Quick Reference Guide for Microsoft Windows XPe-based Thin Clients - t5720 & t5730

Quick Reference Guide

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.

First Edition (January 2008)

Document Part Number: 453901–001

About This Book

This guide supplements the standard Microsoft Windows XPe documents supplied by Microsoft Corporation. This document highlights the differences, enhancements, and additional features provided 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.

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

Table of contents

1 Introduction

HP Compaq t57x0 thin client models use the Microsoft Windows XP Embedded (XPe) operating system. 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
  - Latest versions of Citrix Program Neighborhood, Microsoft RDP, and TeemNT
- User interface similar to familiar Windows XP Professional
- Improved security
  - Sygate Firewall
  - Microsoft Firewall
  - Locked down protected Flash drive
- Multimedia
  - Windows Media Player
  - Midi (Add-on)
  - Windows Messenger
  - Macromedia Flash
- Internet browsing
  - Internet Explorer
  - Adobe Acrobat (Add-on)
  - Sun JVM (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-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 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.

Updates

HP provides add-ons, 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 your image version at http://welcome.hp.com/country/us/en/support.html.

The XPe desktop

This section provides a general overview of Windows 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 Windows XP 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 from **Start** > **Programs**.

NOTE: Links to remote ICA NFuse-published applications may also 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 Windows XPe desktop and Start menu items, refer to the applicable Microsoft documentation at http://msdn2.microsoft.com/en-us/embedded/aa731409.aspx.

For the Web addresses of the Citrix Program Neighborhood and Microsoft RDP help documents, see Citrix Program Neighborhood on page 22.

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

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

For information about the functionality of the standard Windows XPe desktop and Start menu items, refer to the Microsoft Web site at http://msdn2.microsoft.com/en-us/embedded/aa731409.aspx.

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 your 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 Citrix MetaFrame or Presentation Server for Microsoft Windows 2000 Server family, and Windows 2003 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 Server with Terminal Services installed
- Microsoft Windows Server 2000/2003

NOTE: If a Windows 2000/2003 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 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/def ault.asp.

Terminal emulation support

All t57x0 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 service - Altiris Deployment Solution

The Altiris Deployment Solution™ support service is available for your 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 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 your thin client. The Altiris Deployment Solutions software uses a Preboot Execution Environment (PXE) session and protocol to reimage or recover your 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*.

2 Configuration

Logging on

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

Automatic logon

The default for the 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 issue the `-commit` command anytime during the current boot session. See Enhanced Write Filter Manager on page 29 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 Accounts** 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, use the mouse to initiate logoff of the User (invoked from the **Start** menu).

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. For instructions for logging on as a different user, see Logging on on page 5.

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 29. 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.

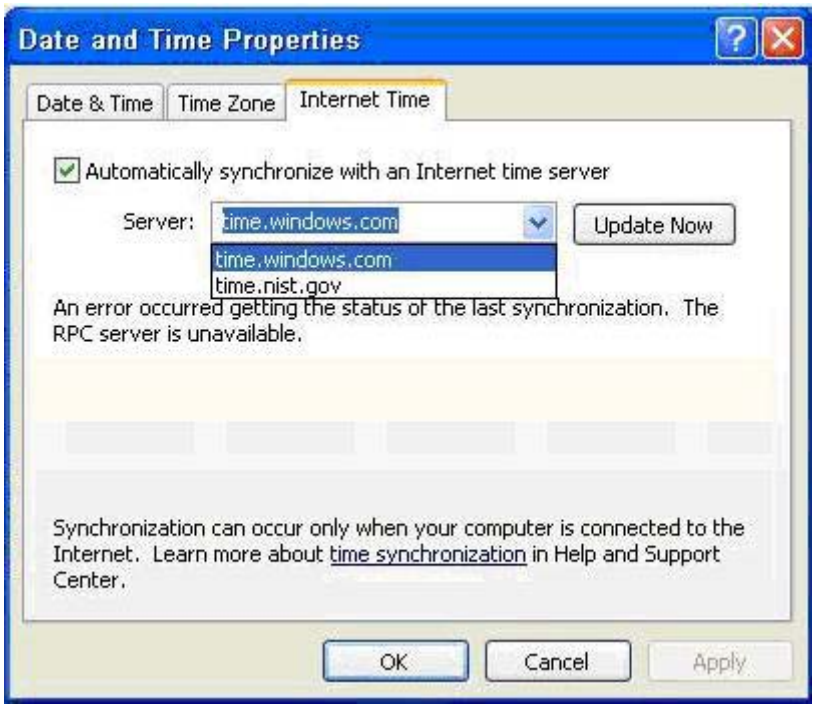
A user logon account does not have write filter disabling privileges; this is a local or remote administrator function.

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. Parameters for this mode are available by right-clicking on the desktop background and selecting **Properties** > **Screen Saver** > **Power**.

System time

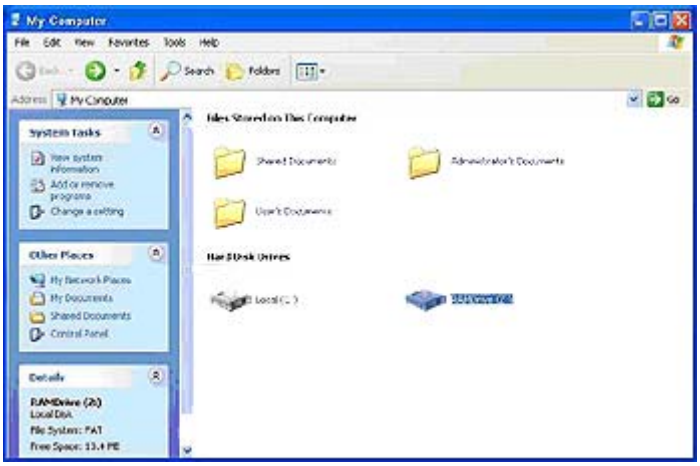
After power off, clock time is not lost as long as the power source remains plugged in. You can manually set the local time, or you can automatically set the local time utility to synchronize the thin client clock to a time server at a designated time.



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 32. For information about using the Z drive for roaming profiles, see Roaming profiles on page 10.

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 3 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 29 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 your 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 11.

Mapping network drives

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

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 or by other means known to administrators.

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

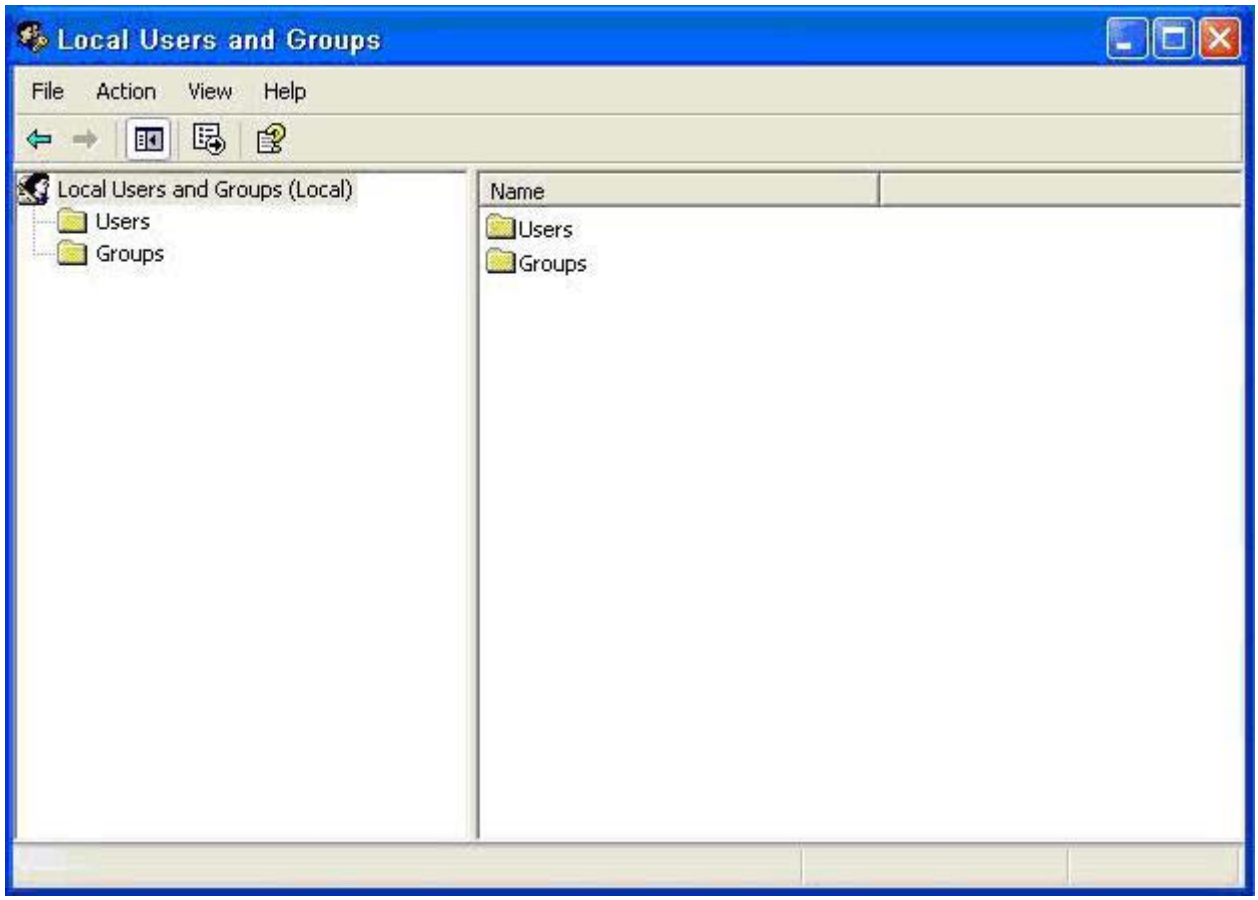
△ **CAUTION:** Make sure to disable the write filter cache during the boot session in which a new account is created. Remember to enable the write filter after saving all of your permanent changes to flash.

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** > **Performance and Maintenance** > **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 profile is automatically configured from a template based on the default user or administrator access settings in the registry, browser profiles, and ICA and Microsoft RDP initial settings. If the default user or administrator profile settings are changed from those set at the factory, the changed settings are automatically applied to the new user profile.

For the new user to match the characteristics of the default user, the administrator must create the user in the User group and add the new user to the Administrator group. The default user is in both groups; 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 Administrator group.

To create the user:

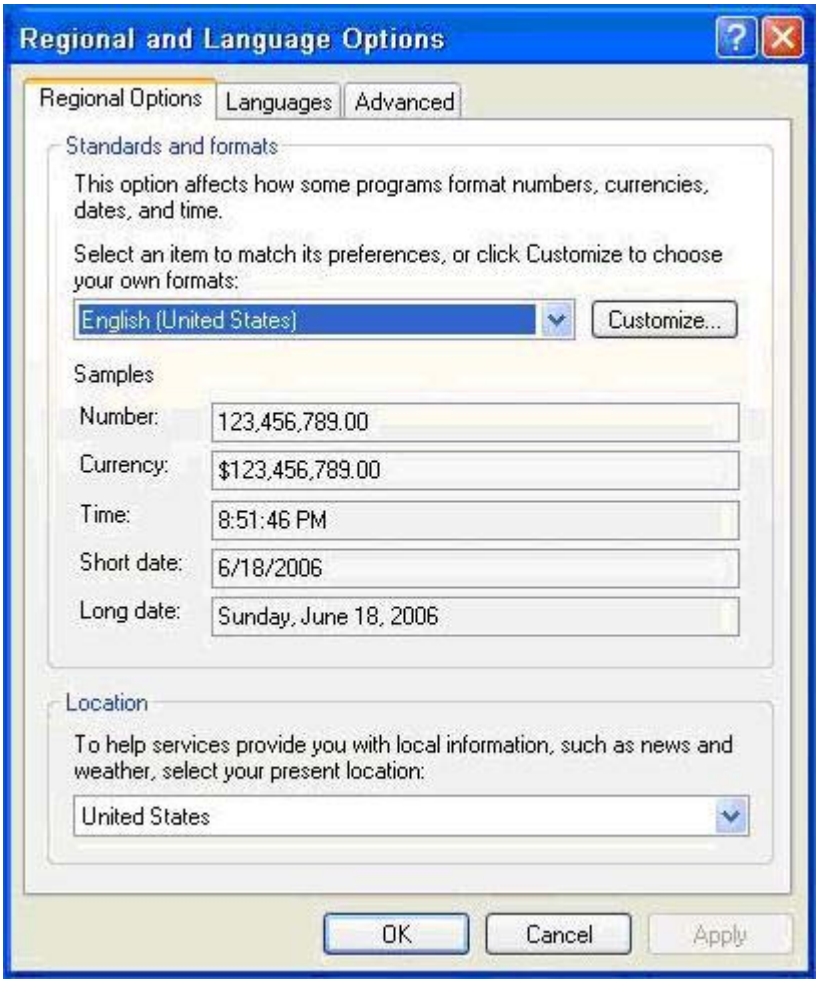
△ **CAUTION:** Because of the limited size of flash memory, HP strongly recommends that you configure other applications available to the new and existing users to prevent writing to the local file system. For the same reason, HP also recommends that you exercise extreme care when changing configuration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

1. Log in as Administrator.
2. Open the **Administrative Tools** window by clicking **Start** > **Control Panel** > **Performance and Maintenance** > **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, then and 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 `Administrators` 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 administrators and users groups and should match the privileges of the default user account.

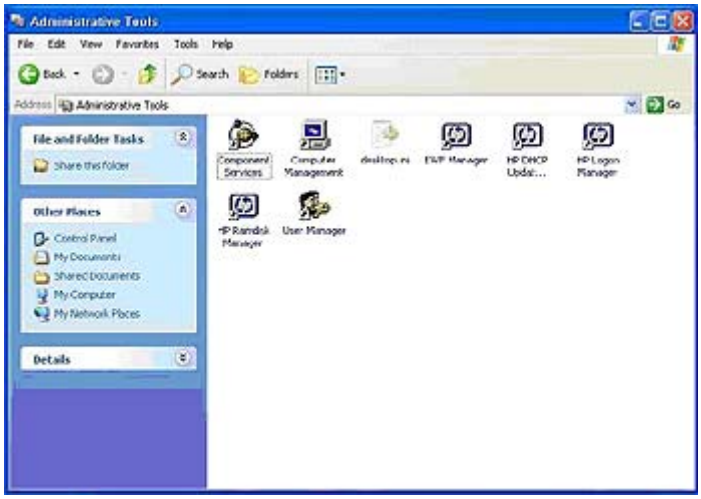
Regional and Language Options

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:



3 Applications

The XP Embedded image that ships with your thin client has the following preinstalled applications:

- Sygate Firewall
- Citrix Program Neighborhood
- Microsoft RDP
- HP PC Session Allocation Manager (SAM) Client
- TeemNT Terminal Emulation
- Altiris Client Agent
- Internet Explorer
- Windows Messenger
- Media Player
- Macromedia Flash Player

Access to the following applications is limited to the Administrator logon account:

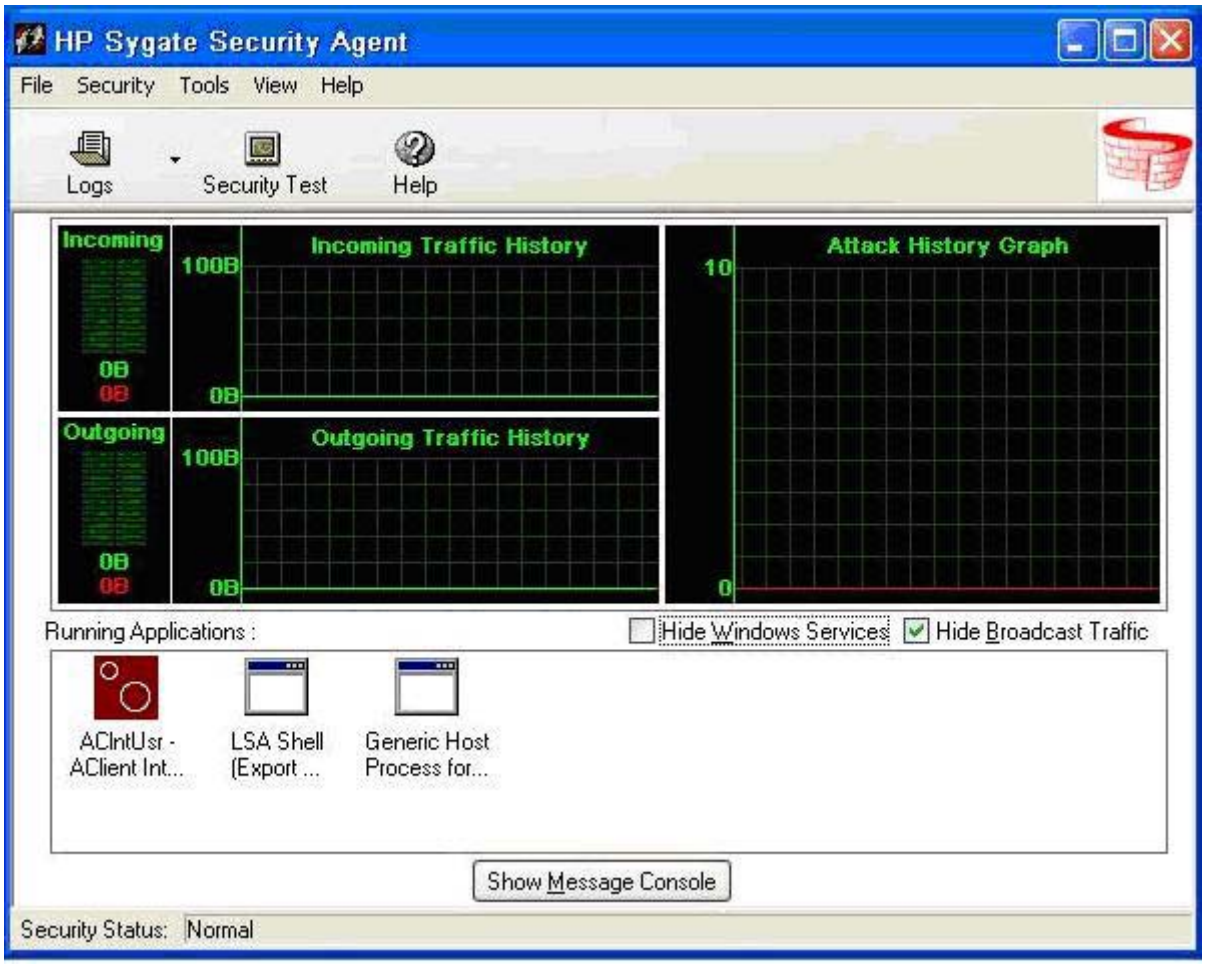
- Sygate Firewall
- Altiris Client Agent
- Macromedia Flash Player

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://welcome.hp.com/country/us/en/support.html.

Sygate firewall

The HP XPe SP2 image includes a Sygate firewall.



HP Sygate Security Agent provides a customizable firewall that helps protect your computer from intrusion and misuse, whether malicious or unintentional. The firewall detects and identifies known Trojans, port scans, and other common attacks, and in response, selectively allows or blocks the use of various networking services, applications, ports, and components.

HP Sygate Standalone Agent has the ability to allow or block any port or protocol, inbound or outbound, by either application or traffic signature. The Agent not only blocks according to these parameters, but can also link them with logical and/or conditional statements, increasing the scope and flexibility of polices that you can apply. The Agent can also block and apply policy to custom protocol adapters, enabling enterprises to use custom network-enabled applications and to block applications that circumvent the TCP/IP stack with custom protocol adapters.

Additional information about the Sygate Firewall is available in the *HP Sygate Security Agent and Symantec Embedded Security: Frequently Asked Questions* white paper at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00632596/c00632596.pdf.

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.

NOTE: The Microsoft Windows Firewall is provided only as an add-on and is not included in the image. Before installing the Microsoft Windows Firewall, you must remove the Sygate Firewall. A Sygate Firewall removal add-on is available at http://welcome.hp.com/country/us/en/support.html.

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.

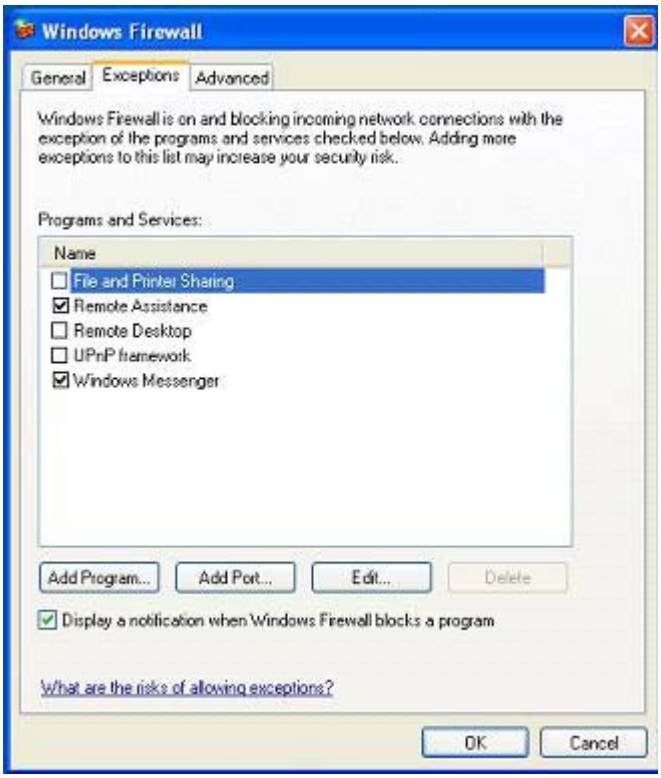
- **General Tab**: The General tab provides access to the main three configuration options as shown below.
  - On (Recommended)
  - Don’t allow exceptions
  - Off (Not Recommended)

  When you select Don't allow exceptions, Windows Firewall blocks all requests to connect to your 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 your computer by blocking all attempts to connect to your 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.

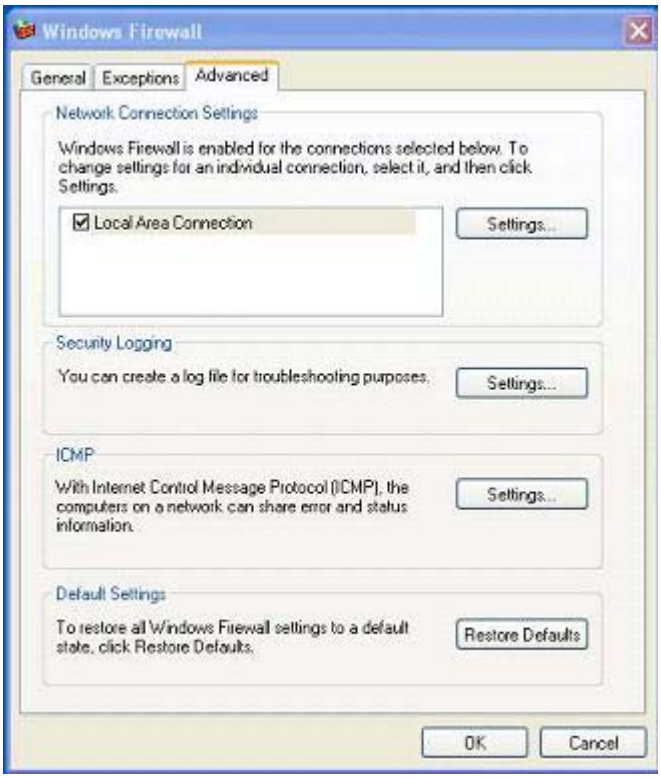
  You can specify three different modes of access:
  - Any computer (including those on the Internet)
  - My network (subnet) only
  - Custom list



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 Windows XPe 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.

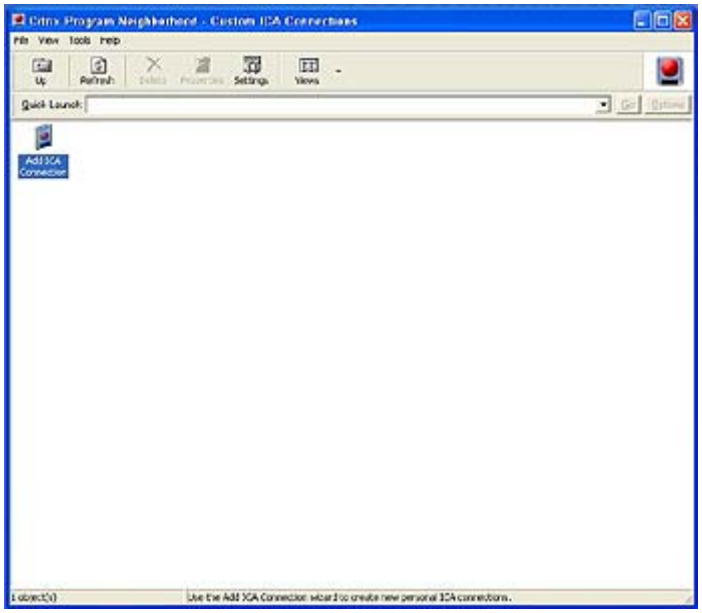
Once you have the port number and protocol, add an exception for that port.

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

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.



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

Remote Desktop Connection

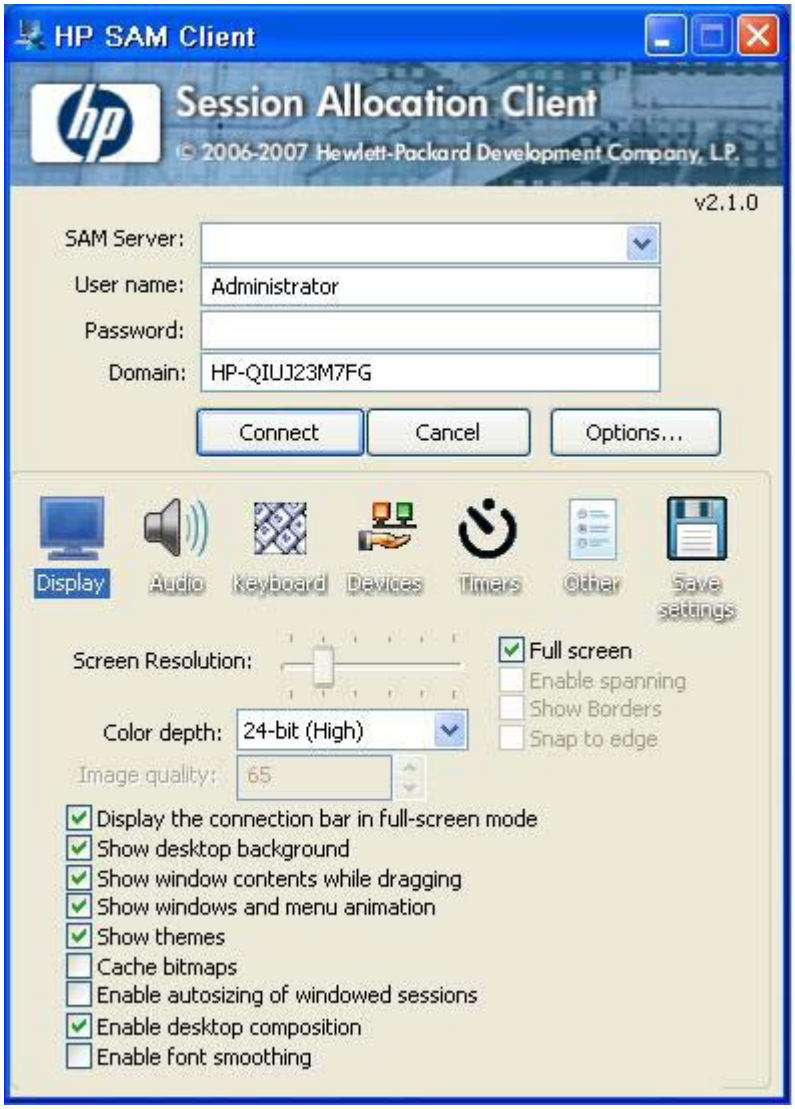
Use the Remote Desktop Connection dialog box to establish connections to a Windows Terminal Server or to access remote applications using Microsoft RDP.

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

HP PC 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 PC Session Allocation Manager (HP SAM) and is an extension the HP SAM client. HP SAM client is included in the latest HP Thin Client XP Embedded image, and can be accessed from **Start** > **Programs**.

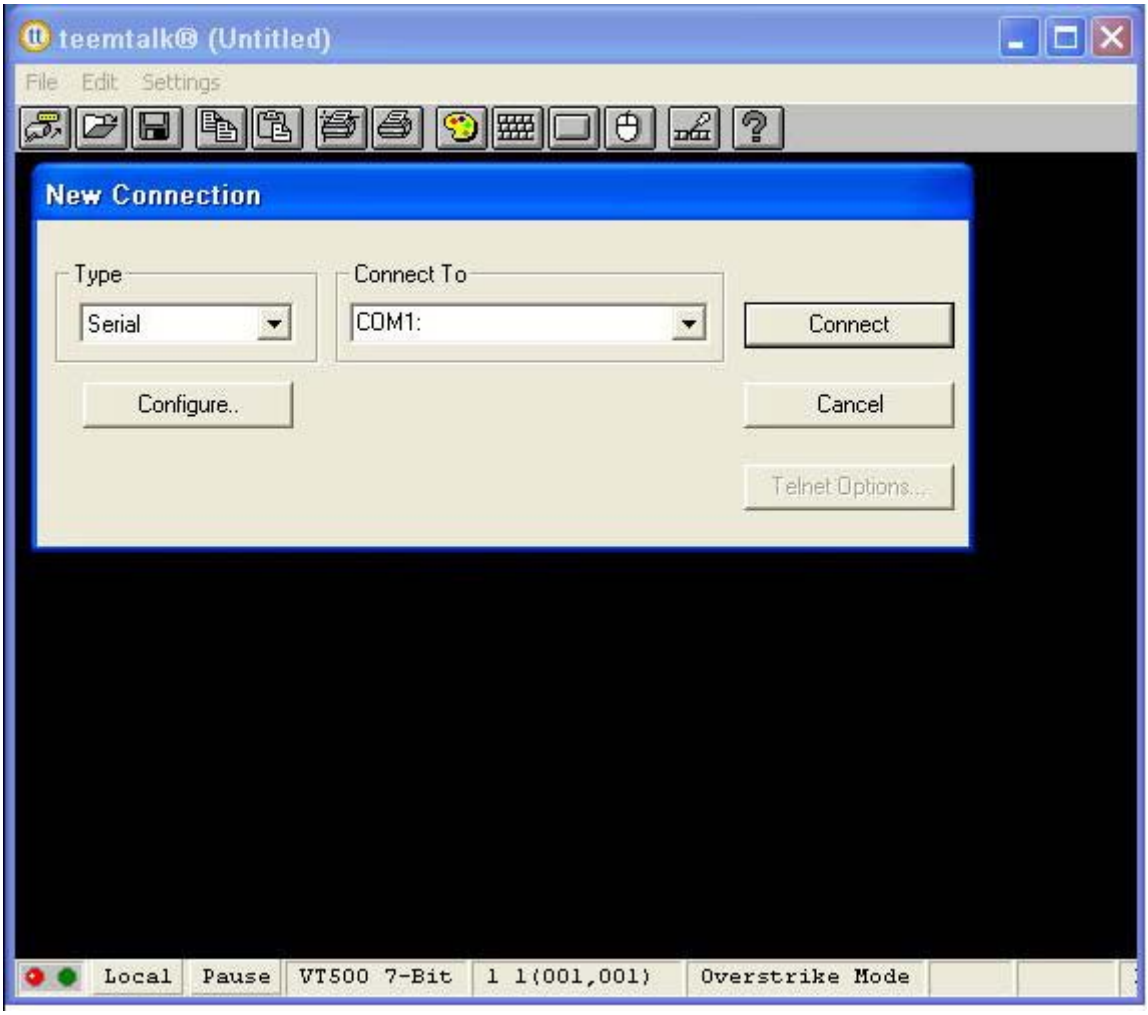


HP SAM becomes the control point in managing a CCI deployment. Specifically, it manages the assignment of Microsoft Remote Desktop connections from a user's access device (thin client) to Remote Desktop sessions (blade PCs). Whether the session resides on a dedicated physical blade or resides together 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 PC SAM, see http://h71028.www7.hp.com/enterprise/cache/323204-0-0-225-121.html.

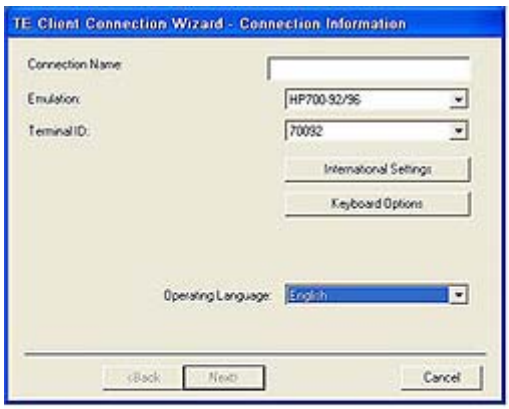
TeemNT Terminal Emulation

All t57x0 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 TeemNT Connection Wizard and the TeemNT Emulator from Start > All Programs.



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.



Microsoft Internet Explorer

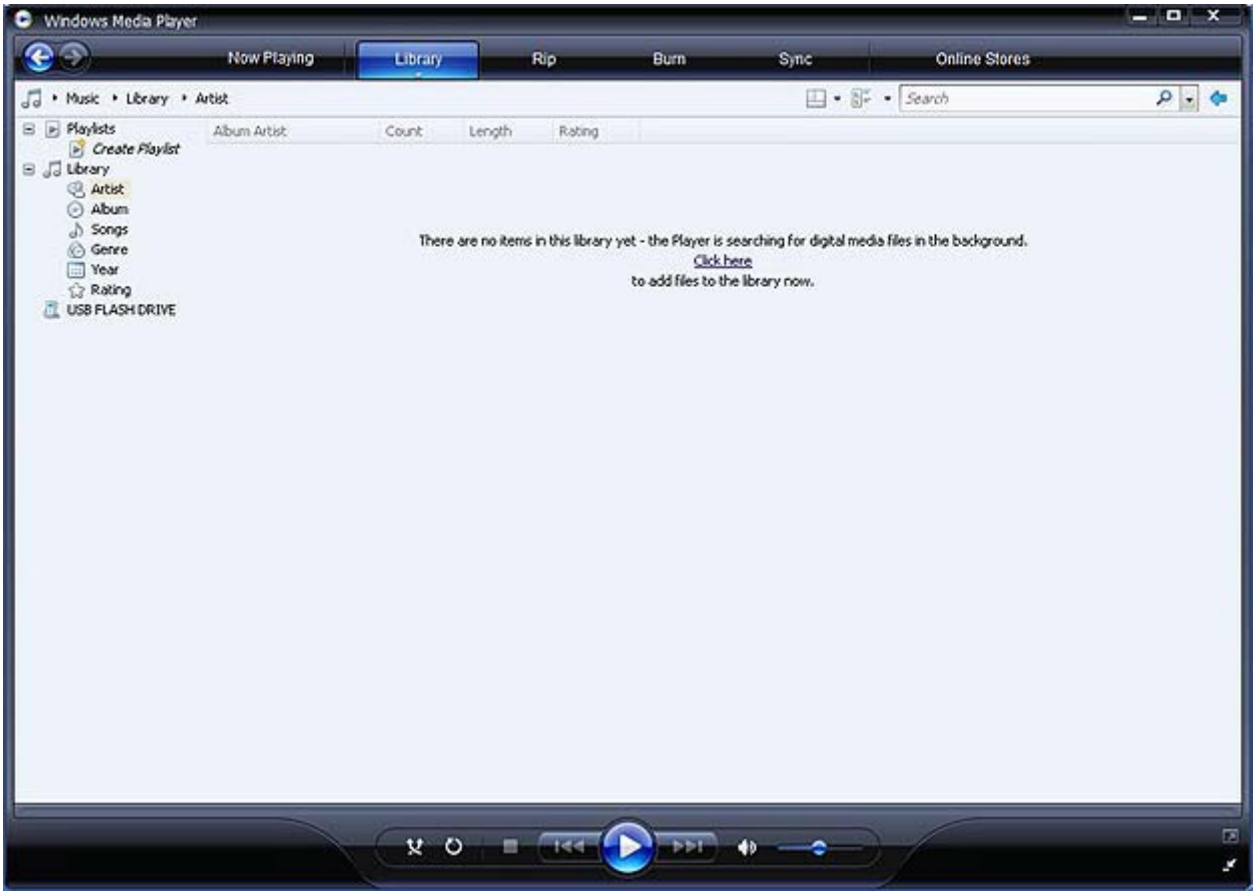
Version 7.0 of the Microsoft Internet Explorer browser is installed locally on the thin client. The Internet options settings for the browser have been preselected at the factory to limit writing to the flash memory. These settings prevent exhaustion of the limited amount of flash memory available and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

Service Pack 2 makes Microsoft Internet Explorer 7.0 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.

Windows XPe Service Pack 2 added a block unsafe file transfers feature to Windows Messenger. 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://go.microsoft.com/fwlink/.

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.



Macromedia Flash Player

Macromedia Flash Player is the agent for rich Web experiences across multiple platforms. With Macromedia Flash Player, Web users worldwide can view and interact with content developed in Macromedia Flash.

Some Web sites require newer versions of the player. To install newer players, administrator must temporarily increase the RAMDisk to 64MB using the HP RAMDisk control panel applet.

4 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

The Enhanced Write Filter Manager provides a secure environment for thin client computing by protecting the thin client from undesired flash memory writes (the operating system and functional software components reside in flash memory). 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 that are stored in cache are available as long as the thin client remains active, but are lost when you reboot or shut down the unit. To preserve the results of writes to the registry, favorites, cookies, and so forth, transfer the contents of the cache to the flash on demand using the Altiris Deployment Solution software or manually using the Enhanced Write Filter Manager.

After you disable the write filter, all future writes during the current boot session are written to the flash with no further caching until reboot. You can also enable/disable the write filter using the command line. Always enable the writer filter after you have made all of your permanent changes.

The administrator should periodically check the status of the cache and reboot the thin client if the cache is more than 80 percent full.

△ **CAUTION:** Never disable the write filter cache if it is more than 80 percent full.

Access to the Enhanced Write Filter is limited to the Administrator account.

NOTE: To avoid flash corruption when administering the thin client for permanent changes, HP strongly recommends that you disable the write filter cache before making permanent modifications to the system. Remember to enable the writer filter after making all of your changes.

The following section describes how you can manipulate the write filter through the command line.

Enhanced Write Filter Manager command line control

△ **CAUTION:** Terminal Administrators should use Microsoft Windows NT file security to prevent undesired usage of these commands.

When using the `-commit` command, all the temporary contents are permanently written to the flash memory.

NOTE: Because the Enhanced Write Filter Manager commands are executed on the next boot, you must reboot the system for the command to take effect.

Windows XPe includes the Enhanced Write Filter (EWF) console application command line tool, Ewfmgr.exe, which you can use 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 your configuration and building it into your image, you enable use of Ewfmgr.exe and the corresponding commands.

To use the Enhanced Write Filter Manager using the command line:

1. Select **Start** > **Run** > **Open**.
2. Type `CMD` in the Open field to access the system DOS prompt.
3. Click **OK**.

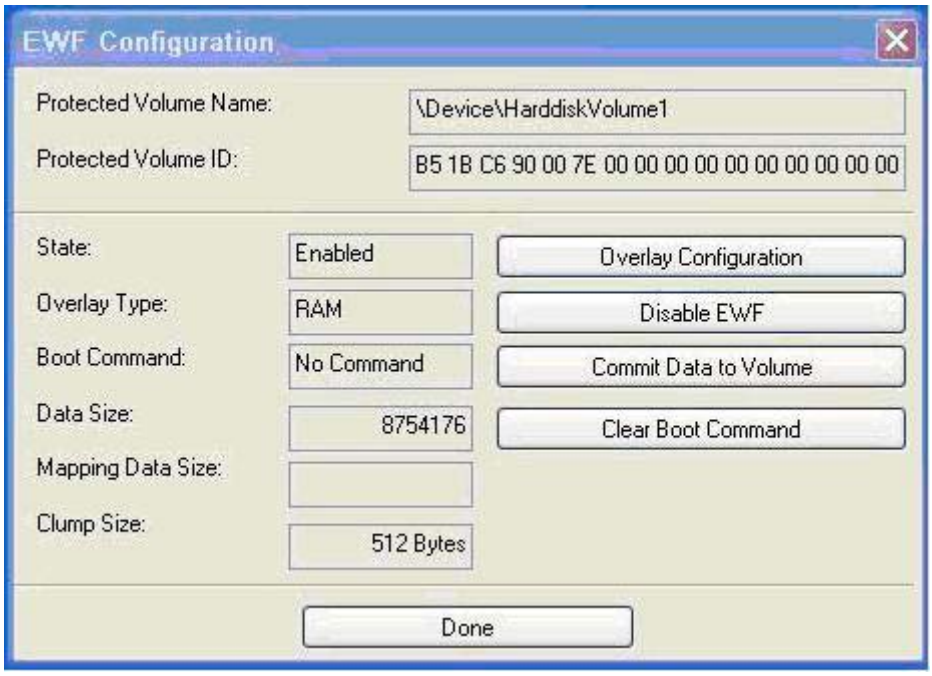
4. Type `ewfmgr c:`.
5. Press Enter.

Using the `ewfmgr <drive-letter> -[boot command]` syntax, use the following commands in the boot command variable of the command line:

- **-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 value to 1. You can combine `-commit` with the `-disable` command to commit and then disable.
- **-disable**: Disables the overlay on the specified protected volume.
- **-enable**: Enables the Enhanced Write Filter so that data written to the protected media is cached in the overlays. The current overlay level becomes 1 as soon as EWF is started, and a new overlay is created at level 1.
- **-commitanddisable**: Combination of the commit and disable commands. This command commits data in the overlay upon shutdown and disables EWF after the system reboots.

Enhanced Write Filter user interface

In addition to the DOS command-line tool, the Windows XP Embedded image includes an Enhanced Write Filter (EWF) user interface. You can access the EWF interface through the Control Panel or the Administrative Tools option for the administrator.



To access the EWF user interface:

1. Log in as an Administrator.
2. Select **Start** > **Control Panel** > **Other Control Panel Options** or **Start** > **Control Panel** > **Performance and Maintenance** > **Administrative Tools**.

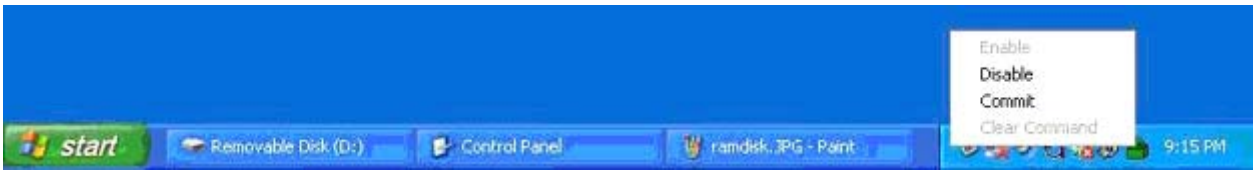
3. Click the **EWF Manager** icon.
4. Use the EWF user interface to select **Write Filter** options.

The EWF user interface includes the following buttons:

- **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 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.

Enhanced Write Filter status tool

The HP XPe Images include an EWF status service, which creates an icon in the System Tray that shows the status of the EWF. In addition, you can right-click on the icon to display and execute the available options.



The EWF Status icon appears as a:

- red lock when disabled
- green lock when enabled
- yellow lock when the state is set to change on next boot

NOTE: In the event of a corrupted EWF state, you must re-flash the thin client with the standard shipping image provided on the Web. For additional information, see the *HP Compaq Thin Client Imaging Tool* white paper located at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00485307/c00485307.pdf.

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

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

If you modify the EWF using the command line, you must right-click the icon (you can then click anywhere on the screen to close the context menu) to refresh the status icon display. The status icon display is refreshed automatically when you make modifications through the EWF Control Panel applet. The EWF applet always reflects the current status.

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 9).

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 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 settings to an HP XP Embedded 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://welcome.hp.com/country/us/en/support.html.

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 XP Embedded image, which you can then deploy to another HP thin client of identical model and hardware.

What do you need to have?

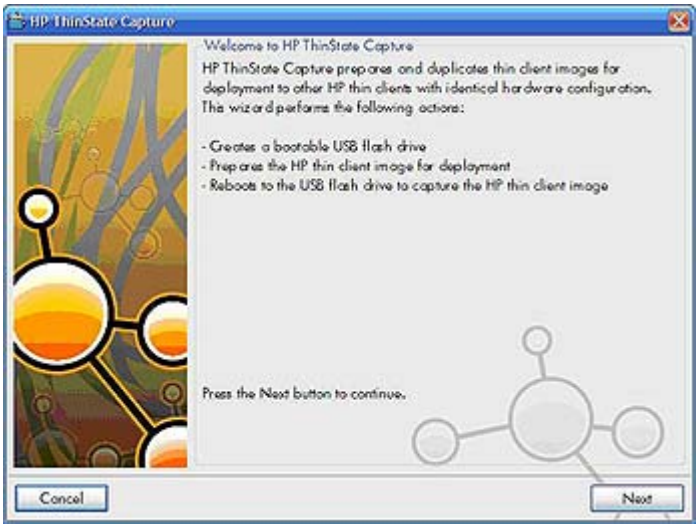
- An HP thin client XP embedded unit that contains the latest HP provided image
- An HP-approved USB flash drive (Disk-On-Key). Consult the t5720 quick specs for the latest approved USB flash drives.

⚠ **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 Bias Features section of the F10 System Bias to USB.

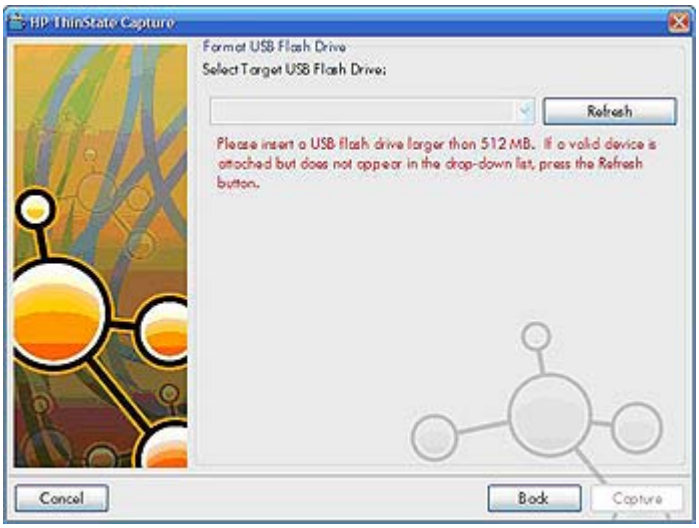
NOTE: The HP ThinState Capture tool is not a standalone tool and can only be accessed by the administrator from within the thin client image.

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.



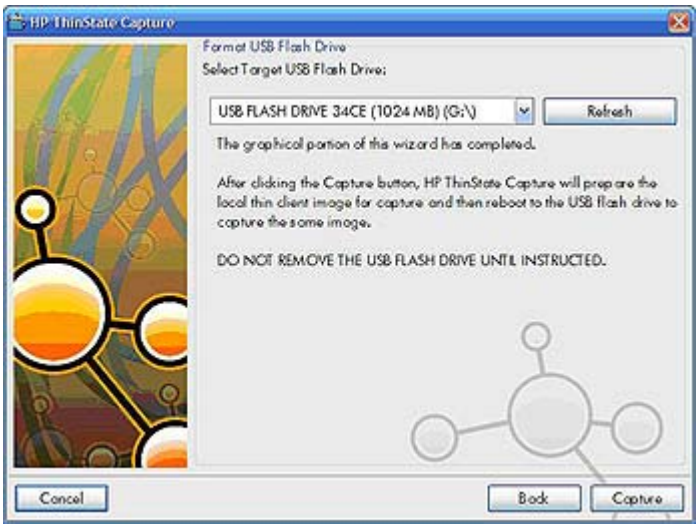
2. Click **Next**.



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 your 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.

5. 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.

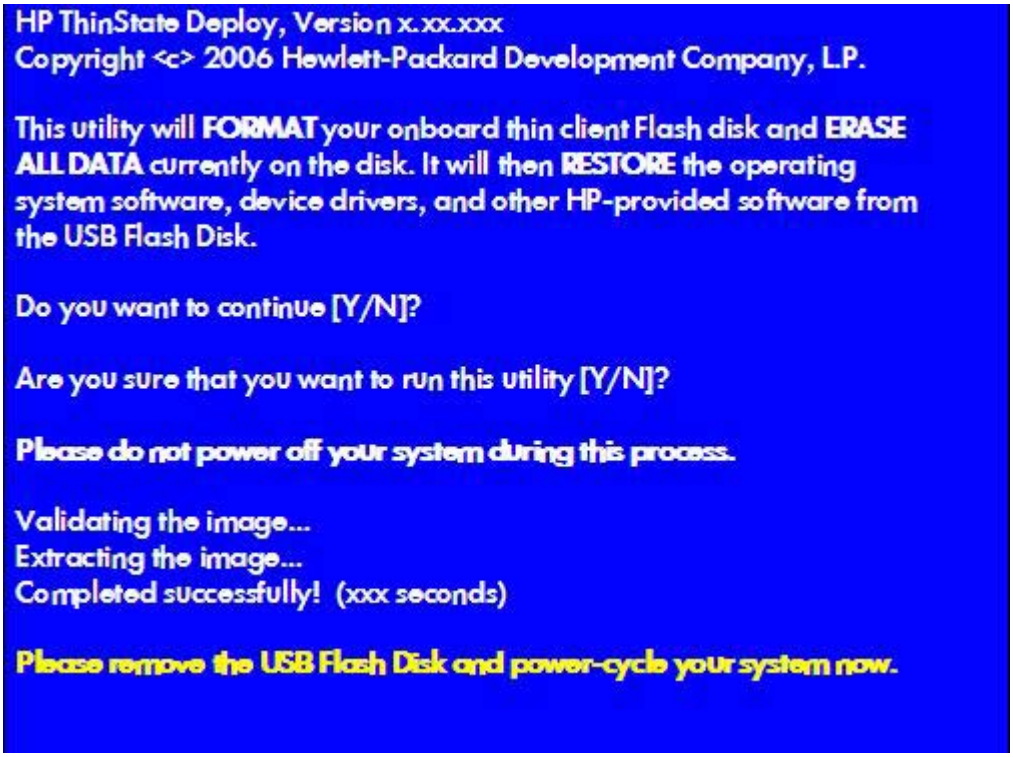
The following table lists the supported capture and deploy scenarios:

	Deploy To:		
	t5730	t5720	t5720
Capture From:	1GB Flash	512MB Flash	1GB Flash
t5730 1GB Flash	X		
t5720 512MB Flash		X	X
t5720 1GB Flash			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 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 Altiris' rdeploy.exe or rdeployt.exe utilities. Please consult the HP Compaq Thin Client Imaging Tool at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00485307/c00485307.pdf.

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

5 Administration and image upgrades

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

Add-on upgrades

If you want to install an add-on module, you can use the 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 3 MB, 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 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 XP Embedded 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 34.

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 Compaq t5000 thin client. You can use this utility to restore the original factory image to your thin client.

This utility allows you to perform the following options:

- Generate an ISO image to use with CD creation software to create a bootable CD for deployment using a USB CD ROM drive.
- 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 Universal Print Driver for Thin Clients Add-on

HP has developed a printing add-on for the t5700 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 www.hp.com, click **Software & Driver Downloads**, select your thin client model and then your 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.pdf.

6 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 Solution software. For more information, see Altiris Client Agent on page 26.

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.

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 Thin Clients white paper on the HP support site at http://welcome.hp.com/country/us/en/support.html.

△ **CAUTION:** If the available free space on the flash memory is reduced to less than 3 MB, 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.

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