Quick Reference Guide

Microsoft Windows XPe-based Thin Clients - t5000 Series

Document Part Number: 253378-007

October 2005

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.

The information in this document 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.

⚠ **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.

Quick Reference Guide

Microsoft Windows XPe-based Thin Clients - t5000 Series

Seventh Edition (October 2005)

Document Part Number: 253378-007

Contents

Introduction 1
Image updates 1
Server environment requirements 1
Session services 1
Citrix ICA. 2
Microsoft RDP 2
Terminal emulation support 2
Support service - Altiris Deployment Solution. 3
Extended Windows XPe features 3
Logging on 4
Automatic logon. 4
Manual logon 4
Administrator logon access 5
Pre-installed utilities 5
Altiris Client Agent 6
Citrix Program Neighborhood 6
Enhanced Write Filter Manager 6
Macromedia Flash Player. 6
Remote Desktop Connection 7
The XPe desktop. 7
User desktop. 7
Administrator desktop 8
Logging off from, restarting, and shutting down the thin client 9
Programs menu extended selections 10
Citrix Program Neighborhood 10
Remote Desktop Connection 11
TeemNT 11
Internet Explorer 11
Control Panel extended selections 11
HP RAMDisk. 11
Regional and Language Options 12

Administrative Tools 12

Peripherals 13

USB to Serial converter cable 13

Printers 14

Adding printers—using generic text-only print driver. 14

Using manufacturer print drivers 15

Audio 15

Microsoft Windows XPe Service Pack 2 (SP2) 16

Network protection 16

Sygate firewall 16

Microsoft Windows Firewall 17

Microsoft Internet Explorer 25

Windows Messenger. 25

Windows Media Player 9 25

Utilities and settings 25

Enhanced Write Filter Manager 26

Enhanced Write Filter Manager command line control. 27

Enhanced Write Filter user interface 28

Enhanced Write Filter status tool. 29

Local drives. 30

Drive Z 30

Drive C and Flash. 30

Saving files. 31

Mapping network drives 31

Roaming profiles 31

User log accounts 32

Creating a new user account. 32

User profiles 32

Remote Administration and firmware upgrades 34

Altiris Deployment Solution software 34

Add-on modules 34

Firmware upgrades. 34

HP Compaq Thin Client Imaging Tool. 35

Introduction

HP Compaq t57x0 thin client models use the Microsoft Windows XP Embedded (XPe) operating system. These thin clients provide access to applications, files, and network resources made available on machines hosting Citrix ICA and Microsoft RDP session services. Only the keyboard, mouse, audio/video, and display data are transmitted over the network between the thin clients and session servers.

Image updates

HP provides periodic updates to the image for HP Compaq t57x0 thin clients. Check the HP support site for important documentation that provides specific information for your image version. You can find support documentation at:

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

This guide provides information about Microsoft Windows XPe. For more information about the latest features, see "Microsoft Windows XPe Service Pack 2 (SP2)" on page 16.

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 where 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 and Presentation Server for Microsoft Windows NT 4.0, 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 RDP available on the network using any of the following services:

- Microsoft Windows 2000/2003 Server with Terminal Services installed
- Microsoft Windows NT 4.0 Terminal Server Edition
- Microsoft Windows Server 2000/2003

✎ 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:

http://www.microsoft.com/windows2000/technologies/terminal/default.asp

Terminal emulation support

All t57x0 thin-client models include third-party 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 NT 4.0 or 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: www.altiris.com/documentation and review the *Altiris Deployment Solution User Guide*.

Extended Windows XPe features

The operating system of the Microsoft Windows XPe-based thin client has extended features not found in the standard Microsoft Windows XP operating system. Controls for extended Windows XPe features are only available through the Administrator logon account with the exception of the following:

- Microsoft Terminal Server Client (Remote Desktop Connection Manager)
- Citrix Program Neighborhood
- If installed, a special-order terminal emulation application

△ **CAUTION:** 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 26 for instructions to disable the cache. Enable the write filter when you no longer want permanent changes.

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 Logon Manager in the Control Panel to enable/disable auto logon and change the auto logon user name, password, and domain. Only the administrator logon account can change auto logon properties.

✎ 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 26 for information about the write filter 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 manually enter 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 logon account, the factory-default user name and password are both **User**.
- For an administrator logon 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 log accounts" on page 32.

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 logon screen for Administrator logon displays.

✎ The default username and password for the Administrator account is **Administrator**. The default username and password for the User account is **User**.

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

Pre-installed utilities

There are several preinstalled utilities on the thin client, including:

- Altiris Client Agent
- Citrix Program Neighborhood
- Enhanced Write Filter Manager
- Macromedia Flash Player
- Remote Desktop Connection

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.

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.

Enhanced Write Filter Manager

Booting the system launches the Enhanced Write Filter Manager utility. The write filter provides security and protects flash memory from excessive write activity. See "Enhanced Write Filter Manager" on page 26 for information about the write filter.

✎ Changes made to the thin client configuration will be lost when the thin client is rebooted unless you disable the write filter cache or issue a **-commit** command during the current boot session. See "Enhanced Write Filter Manager" on page 26 for instructions on how to disable the write filter. Enable the write filter when you no longer want permanent changes.

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.

Remote Desktop Connection

The Microsoft Remote Desktop Connection allows an administrator to access a Windows XPe-based thin client (disabled by default) or a Windows Terminal Server from a remote location. With this connection, the administrator can take control of the local thin client and its applications.

The XPe desktop

This section gives a general overview of the 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, except that the Citrix Program Neighborhood, Remote Desktop Connection, and Internet Explorer are the only icons present. These selections are also available from the Start menu. If the terminal emulator application is installed, you can open it from **Start > Programs**.

✎ 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://msdn.microsoft.com/embedded/windowsxpembedded/default.aspx

For the Web addresses of the Citrix Program Neighborhood and Remote Desktop Connection help documents, see “Programs menu extended selections” on page 10.

✎ The Control Panel, available to users 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 the user's desktop background does not open a pop-up menu.

✎ You may copy and paste text between remote session and local computer using standard copy and paste methods.

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
- Remote Desktop Connection
- Internet Explorer

The desktop that displays when you are logged on as Administrator is a standard Windows XP desktop, except that the Citrix Program Neighborhood, Remote Desktop Connection, and Internet Explorer are the only icons present. These selections are also available from the Start menu. If installed, you can open the terminal emulator application from **Start > Programs**. Administrators can access extended resources from the Start menu.

For information about the functionality of the standard Windows XPe desktop and Start menu items, refer to the Microsoft Web site at:

http://msdn.microsoft.com/embedded/windowsxpembedded/default.aspx

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

Logging off from, 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 click **OK.**

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

✎ 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 4.

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 26. 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, allowing the monitor to enter a power-saving mode after a designated idle time. 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.

✎ You should 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.

Programs menu extended selections

Open the Programs menu by clicking **Start > Programs.** Additional selections available on the Programs menu include:

- Citrix Program Neighborhood - also available as a desktop icon
- Remote Desktop Connection - also available as a desktop icon
- TeemNT
- Internet Explorer - also available as a desktop icon

Citrix Program Neighborhood

This selection opens the Citrix Program Neighborhood window, which facilitates connections to remote applications running on ICA servers. Documentation for the ICA client application is available from the Citrix Corporation Web site at:

www.citrix.com/support

Search under Product Documentation.

Remote Desktop Connection

This selection opens the Remote Desktop Connection dialog box. which is used to establish connections to remote applications using RDP. Refer to the Microsoft Web site for documentation that offers a detailed explanation and instructions on how to use the Remote Desktop Connection dialog box.

TeemNT

The TeemNT terminal emulation application is installed on the thin client. Refer to the terminal emulation documentation (supplied separately) for instructions. By default, a desktop icon is not installed.

Internet Explorer

Version 6.0 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.

Control Panel extended selections

The Control Panel is accessed by clicking **Start** on the task bar and selecting **Start > Control Panel.** Some of the extended selections available on the Control Panel are discussed in the following sections.

HP RAMDisk

The RAM disk 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 RAM disk:

- Browser Web page cache
- Browser history
- Browser cookies
- Browser cache
- Temporary Internet files

- Print spooling
- User/system temporary files

You can also use the RAM disk for temporary storage of other data (such as roaming profiles) at the administrator's discretion (see "Local drives" on page 30).

Use the Ramdisk Configuration dialog box to configure the RAM disk size. If you change the size of the RAM disk, 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.

✎ The default RAM disk size may vary depending on the thin client model and the installed memory size. The maximum Ramdisk size that you can is 64 MB. The minimum is 2 MB.

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 open a window that allows access to the following:

- Services
- User Manager

Services

The Services selection lists the services installed on the thin client.

User Manager

User Manager is a utility that allows the administrator to create, delete, and maintain user accounts. For more information, see "User profiles" on page 32.

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 "Firmware upgrades" on page 34.

USB to Serial converter cable

Use this procedure to determine the port assigned to a device connecting to the thin client through a USB to serial converter cable.

1. Connect a printer or other device to the serial port of the converter cable. Do not connect the USB end of the converter cable to the thin client at this time.
2. Open the Device Manager window (**Control Panel > System > Hardware Tab > Device Manager**).
3. A Ports (COM & LPT) listing may or may not display, depending on thin client model and whether a device driver was previously installed to a port. If the listing does display, expand it to display ports currently used.
4. Plug in the USB end of the converter cable to the thin client.
5. The Ports (COM & LPT) listing will display if not already shown. Under the Ports (COM & LPT) listing, a new COM port will display for the new connection. Note which COM port number is assigned to the new connection.
6. Continue the installation procedure for the connected device using the discovered port number when prompted. Use the manufacturer's procedures for other devices, such as a serial touch screen.

✎ You cannot use more than two USB to serial converters at one time.

Printers

A 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 more information, review the following document: http://h200001.www2.hp.com/bc/docs/support/SupportManual/c00298847/c00298847.pdf

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

✎ 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.** T

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.

Microsoft Windows XPe Service Pack 2 (SP2)

Microsoft Windows XPe Service Pack 2 (SP2) addresses new challenges to the security of personal computers by making a number of basic improvements to the operating system.

The HP Compaq Thin Clients Microsoft XPe SP2 image includes improvements to the following features:

- Network Protection
- Microsoft Internet Explorer
- Windows Messenger
- Windows Media Player

Network protection

Network protection is the largest area of improvement in Windows XPe Service Pack 2, and the one with the most implications for existing software.

Sygate firewall

HP's 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. It 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: Frequently Asked Questions" white paper at:

http://h200006.www2.hp.com/bc/docs/support/SupportManual/c00282639/c00282639.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.

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://h18007.www1.hp.com/support/files/ThinClients/us/download/22630.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 does not work with stateful filtering by default.

Configuring Microsoft Windows Firewall

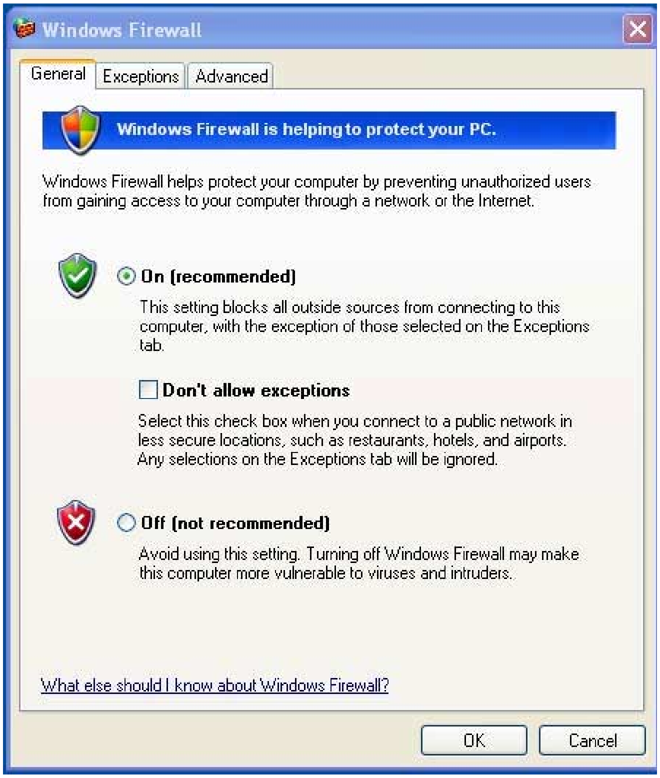
In order to provide the best security and usability, Windows Firewall provides the ability to add exceptions for applications and services so that they can receive inbound traffic.

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 the Windows Firewall add-on is applied, the FIREWALL.CPL control panel applet is only available for the Administrator account.

✎ 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)



Windows Firewall is helping to protect your PC.

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through a network or the Internet.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this check box when you connect to a public network in less secure locations, such as restaurants, hotels, and airports. Any selections on the Exceptions tab will be ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

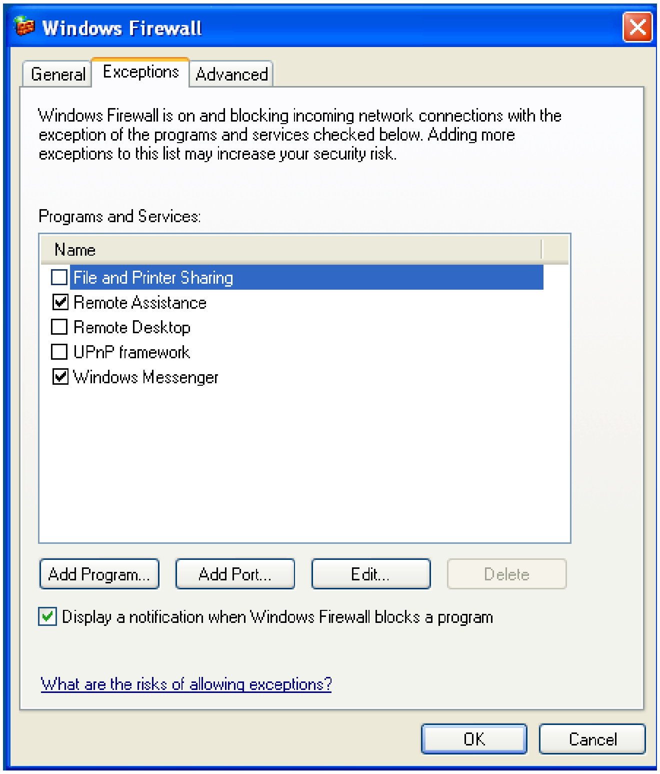
When you select **Don't allow exceptions**, Windows Firewall blocks all requests to connect to your computer, including those from programs or services on the Exceptions tab. The firewall also blocks file and printer sharing and discovery of network devices.

Using Windows Firewall with no exceptions is useful when connecting to a public network, such as one at an airport or hotel. 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



Windows Firewall

Windows Firewall is on and blocking incoming network connections with the exception of the programs and services checked below. Adding more exceptions to this list may increase your security risk.

Programs and Services:

Name

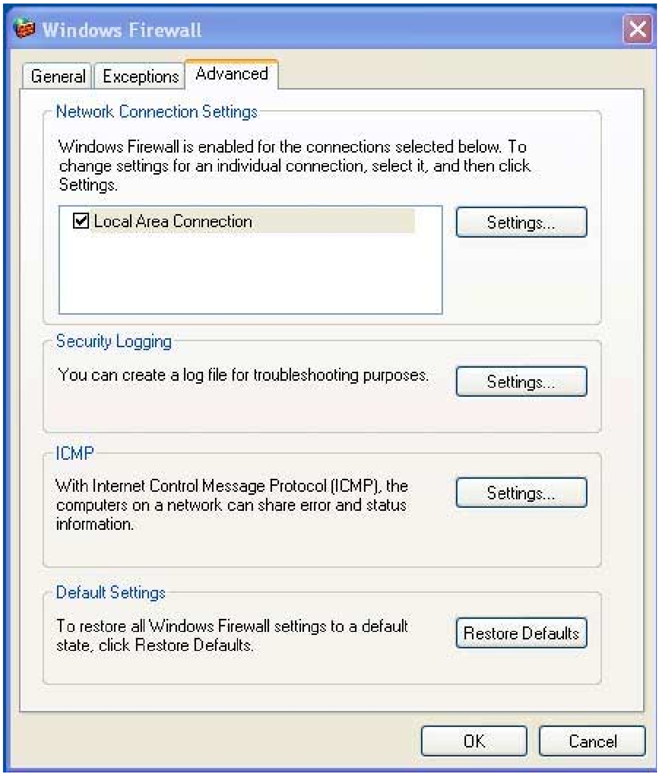
- ☐ File and Printer Sharing
- ☑ Remote Assistance
- ☐ Remote Desktop
- ☐ UPnP framework
- ☑ Windows Messenger

☑ Display a notification when Windows Firewall blocks a program

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.


Windows Firewall

General | Exceptions | Advanced

Network Connection Settings

Windows Firewall is enabled for the connections selected below. To change settings for an individual connection, select it, and then click Settings.

☑ Local Area Connection

Settings...

Security Logging

You can create a log file for troubleshooting purposes.

Settings...

ICMP

With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.

Settings...

Default Settings

To restore all Windows Firewall settings to a default state, click Restore Defaults.

Restore Defaults

OK | Cancel

Gathering configuration information

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

Troubleshooting applications

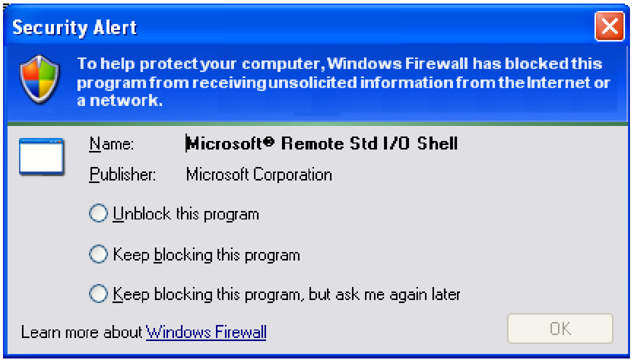
Modifying an application to work with a stateful filtering firewall is the ideal way to resolve issues. This is not always possible, so the firewall provides an interface for configuring exceptions for ports and applications.

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 email applications.
- Server applications running on the Windows XP computer may not respond to client requests. Examples include a Web server such as Internet Information Services (IIS), Remote Desktop, and File Sharing.

✎ 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.



Security Alert

To help protect your computer, Windows Firewall has blocked this program from receiving unsolicited information from the Internet or a network.

Name: Microsoft® Remote Std I/O Shell

Publisher: Microsoft Corporation

○ Unblock this program

○ Keep blocking this program

○ Keep blocking this program, but ask me again later

Learn more about Windows Firewall

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.

✎ 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 click 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. Enter 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.

Additional resources

Refer to the following resources for additional Microsoft Windows Service Pack 2 and Microsoft Windows Firewall information:

- TechNet Windows XP Professional Web site
  http://www.microsoft.com/technet/prodtechnol/winxppro/default.mspx
- Manually Configuring Windows Firewall in Windows XP Service Pack 2
  http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx
- Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2
  http://www.microsoft.com/downloads/details.aspx?FamilyID=cb307a1d-2f97-4e63-a581-bf25685b4c43&displaylang=en
- Deploying Windows Firewall Settings for Microsoft® Windows® XP with Service Pack 2
  http://www.microsoft.com/downloads/details.aspx?familyid=4454e0e1-61fa-447a-bdcd-499f73a637d1&displaylang=en

Microsoft Internet Explorer

Service Pack 2 made Microsoft Internet Explorer much more secure. Internet Explorer has more control over the execution of all content, including a built-in facility to block unwanted pop-up windows and manage the viewing of desired pop-up windows. Furthermore, Internet Explorer now keeps scripts from moving or resizing windows and status bars to hide them from view or obscure other windows.

Windows Messenger

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/?LinkId=25999

Windows Media Player 9

Version 9 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/9series/default.aspx

Utilities and settings

This section describes some of the utilities and settings found on your thin client.

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, you can 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.

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 manipute 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.

△ **CAUTION:** When using the **-commit** command, all the temporary contents are permanently written to the flash memory.

✎ 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, select **Start > Run > Open** and access the system DOS prompt by typing **CMD** in the **Open** field and clicking **OK.**

At the system prompt, enter **ewfmgr c:** and 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 now includes an Enhanced Write Filter (EWF) GUI. You can access the EWF GUI through the Control Panel or the Administrative Tools option for the administrator.

To access the EWF GUI:

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 GUI to Select Write Filter options.

The EWF GUI 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

Windows XPe Image Refresh 5.1.033 includes the EWF status service, which creates an icon in the System Tray that shows the status of EWF. 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

✎ 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://h200005.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.

✎ 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.

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 11. For information about using the Z drive for roaming profiles, see "Roaming profiles" on page 31.

Drive C and Flash

Drive C is in the onboard non-volatile flash memory. 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 memory is reduced to below 3 MB, the thin client becomes unstable.

The Enhanced Write Filter (if enabled) protects the flash from damage and presents an error message if the cache is overwritten. Items that are written to the write filter cache (or directly to the flash, if the write filter is disabled) during normal operation include Favorites, created connections, and deleted or edited connections.

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, you should update configuration settings as described in "User log accounts" on page 32.

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 the **Reconnect at Logon** check box.

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.

✎ 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 log 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 all of your permanent changes have been saved 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 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 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 the **Close** command button.
8. In the Local Users and Groups window, select (highlight) 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.

Remote Administration and firmware 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 specific information on using Altiris, consult the Altiris help documentation.

Add-on modules

If you want to install an add-on module, you must use the Altiris Deployment Solution for administering 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 below 3 MB, the thin client becomes unstable.

✎ 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.

Firmware 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.

✎ 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 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 and 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://h200005.www2.hp.com/bc/docs/support/SupportManual/c00485307/c00485307.pdf

Index

A

adding printers 14
Administrative Tools 12
Administrator
  desktop 8
  logon access 5
Altiris Client Agent 6
Altiris Deployment Solution 3, 34
audio 15

C

Citrix ICA 2
Citrix Program Neighborhood 6, 10
configuring
  Microsoft Windows Firewall 17, 21
Control Panel
  extended selections 11
corrupted Enhanced Writer Filter 29
creating new user account 32

D

desktop
  Administrator 8
  user 7
drive C 30
drive Z 30

E

Enhanced Write Filter Manager 6, 26
  clear boot command 29
  command line control 27
  disabling 28
  enabling 28
  overlay configuration 29
  status tool 29
  user interface 28
Enhanced Writer Filter manager 9
extended selections
  Control Panel 11

F

firewall
  Microsoft Windows 17
  Sygate 16
Flash 30

H

HP Compaq Thin Client Imaging Tool 35
HP RAMDisk 11
HP Sygate Security Agent 16

I

image updates 1
Internet Explorer 11, 25

L

language options 12
logging on
  Administrator 5
  automatic 4
  manual 4

M

Macromedia Flash Player 6
manufacturer print drivers 15

mapping network drives 31
Microsoft Internet Explorer 25
Microsoft RDP 2
Microsoft Remote Desktop Connection 7, 11
Microsoft Terminal Services 2
Microsoft Windows Firewall 17
    adding a port 23
    adding a program 23
    additional information 24
    configuring 17
    failure symptoms 22
    issue resolution 22
    on-by-default 17
    troubleshooting 21
Microsoft Windows Service Pack 2 16
    additional information 24

N
network drives 31
network protection 16

O
on-by-default 17

P
password rules 5
peripherals 13
power management 10
pre-installed utilities 5
print driver
    manufacturer 15
    text-only 14
printers 14

R
regional and language options 12
roaming profiles 31

S
saving files 31
services 12
session services 1
shutting down 9
support service 3
Sygate Firewall 16
Sygate Security Agent 16
system time 10

T
TeemNT 11
Telnet protocol 2
terminal emulation support 2
Terminal Services Client Access Licenses 2
text-only printer driver 14
time 10
troubleshooting Microsoft Windows Firewall 21
TSCAL 2

U
USB to serial converter cable 13
user
    creating new account 32
    desktop 7
    profiles 32
User Manager 12
user profiles 32
utilities and settings 25

W
Windows Media Player 9 25
Windows Messenger 25
Windows XPe
    extended features 3