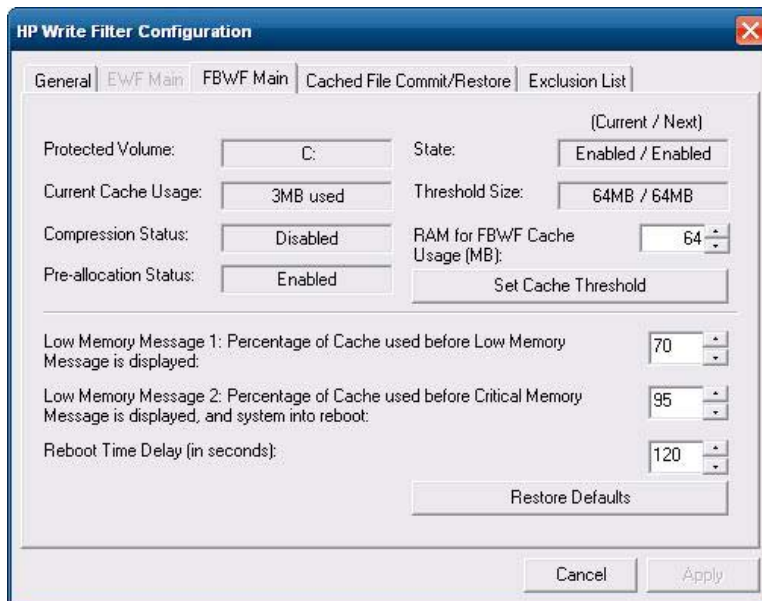
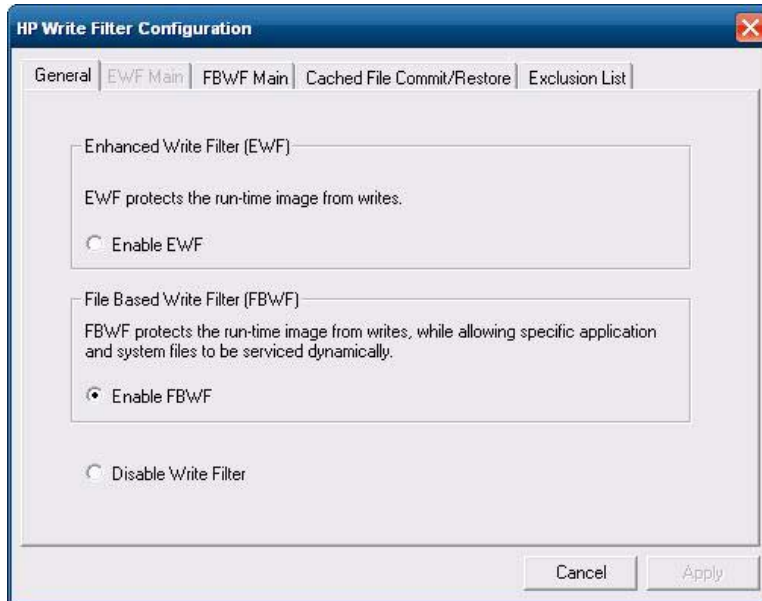


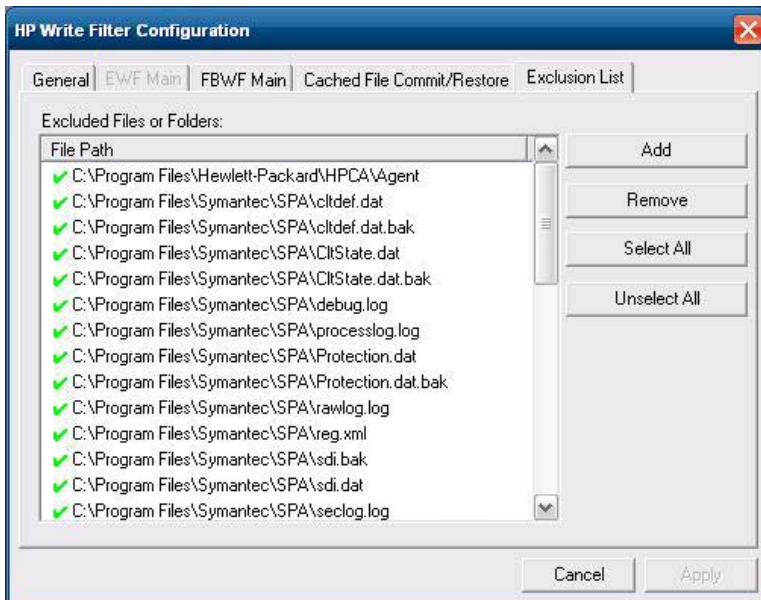
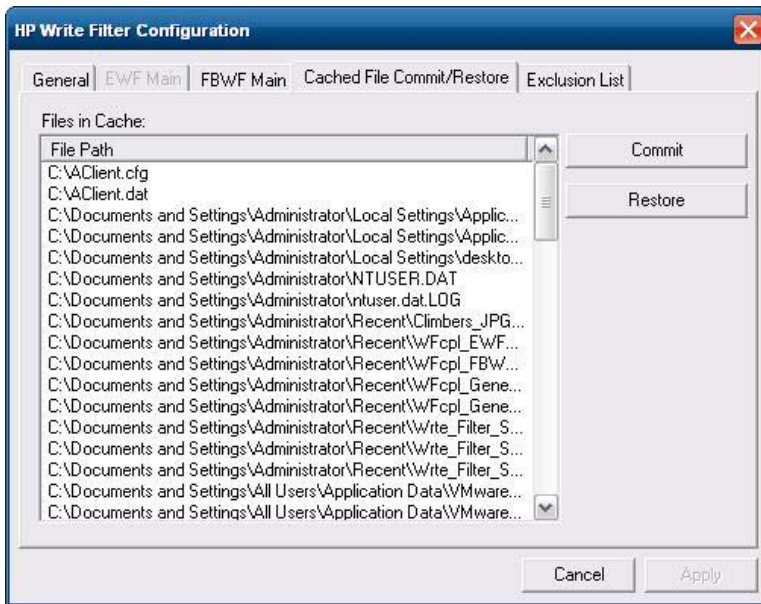
Status	Description	Example
Red	Disabled	
Green	Enabled	
Yellow	Commit Mode	
Yellow with Red 'X'	Write Filter Corrupted	

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

File-Based Write Filter GUI

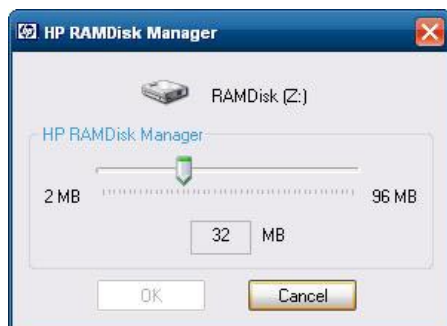
The FBWF GUI (part of the HP Write Filter Configuration) can be accessed through the Control Panel or the Administrative Tools option only by the administrator.





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

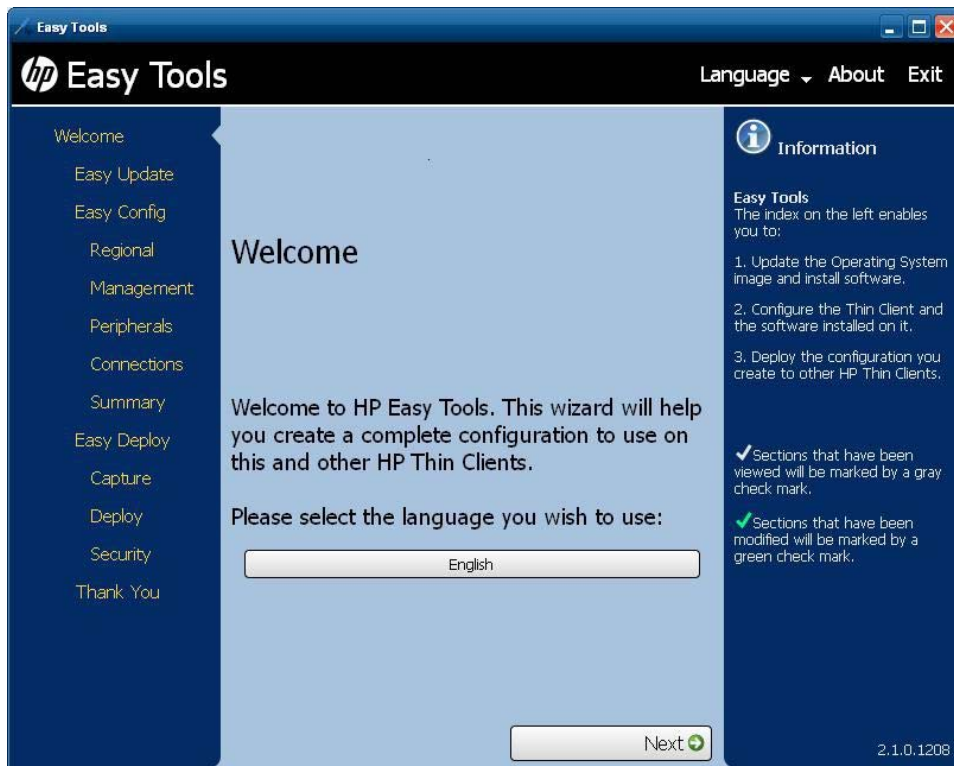
You can also use the RAMDisk for temporary storage of other data (such as roaming profiles) at the administrator's discretion (see [Local Drives on page 11](#)).

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 32 MB. The maximum RAMDisk size that you can set is 96 MB. The minimum is 2 MB. When installing an application that requires greater than 16MB, you may want to temporarily increase the size of the RAMDisk.

HP Easy Tools

The HP Easy Tools wizard helps you to create a thin client configuration. You can use this configuration on a single thin client or deploy it to multiple thin clients with HP ThinState or HP Device Manager.



For more information, see the *HP Easy Tools Administrator's Guide* at <http://www.hp.com/support>.

6 Administration and Image Upgrades

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

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 2009 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/region 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


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>.

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 2009 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 on page 26](#).

Altiris Deployment Solution Software

 **NOTE:** Although the Altiris Client agent is preinstalled, a free license is no longer included on the HP t5740 Series and all new HP thin clients going forward. To purchase a license, contact Altiris at <http://www.altiris.com>.

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 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.

To download your restore image Softpaq, visit the HP Web site at <http://www.hp.com/support>. Select the country from the map, then click **Support & Drivers**. Select **Download drivers and software (and firmware)**, type the thin client model in the field, and click **Enter**. Choose your operating system, and then select and download the appropriate image.


Image Upgrades


Some management tools require PXE to install an operating system image. 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.

Add-on Upgrades

If you want to install an add-on module, you can use the HP Device Manager, HP Client Automation or Altiris Deployment Solution 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.

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 24](#) and [HP Management Agent on page 25](#).


For more information about available peripherals, go to <http://www.hp.com/support> and search for the specific thin client model. 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://www.hp.com/support>. Select the country from the map, then click **Support & Drivers**. Select **See support and troubleshooting information**, type the thin client model in the field, and click [Enter](#).

 **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 2009-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/region 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://www.hp.com/support>. Select the country from the map, then click **Support & Drivers**. Select **See support and troubleshooting information**, type the thin client model in the field, and click **Enter**.

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 12
 - user 12
 - add-on modules 44
 - add-on upgrades 44
 - adding printers 45
 - administration 42
 - Administrative Tools 16
 - administrator
 - desktop 4
 - logon 8
 - Altiris 6
 - Client Agent 24
 - deployment server 6
 - Deployment Solution 43
 - Altiris Web site 6
 - applications 17
 - audio 47
 - automatic logon 7
- C**
 - Capture 5
 - changing the password 8
 - Citrix 19
 - Citrix ICA 5
 - Citrix Web site 19
 - client agent, Altiris 24
 - Client Automation 6, 25, 42
 - configuration 41
 - Control Panel 32
 - creating user account 12
- D**
 - default passwords 8
 - deployment server, Altiris 6
 - desktop 3
 - desktop administrator 4
 - desktop, user 3
 - Device Manager 6, 25, 42
 - disk on key requirements 28
 - drive C 11
 - drive Z 11, 40
 - drives 11
 - drive C and flash 11
 - drive Z 11
- E**
 - Easy Tools 41
 - emulation
 - TeemTalk Terminal Emulation 22
 - terminal 5
 - Enhanced Write Filter Manager 33
 - extended selections, control panel 32
- F**
 - features, thin client 2
 - File-Based Write Filter Manager 37
 - filter
 - write 11, 33, 37
 - Write Filters 9
 - firewall
 - Symantec Endpoint Protection 18
 - flash drive 11
- H**
 - HP Client Automation 6, 25, 42
 - HP Compaq Thin Client Imaging Tool 43
 - HP Device Manager 6, 25, 42
 - HP Easy Tools 41
 - HP Management Agent 25
 - HP RALF 25
 - HP RAMDisk 40
 - HP Registration and Agent Loading Facility 25
 - HP support Web site, 17
 - HP ThinState 26
 - HP ThinState Capture 5, 26, 42
 - HP ThinState Deploy 30, 42
 - HP Universal Print Driver 46
- I**
 - ICA 5
 - image capture 26
 - image capture and deploy 26
 - image deployment 30
 - image upgrades 42, 43
 - imaging tool 43
 - information, Web sites 1
 - internet 3
 - Internet Explorer 30
 - Internet Explorer unsafe file list 30
- L**
 - language options 15
 - local drives 11
 - log on as Administrator 8
 - logging off 9
 - logon
 - automatic 7
 - manual 8
 - Logon Configuration Manager 7
- M**
 - Management Agent 25
 - Management Services 5
 - manual logon 8
 - manufacturer print drivers 46
 - mapping network drives 12
 - Media Player 31
 - memory, volatile 11

Microsoft Internet Explorer 30
Microsoft Internet Explorer unsafe
file list 30
Microsoft RDP 5, 20
monitor saver 10
multimedia 2

P

password 8
password, changing 8
peripherals 45
peripherals, QuickSpecs Web
site 45
PN Agent 19
power management 10
preinstalled applications 17
print driver 46
print drivers 46
printers 45
printers, adding 45
profiles 13
program neighborhood agent 19
PXE 43

R

RALF 25
RAMDisk 40
RDP 5
receiver, RGS 22
redirecting USB drives 20
regional language options 15
Registration and Agent Loading
Facility 25
Remote Desktop Connection 20
Remote Desktop Protocol 20
Remote Graphics Software
receiver 22
requirements
disk on key 28
server 4
restarting 9
RGS receiver 22
roaming profiles 12

S

saving files 12
security 2
Microsoft 18
Symantec Endpoint Protection
firewall 18
server requirements 4

server, Altiris deployment 6
services, session 5
session services 5
shutting down 9
Symantec Endpoint Protection 18
system time 10

T

TeemTalk Terminal Emulation 22
terminal emulation 5
text-only print driver 45
Thin Client Imaging Tool 43
Thin Client Management Services
5
ThinState Capture 5, 26, 42
ThinState Deploy 30, 42
time utility 10

U

Universal Print Driver 46
unsafe file list for Internet
Explorer 30
upgrades 42
upgrades, add-on 44
upgrading images 43
USB drives, redirecting 20
USB enhancements 20
user
accounts 12
profiles 13
user desktop 3
User Manager 13
utilities 13
Client Automation 42
system time 10
Thin Client Imaging Tool 43
Universal Print Driver 46

V

VMware View Manager 23
volatile memory 11

W

Web site 6
Citrix 19
HP support 17
more information 1
peripheral QuickSpecs 45
Windows Media Player 31
Windows Media Player 31

Windows Media Player Web site
31
write filter 11, 33, 37
Write Filters 9

Z

Z drive 40