
# Locking Down Windows Server 2003 Terminal Server Sessions

Microsoft Corporation

Published: July, 2003

**Abstract**

This article demonstrates the ability of Active Directory® to restrict Microsoft® Windows Server™ 2003 Terminal Server sessions to the functionality allowed by an administrator. Highlighting important group policies, considerations are outlined for configuring user interactions with the operating system for a wide variety of deployments.

# Contents

# Introduction

Using Terminal Server in Windows Server 2003, you can operate 32-bit applications, such as Microsoft Word and Microsoft Excel, anytime and anywhere. Terminal Server provides centralized application processing, management, and maintenance. With this flexibility, Terminal Server can be used in a wide variety of applications and environments.

A terminal can reside in an office, kiosk, classroom, laboratory, on a factory floor, or across the internet in another country while the server is in a secure server room. For example; Terminal Server can be used by Application Service Providers to provide access for multiple applications to customers over the Internet. In certain deployments, it might be necessary to restrict user activity to a predefined set of applications or Windows operating system functionality.

## How can this be implemented?

This white paper is intended for administrators who are already familiar with Terminal Server and the Active Directory. It explains how you can use the features of Active Directory to restrict user sessions on the Terminal Server to only the applications and desktop functionality that the administrator deems necessary. Certain group policies are highlighted here with brief explanations of their benefits. Not all of the settings are necessary because they can create a highly restricted user interface. Use this paper as a guide to configure Terminal Server for your environment. For a detailed explanation of each policy mentioned, see the **Explain** tab in the Group Policy Object Editor.

If Active Directory is not available, administrators can use NTFS permissions or the local policy editor to restrict application access. Although many policies can be applied without Active Directory by means of the local policy editor, that method is not recommended. Enabling these policies in the local policy editor restricts all accounts on the Terminal Server, including the administrator account. Using the local policy editor can also be cumbersome and is outside the scope of this paper. Using Active Directory to restrict functionality is the recommended means to restrict Terminal Server sessions in Windows Server 2003.

**Note**

This article does not address methods to secure the Terminal Server against malicious attacks. It does not provide a guarantee against hackers, creative users, applications, or drivers that circumvent the restrictions mentioned in this paper. For more information about securing Terminal Services in Microsoft® Windows® 2000, see Securing Windows 2000 Terminal Services at: http://go.microsoft.com/fwlink/?LinkId=18404.

## Planning

The policies highlighted in the article are basic restrictions for the user interface for the operating system. Not all of the policies are required, and some might not be appropriate in certain environments. Test your implementation before deployment. In addition to determining which restrictions are suitable for your environment, decide how these policies will be implemented.

The policies mentioned in this article can severely restrict functionality for even the administrator account. It is highly recommended that a new organizational unit (OU) and Group Policy object (GPO) be created.

If system-wide restrictions must be applied to the Terminal Server, place the Terminal Server computer object into the locked down OU. Doing so enforces computer-based restrictions on the Terminal Server. Administrators have the option to apply user-based restrictions to all users, including administrators who log on to the Terminal Server. These restrictions can be in addition to, or in place of policies the user typically has when logging on to the domain. Refer to the computer loopback policy for additional information.

If per-user restrictions need to be applied, place the user account object into the locked down OU. Doing so, however, enforces user-based restrictions for that user account regardless of which computer the user uses to log on to the domain.

Here are two recommendations for implementation of group policies:

1. User accounts are placed into the locked down OU.

   Create Terminal-Server-only user accounts and place them in the locked down OU. Allow user logons to the Terminal Server for only these users by using the Terminal Server Configuration MMC snap-in. Instruct the users to only use these accounts on the Terminal Server. If some computer restrictions are necessary, disable loopback processing and place the Terminal Server computer object into the OU. Aside from the restrictive computer policies, users can have different levels of restrictions on the same Terminal Server. This implementation allows Administrators to perform some operations on the Terminal Server while users are active.

2. Only the Terminal Server computer object is placed into the locked down OU.

   After installing and configuring all applications on the Terminal Server, place the Terminal Server computer object into the locked down OU. Enable loopback processing. All users who log on to the Terminal Server are then restricted by user-based policies as defined by the locked down GPO, regardless of the OU the user is located in. This can prevent many local changes from being applied to the Terminal Server; however, the server can still be remotely maintained. If administrators need access to the Terminal Server, log off all users and temporarily restrict their logons to the Terminal Server. Move the Terminal Server computer object out of the locked down OU, then log on. Return the Terminal Server computer object to the locked down OU, and re-enable user logins after maintenance is complete. This implementation does not require users to have multiple user accounts. It can also prevent configuration changes to the Terminal Server while it is in production.

For more information on configuring security settings, see "To edit a security setting on a Group Policy object" at: http://go.microsoft.com/fwlink/?linkid=18541.

## Installing Terminal Server

When installing Terminal Server on a Windows Server 2003 computer, you are asked to select a permissions compatibility setting for either Full Security or Relaxed Security. This setting can be changed later by using the Terminal Server Configuration MMC snap-in.

It is recommended that you select the Full Security option. Doing so restricts permissions for Terminal Server users to the - Users group. The Full Security setting, however, might have compatibility issues with some legacy applications. If this is the case, select the Relaxed Security setting. The Relaxed Security setting provides Terminal Server users with nearly Power User level access to certain system folders and registry keys. If the Relaxed Security setting is selected, consider enabling policies to restrict access to registry editors and file browsers.

## Restrictive Computer Policies

These policies are only applied to computer objects that are placed into the locked down OU. These settings are system wide, affecting all users.

**[Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options]**

- Devices: Restrict CD-ROM access to locally logged-on user only

  Recommended setting: **Enabled**

  This policy allows only users who log on to the console of the Terminal Server access to the CD-ROM drive. It is recommended that you enable this policy to prevent users and administrators from remotely accessing programs or data on a CD-ROM.

- Devices: Restrict floppy access to locally logged-on user only

  Recommended setting: **Enabled**

  This policy allows only users who log on to the console of the Terminal Server access to the floppy disk drive. It is recommended that you to enable this policy to prevent users and administrators from remotely accessing programs or data on a floppy disk.

- Interactive logon: Do not display last user name

  This policy does not display the last logged on user account at the Windows logon prompt on the console of the Terminal Server. This policy does not affect Terminal Server clients that locally cache the logon user name.

**[Computer Configuration\Windows Settings\Security Settings\System Services]**

- Help and Support

  Recommended setting: **Disabled**

  This policy disables Help and Support Center service. It prevents users from starting the new Windows Help and Support Center application. This policy does not disable the old help files (such as the *.chm) or Help in other applications. Disabling this service might cause issues with other programs and services that depend on this service. It is recommended that you disable this service to prevent users from starting other applications or viewing system information about the Terminal Server.

**[Computer Configuration\Administrative Templates\Windows Components\Terminal Services]**

- Restrict Terminal Services users to a single remote session

  This policy can prevent a single user from creating multiple sessions on the Terminal Server using a single user account.

- Remove Disconnect option from Shut Down dialog box

This policy removes the disconnect option from the **Shut Down Windows** dialog box. It does not prevent users from disconnecting session to the Terminal Server. Use this policy if you do not want users to easily disconnect from their session and you have not removed the **Shut Down Windows** dialog box.

**[Computer Configuration\Administrative Templates\Windows Components\Terminal Services \Client/Server data redirection]**

- Do not allow drive redirection

  Recommended setting: **Enabled**

  By default, Terminal Server maps client drives automatically upon connection. It is recommended that you enable this policy to prevent users from having easy access to applications on their local computer.

**[Computer Configuration\Administrative Templates\Windows Components\Terminal Services \Sessions]**

- Set time limit for disconnected sessions

  By default, Terminal Server allows users to disconnect from a session and keep all of their applications active for an unlimited amount of time. This policy specifies a time limit for disconnected Terminal Server sessions to remain active. Use this policy if you do not want disconnected sessions to remain active for a long time on the Terminal Server.

**[Computer Configuration\Administrative Templates\Windows Components\Windows Installer]**

- Disable Microsoft® Windows® Installer

  Recommended setting: **Enabled** - Always

  If this is set for non-managed applications only, the Windows Installer still functions for applications that are published or assigned by means of group policies. If this is set to **Always**, Windows Installer is completely disabled. This may be beneficial if some published or assigned applications are not wanted on Terminal Server. Disabling Windows Installer does not prevent installation of applications by means of other setup programs or methods. It is recommended that applications be installed and configured prior to enabling this policy. After the policy is enabled, administrators cannot install applications that use Windows Installer.

**[Computer Configuration\Administrative Templates\System\Group Policy]**

- User Group Policy loopback processing mode

If the Terminal Server computer object is placed in the locked down OU, and the user account is not, loopback processing applies the restrictive user configuration policies to all users on the Terminal Server. If this policy is enabled, all users, including administrators, logging on to the Terminal Server are affected by the restrictive user configuration policies, regardless of where the user account is located. Two modes are available. Merge mode first applies to the user's own GPO, then to the locked down policy. The lockdown policy takes precedence over the user's GPO. Replace mode just uses the

locked down policy and not the user's own GPO. This policy is intended for restrictions based on computers instead of the user account.

> If this policy is disabled, and the Terminal Server computer object is placed in the locked down OU, only the computer configuration policies is applied to the Terminal Server. Each user account must be placed into the OU to have user configuration restriction placed on that user.

## Restrictive User Policies

These policies are applied to user accounts that are in the locked down OU. If loopback processing is used, all user accounts that log on to computers that are in the locked down OU also have these restriction applied.

**[User Configuration\Windows Settings\Folder Redirection]**

- Application Data

  Recommended setting: Basic redirection and create a folder for each user under the root path. On the **Settings** tab, enable grant the user exclusive rights. Enable move contents of folder to new location. Set the policy removal to redirect the folder back to the local user profile location when policy is removed.

- Desktop

  Recommended setting: Basic redirection and create a folder for each user under the root path. On the **Settings** tab, enable grant the user exclusive rights. Enable move contents of folder to new location. Set the policy removal to redirect the folder back to the local user profile location when policy is removed.

- My Documents

  Recommended setting: Basic redirection and create a folder for each user under the root path. On the **Settings** tab, enable grant the user exclusive rights. Enable move contents of folder to new location. Set the policy removal to redirect the folder back to the local user profile location when policy is removed.

- Start Menu

  Recommended setting: Basic redirection and redirect to the following location. On the **Settings** tab, set the policy removal to redirect the folder back to the local user profile location when the policy is removed. Create a \Programs\Startup folder under this shared folder.

  Enabling these policies can provide a central point for backing up user data. Additionally, if the policy to restrict access to local drives is enabled (below), the users need folder redirection if they do not want to see messages saying that they have restricted access.

  If a roaming profile server is not available, local shares can be used. Create a master folder for all of the user data (such as C:\userdata). Create four sub folders, one for each folder type (such as AppData, Desktop, MyDocs, and Start). Share each of the sub folders and set the share permissions for the “everyone” group to “change”. Set each path to its corresponding share.

  The Start Menu can be configured differently. It can be shared across all users. Place links to applications in here. Change the share permissions for the “everyone” group to “read”. You should manually create the “Programs\Startup” folder under the shared Startup folder (C:\userdata\Start\Programs\Startup).

**[User Configuration\Administrative Templates\Windows Components\Internet Explorer]**

- Search: Disable Find Files via F3 within the browser

  Recommended setting: **Enabled**

  This policy disables the use of the F3 key to search in Microsoft® Internet Explorer and Windows Explorer. Users cannot press F3 to search the Internet (from Internet Explorer) or to search the hard disk (from Windows Explorer). If the user presses F3, a prompt appears that informs the user that this feature has been disabled. This policy can prevent a user form easily searching for applications on the hard disk. It is recommended that you enable this policy to prevent users from searching for applications on hard drive or browsing the Internet.

**[User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser menus]**

- Disable **Context** menu

  Recommended setting: **Enabled**

  This policy prevents the shortcut menu from appearing when users click the right mouse button while using the browser. It is recommended that you enable this policy to prevent users from using the shortcut menu as an alternate method of running commands.

- Hide **Favorites** menu

  This policy prevents users from adding, removing, or editing the list of Favorite links. If you enable this policy, the **Favorites** menu is removed from the interface and the **Favorites** button on the browser toolbar appears dimmed. Use this policy if you want to remove the **Favorites** menu from Windows Explorer and do not want to give users easy access to Internet Explorer.

**[User Configuration\Administrative Templates\Windows Components\Application Compatibility]**

- Prevent access to 16-bit applications

  Recommended setting: **Enabled**

  This policy prevents the MS-DOS subsystem (ntvdm.exe) from running for the user. This setting affects the starting of all 16-bit applications in the operating system. By default, the MS-DOS subsystem runs for all users. Many MS-DOS applications are not Terminal Server friendly and can cause high CPU utilization due to constant polling of the keyboard. It is recommended that you enable this policy to prevent the 16-bit command interpreter, Command.com, from executing.

---

**Note**

The “Prevent access to 16-bit applications” policy can be configured in both Computer Configuration (system-wide) and User Configuration (user specific).

---

**[User Configuration\Administrative Templates\Windows Components\Windows Explorer]**

- Removes the **Folder Options** menu item from the Tools menu

  Recommended setting: **Enabled**

  Removes the Folder Options item from all Windows Explorer menus and removes the Folder Options item from Control Panel. As a result, users cannot use the **Folder Options** dialog box. It is recommended that you enable this policy to prevent users from configuring many properties of Windows Explorer, such as Active Desktop, Web view, Offline Files, hidden system files, and file types.

- Remove File menu from Windows Explorer

  Recommended setting: **Enabled**

  This policy removes the **File** menu from My Computer and Windows Explorer. It does not prevent users from using other methods to perform tasks available on the File menu. It is recommended that you enable this policy to remove easy access to tasks such as "New," "Open With," and shell extensions for some applications. Enabling this policy also prevents easy creation of shortcuts to executables.

- Remove Map Network Drive and Disconnect Network Drive

  Recommended setting: **Enabled**

  This policy prevents users from connecting and disconnect to shares with Windows Explorer. It does not prevent mapping and disconnecting drives from other applications or the run command. It is recommended that you enable this policy to remove easy access to browsing the domain from Windows Explorer. If mapped drives are necessary, they can be mapped from a logon script.

- Remove Search button from Windows Explorer

  Recommended setting: **Enabled**

  It is recommended that you enable this policy to prevent users from searching for applications from Windows Explorer. This policy does not prevent search routines in other applications or the Start Menu.

- Remove Security Tab

  Recommended setting: **Enabled**

  This policy removes the **Security** tab from Windows Explorer. If users can open the **Properties** dialog box for file system objects, including folders, files, shortcuts, and drives, they cannot access the **Security** tab. It is recommended that you enable this policy to prevent users from changing the security settings or viewing a list of all users who have access to the object.

- Remove Windows Explorer's default context menu

  Recommended setting: **Enabled**

  This setting removes the shortcut menu from Windows Explorer. It is recommended that you enable this policy to prevent easy access to applications that place hooks into the shortcut

menu. This policy does not remove other methods of accessing applications on the shortcut menu, such as using shortcut hotkeys.

- Hides the Manage item on the Windows Explorer shortcut menu

  Recommended setting: **Enabled**

  This policy removes the **Manage** option from Windows Explorer or My Computer. The **Manage** option opens the Computer Management MMC snap-in (compmgmt.msc). Items like Event Viewer, System Information, and Disk Administrator can be accessed from Computer Management. This policy does not restrict access to these tasks from other methods such as Control Panel and the run command. It is recommended that you enable this policy to remove easy access to system information about the Terminal Server.

- Hide these specified drives in My Computer

  Recommended setting: **Enabled** – Restrict A, B, C, and D drives only

  This policy only removes the icons from My Computer, Windows Explorer, and the standard file dialog box. It does not prevent users from access these drives by using other means such as the command prompt. The policy only allows you to hide drives A through D. It is recommended that you enable this policy to hide the floppy disk drive, the CD-ROM drive, and the operating system partition. A partition for public data can be configured to be the only drive viewable to the users. If required, NTFS permissions can be used to restrict access to this partition.

- Prevent access to drives from My Computer

  Recommended setting: **Enabled** – A, B, C, and D drives only

  This policy prevents access to drives A through D with My Computer, Windows Explorer and the standard file dialog box. This policy does not prevent access from programs that do not use the common dialog boxes. The users can still start applications that reside on the restricted drives. It is recommended that you enable this policy to restrict file browsing of system partitions.

- Remove Hardware tab

  Recommended setting: **Enabled**

  This policy removes the **Hardware** tab from Mouse, Keyboard, and Sounds and Audio Devices in Control Panel. It also removes the **Hardware** tab from the **Properties** dialog box for all local drives, including hard drives, floppy disk drives, and CD-ROM drives. It is recommended that you enable this policy to prevent users from using the **Hardware** tab to view the device list or device properties.

- Remove Order Prints from Picture Tasks

  Recommended setting: **Enabled**

  It is recommended that you enable this policy to remove the "Order Prints Online from Picture Tasks" link in the My Pictures folder.

- Remove Publish to Web from File and Folders Tasks

  Recommended setting: **Enabled**

This policy setting removes **Publish this file to the Web**, **Publish this folder to the Web**, and **Publish the selected items to the Web from File and Folder** tasks in Window Explorer. It is recommended that you enable this policy to prevent users from publishing files or folders to a Web page.

- No “Computers Near Me” in My Network Places

  Recommended setting: **Enabled**

  This policy removes computers in the user's domain from lists of network resources in Windows Explorer and My Network Places. It does not prevent users from connecting to other computers by other methods, such as the command prompt or the **Map Network Drive** dialog box. It is recommended that you enable this policy to remove easy access to browsing the domain.

- No “Entire Network” in My Network Places

  Recommended setting: **Enabled**

  This policy removes all computers outside of the user's local domain from lists of network resources in Windows Explorer and My Network Places. It does not prevent users from connecting to other computers by other methods, such as command prompt or the **Map Network Drive** dialog box. It is recommended that you enable this policy to remove easy access to browsing the network.

- Turn off Windows+X hotkeys

  Recommended setting: **Enabled**

  This policy turns off Windows+X hotkeys. Keyboards with a Windows logo key provide users with shortcuts to common shell features. For example, pressing the keyboard sequence Windows+R opens the **Run** dialog box; pressing the Windows+E starts Windows Explorer. It is recommended that you enable this policy to prevent users from starting applications with the Windows logo hotkey.

- Turn on Classic Shell

  Recommended setting: **Enabled**

  This policy allows you to remove the Active Desktop and Web view features. If you enable this setting, it disables the Active Desktop and Web view. Also, users cannot configure their system to open items by single-clicking (such as in Mouse in Control Panel). As a result, the user interface looks and operates like the interface for Windows NT 4.0, and users cannot restore the new features. It is recommended that you enable this policy to remove Folder Tasks. Some Folder Task, such as for the My Music folder can start Internet Explorer.

**[User Configuration\Administrative Templates\Windows Components\Windows Explorer \Common Open File Dialog]**

- Hide the common dialog places bar

  Recommended setting: **Enabled**

  This policy removes the shortcut bar from the **Common Open File** dialog box. This feature was originally added in Windows 2000, so disabling it makes it look as it did in Windows NT 4.0 and

earlier. These policies affect only programs that use the common dialog box. It is recommended that you enable this policy to remove easy access to browsing the network or the local computer.

- Items displayed in Places Bar

  This policy allows you to replace the Place Bar items in the **Common Open File** dialog box with predefined entries. To view this bar, start Notepad, select File, and then click Open.

**[User Configuration\Administrative Templates\Windows Components\Task Scheduler]**

- Hide Property Pages

  Recommended setting: **Enabled**

  It is recommended that you enable this policy to prevent users from viewing and changing the properties of an existing task.

- Prohibit Task Deletion

  This policy prevents administrators from deleting tasks from the Scheduled Tasks folder. This does not prevent administrators from deleting tasks with the AT command, or from a remote computer.

- Prevent Task Run or End

  This policy prevents administrators from starting and stopping tasks.

- Prohibit New Task Creation

  Recommended setting: **Enabled**

  It is recommended that you enable this policy to prevent users from creating new scheduled tasks and browsing for applications. This does not prevent administrators from creating new tasks with the AT command, or from a remote computer.

**[User Configuration\Administrative Templates\Windows Components\Windows Messenger]**

- Do not allow Windows Messenger to be run

  Recommended setting: **Enabled**

  This policy disables Windows Messenger for the user. It is recommended that you enable this policy to prevent users from receiving links or files from other Windows Messenger users.

**[User Configuration\Administrative Templates\Windows Components\Windows Update]**

- Remove access to use all Windows Update features

  This policy removes access to Windows Update. If you enable this setting, all Windows Update features are removed. This includes blocking access to the Microsoft Windows Update Web site at http://go.microsoft.com/fwlink/?LinkId=18539, from the Windows Update hyperlink on the **Start** menu, and also on the **Tools** menu in Internet Explorer. Windows automatic updating is

also disabled; you are neither notified about critical updates nor do you receive critical updates from Windows Update. This setting also prevents Device Manager from automatically installing driver updates from the Windows Update Web site. This policy can be used to prevent changes to the Terminal Server while it is production. If you disable Windows Update, you should schedule periodic checks to ensure Windows has latest critical updates.

**[User Configuration\Administrative Templates\Start Menu & Taskbar]**

- Remove links and access to Windows Update

  Recommended setting: **Enabled**

  This policy removes links and access to the Windows Update Web site. The Windows Update Web site is only available for administrators. It is recommended that you enable this policy to remove easy access to Internet Explorer for users.

- Remove common program groups from Start Menu

  Recommended setting: **Enabled**

  This policy removes shortcuts to programs from the all users' profile. Only the Start Menu in the user's profile or the redirected Start Menu is available. It is recommended that you enable this policy to remove easy access to built-in applications like games, calculator, and media player.

- Remove pinned programs list from Start Menu

  This policy removes the Pinned Programs list from the new Start Menu. It also removes the default links to Internet Explorer and Outlook Express if they are pinned, and it prevents users from pinning any new programs to the Start Menu. The Frequently Used Programs list is not affected.

- Remove programs on Settings menu

  Recommended setting: **Enabled**

  This policy removes Control Panel, Printers, and Network Connections from **Settings** on the **Classic Start** menu, My Computer and Windows Explorer. It also prevents the programs represented by these folders (such as Control.exe) from running. However, users can still start Control Panel items by using other methods, such as right-clicking the desktop to open Display Properties or right-clicking My Computer to open System Properties. It is recommended that you enable this policy to prevent easy access to viewing or changing system settings.

- Remove Network Connections from Start Menu

  Recommended setting: **Enabled**

  This policy prevents the Network Connections folder from opening. The policy also removes Network Connections from Settings on Start Menu. Network Connections still appears in Control Panel and in Windows Explorer, but if users try to start it, a message appears explaining that a setting prevents the action. It is recommended that you enable this policy to prevent users from creating new connections such as VPN or Dial-up.

- Remove the Search menu from Start Menu

  Recommended setting: **Enabled**

  This policy removes the search function from the **Start** menu. This setting removes **Search** from the **Start** menu and from the shortcut menu that appears when you right-click Start Menu. Also, the system does not respond when users press Windows+F or the F3 key. In Windows Explorer, the search item still appears on the Standard buttons toolbar, but the system does not respond when the user presses CTRL+F. Also, Search does not appear in the shortcut menu when you right-click an icon representing a drive or a folder. This setting affects the specified user interface elements only. It does not affect Internet Explorer and does not prevent the user from using other methods to search. It is recommended that you enable this policy to prevent users from easily searching for applications that they are not assigned to them.

- Remove Drag-and-Drop shortcut menus on Start Menu

  Recommended setting: **Enabled**

  This policy prevents users from using the drag-and-drop method to reorder or remove items on the **Start** menu. This setting does not prevent users from using other methods of customizing the **Start** menu or performing the tasks available from the shortcut menus. It is recommended that you enable this policy to remove shortcut menus from the **Start** menu, including tasks such as creating a new shortcut.

- Remove Favorites menu from Start Menu

  This policy prevents users from adding the **Favorites** menu to the **Start** menu or the **Classic Start** menu. Use this policy if you do not want users to execute Internet Explorer.

---

**Note**

The **Favorites** menu does not appear on the **Start** menu by default, but this policy disables the Favorites link. This setting only affects the **Start** menu. The **Favorites** menu still exists in Windows Explorer and Internet Explorer.

---

- Remove Help menu from Start Menu

  Recommended setting: **Enabled**

  This policy removes the Help link from the **Start** menu. This setting only affects the **Start** menu. To disable the new Help and Support application disable the service in Computer Configuration (See Restricted Computer Policies). It is recommended that you enable this policy to prevent users from easily viewing System Information about the Terminal Server.

- Remove Run menu from Start Menu

  Recommended setting: **Enabled**

  It is highly recommended that you enable this policy to prevent users from attempting to execute any application. This is very critical for locking down the Terminal Server. Enabling this removes the **Run** command from the **Start** menu, New Task from Task Manager, and users are blocked from entering a UNC path, local drive, and local folders into the Internet Explorer address bar. Also, users with extended keyboards can no longer display the **Run** dialog box by pressing Windows+R.

---

**Note**

The "Remove Run menu from Start Menu" setting affects the specified interface only. It does not prevent users from using other methods to run programs.

---

- Remove My Network Place icon from Start Menu

  Recommended setting: **Enabled**

  This policy removes the My Network Places icon from the **Start** menu. It is recommended that you enable this policy to prevent easy access to browsing the network.

- Add Logoff to Start Menu

  Recommended setting: **Enabled**

  It is recommended that you enable this policy to make it easy for users to log off of their Terminal Server sessions. This policy adds the "Log Off <user name>" item to the **Start** menu and prevents users from removing it. This setting affects the **Start** menu only. It does not affect the Log Off item on the **Windows Security** dialog box that appears when you press CTRL+ALT+DEL or CTRL+ALT+END from a Terminal Server client.

- Remove and prevent access to Shut Down command

  Recommended setting: **Enabled**

  This policy removes the ability for the user to open the **Shutdown** dialog box from the **Start** menu and from the **Windows Security** dialog box (CTRL+ALT+DEL). This policy does not prevent users from running programs to shut down Windows. It is recommended that you enable this policy help remove confusion from the users and prevent administrators from shutting down the system while it is in production.

- Prevent changes to Taskbar and Start Menu settings

  Recommended setting: **Enabled**

  This policy prevents customization of the taskbar and the **Start** menu. It can simplify the desktop by adhering to the configuration set by the administrator. It is recommended that you enable this policy to restrict the ability to add other applications to the start menu by browsing or typing the location of an application.

- Remove access to the shortcut menus for the taskbar

  Recommended setting: **Enabled**

  This policy removes the right-click menu on the taskbar. This setting does not prevent users from using other methods to issue the commands that appear on this menu. It is recommended that you enable this policy to prevent potential access to files and applications by starting Windows Explorer or Search.

- Force Classic Start Menu

  This policy effects the presentation of the **Start** menu. The **Classic Start** menu in Windows 2000 allows users to begin common tasks, while the new **Start** menu consolidates common items onto one menu. When the **Classic Start** menu is used, the following icons are placed on the desktop: My Documents, My Pictures, My Music, My Computer, and My Network Places. The new **Start** menu starts them directly. Disabling the new **Start** menu removes Printers and Faxes. From Printers and Faxes, users can view Server Properties to see where the Spool folder is installed.

**[User Configuration\Administrative Templates\Desktop]**

- Remove Properties from My Documents shortcut menu

  Recommended setting: **Enabled**

  This setting hides Properties for the shortcut menu on My Documents. It is recommended that you enable this policy if shortcut menus are not disabled and you do not want the users to easily view or edit the location of their My Document folder.

- Remove Properties from My Computer shortcut menu

  Recommended setting: **Enabled**

  This setting hides Properties on the shortcut menu for My Computer. It is recommended that you enable this policy if shortcut menus are not disabled and you do not want the users to easily view configuration information about the Terminal Server.

- Remove Properties from Recycle Bin shortcut menu

  Recommended setting: **Enabled**

  This policy removes the Properties option from the Recycle Bin shortcut menu. It is recommended that you enable this policy if shortcut menus are not disabled and you do not want the users to easily view or change Recycle Bin settings.

- Hide My Network Places icon on desktop

  Recommended setting: **Enabled**

  It is recommended that you enable this policy to remove easy access to browsing the network for applications. This setting only affects the desktop icon. It does not prevent users from connecting to the network or browsing for shared computers on the network with other methods.

- Hide Internet Explorer Icon on the desktop

  This policy removes the Internet Explorer icon from the desktop. This setting does not prevent the user from starting Internet Explorer by using other methods.

- Prohibit user from changing My Documents path

  Recommended setting: **Enabled**

  This policy restricts the My Documents location to the designated location. It is recommended that you enable this policy to prevent browsing for applications.

- Hide and disable all items on the desktop

  This policy removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, My Computer, and My Network Places. Removing icons and shortcuts does not prevent the user from using another method to start the programs or opening the items they represent. User can still save and open items on the desktop by using the **Common File** dialog box or Windows Explorer. The items; however, are not displayed on the desktop.

- Remove My Documents icon on the desktop

  This policy removes most occurrences of the My Documents icon. It does not prevent the user from using other methods to gain access to the contents of the My Documents folder.

- Remove My Computer icon on the desktop

  Recommended setting: **Enabled**

  This policy hides My Computer from the desktop and from the new **Start** menu. It also hides links to My Computer in the Web view of all Explorer windows, and it hides My Computer in the Explorer folder tree pane. If the user navigates into My Computer by using the **Up** icon while this setting is enabled, they view an empty My Computer folder. It is recommended that you enable this policy to present users with a simpler desktop environment and remove easy access to Computer Management and System Properties by no longer allowing right-clicking of the icon.

---

**Note**

Hiding My Computer and its contents does not hide the contents of the child folders of My Computer. For example, if the users navigate into one of their hard drives, they see all of their folders and files there even if this setting is enabled.

---

**[User Configuration\Administrative Templates\Control Panel]**

- Prohibit access to the Control Panel

  Recommended setting: **Enabled**

  This policy removes access to Control Panel and disables all Control Panel programs. It also prevents Control.exe, the program file for Control Panel, from starting. It is recommended that you enable this setting to prevent users from viewing configuration information about the Terminal Server.

**[User Configuration\Administrative Templates\Control Panel\Add or Remove Programs]**

- Remove Add or Remove Programs

  Recommended setting: **Enabled**

  This policy removes Add or Remove Programs from Control Panel and removes the Add or Remove Programs item from menus. If access to Control Panel is prohibited, this policy can be used to remove the links to Add or Remove Programs from places like My Computer. The link then displays an access denied message if clicked. This setting does not prevent users from using other tools and methods to install or uninstall programs. It is recommended that you enable this policy to prevent users to viewing Terminal Server configuration information.

**[User Configuration\Administrative Templates\Control Panel\Printers]**

- Prevent addition of printers

  Recommended setting: **Enabled**

  This policy prevents users from using familiar methods to add local and network printers. It is recommended that you enable this policy to prevent users from browsing the network or searching the active directory for printers. This policy does not prevent the auto-creation of Terminal Server redirected printers, nor does it prevent users from running other programs to add printers.

**[User Configuration\Administrative Templates\System]**

- Prevent access to the command prompt

  Recommended setting: **Enabled** – Set “Disable the command prompt script processing also” to **No**.

  This policy prevents users from running the interactive command prompt Cmd.exe. From the command prompt users can start applications. This setting also determines whether batch files (.cmd and .bat) can run on the computer.

---

**Note**

Do not prevent the computer from running batch files on a Terminal Server. This policy does not prevent access to Command.com (16-bit command interpreter). To disable the Command.com, you can restrict access with NTFS permission, or disable all 16-bit applications with the “Prevent access to 16-bit application” policy.

---

  It is recommended that you enable the “Prevent access to the command prompt” policy to prevent users from bypassing other policies by using the command prompt instead of Windows Explorer as the shell.

- Prevent access to registry editing tools

  Recommended setting: **Enabled**

  This policy restricts users from changing registry settings by disabling Regedit.exe. It is recommended that you enable this policy to prevent users from changing their shell to the command prompt or bypassing several other policies. This policy does not prevent other applications for editing the registry.

- Run only allowed Windows applications

  Recommended setting: **Enabled** – Define list of authorized applications

  It is recommended that you enable this policy to restrict users to only run programs that are added to the List of Allowed Applications. This setting only prevents users from running programs that are started by Windows Explorer. It does not prevent users from running programs such as Task Manager, which can be started by a system process. Also, if users have access to the command prompt, Cmd.exe, this setting does not prevent them from starting programs from the command window that they are not permitted to start by using Windows Explorer.

**[User Configuration\Administrative Templates\System\CTRL+ALT+DEL Options]**

- Remove Task Manager

  Recommended setting: **Enabled**

  This policy prevents users from starting Task Manager. It is recommended that you enable this policy to prevent users from using task manager to start and stop programs; monitor the performance of the Terminal Server; and find the executable names for applications.

- Remove Lock Computer

  This policy prevents users from locking their sessions. Users can still disconnect and log off. While locked, the desktop can not be used. Only the user who locked the system or the system administrator can unlock it.

**[User Configuration\Administrative Templates\System\Scripts]**

- Run legacy logon scripts hidden

  Recommended setting: **Enabled**

  This policy hides the instructions in logon scripts written for Windows NT 4.0 and earlier. It is recommended that you enable this policy to prevent users from viewing or interrupting logon scripts written for Windows NT 4.0 and earlier.

# Non-Policy Settings

## Disable Internet Explorer Search Companion

Users can access the Internet Explorer Search Companion by clicking **Search** on the toolbar, or pressing CTRL-E in Internet Explorer. With the Internet Explorer Search Companion, users can browse or search for files and folders. There is no policy to disable the Internet Explorer Search Companion. This operation needs to be preformed manually.

1. Create a text file on the local partition, (c:\windows\nosearch.txt)
2. The content of the text file can be "Search is disabled."
3. Set the NTFS permissions of the file to “Everyone – Read and Execute”.
4. Then modify the following registry values:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search

   “SearchAssistant” = REG_SZ: c:\windows\nosearch.txt

   “CustomizeSearch” = REG_SZ: c:\windows\nosearch.txt

When the users open the Search Companion, the contents of the text file are displayed. It is possible to use a Hypertext (Html) file instead of a text file.

## Remove Printers and Faxes from New Start Menu

The new Start Menu offers a link to the Printers and Faxes folder. From this folder users can view Server Properties for the print spooler. On the **Advanced** tab, users can view, not edit, the location of the spool folder. To disable easy access to the **Server Properties** dialog box, do one of the following:

1. Enable the “Turn on Classic Shell” and “Remove File menu from Windows Explorer” policies.
2. Set the following regvalue:

   [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]

   "Start_ShowPrinters" = REG_DWORD: 0x00000000
3. Enable the “Prevent changes to Taskbar and Start Menu Settings” policy. (The registry setting can be deployed by means of logon scripts (executing regedit /s hideprinters.reg) or by using a custom ADM file.)
4. Right-click the **Start** button, select **Properties**, select the **Start Menu** tab, and then click **Customize**.
5. Select the **Advanced** tab, clear the **Printers and Faxes** check box, and then enable the “Prevent changes to Taskbar and Start Menu Settings” policy. (It is recommended that you remove the Start Menu shortcut menus, and then disable access to Control Panel.
6. Disable the new Start Menu by enabling the “Force Classic Start Menu” policy, and then enable the “Remove File menu from Windows Explorer” policy.

## Disable the Full Path in Windows Explorer

By default the full path to the current folder in Windows Explorer is displayed. If Folder Redirection is used and users navigate beyond the My Documents folder, the address bar displays the full path to the folder. This is a configurable Folder Option that can not be set by group policies. To disable the full path, do one of the following:

1. In Windows Explorer, click **Tools** on the Toolbar, then select **Folder Options**.
2. Click the **View** tab, and then clear the **Display the full path in the address bar** and **Display the full path in the title bar** check boxes.
3. Enable the “Remove Folder Options menu item from Tools menu” policy.
4. Set the following regvalues:

   [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState]

   “FullPathAddress” = REG_DWORD: 0x00000000

   “FullPath” = REG_DWORD: 0x00000000

The registry setting can be deployed by means of logon scripts (executing regedit /s addressbar.reg) or by using a custom ADM file.

## Remove Internet Explorer and Windows Explorer from the Quick Launch Bar

By default links to Internet Explorer and Windows Explorer are added to the **Quick Launch** bar. These links can be removed from a logon script by adding the following lines:

```
del "%userprofile%\Application Data\Microsoft\Internet Explorer\Quick Launch\explorer.exe.lnk"

del "%userprofile%\Application Data\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk"
```

## Disable Help

Help files can be opened from many applications by pressing F1. Many of these help files can provide users with links to other applications and Web sites that they would normally not have access to. Group Policy does not exist to restrict access to help in applications. It is necessary to restrict NTFS access to .chm and .hlp files. The majority of Windows help files reside in the %SystemRoot%\Help folder—typically, c:\windows\help. Simply remove the user groups from the access control list to the folder. Then select the option to replace permission entries on all child objects. Doing so prevents Help files from opening for users.

## Network Browsing by Using the Common Open/Save File Dialog Box

The **Common Open/Save File** dialog box is used by many applications to open or save files. It can be seen by selecting **Open** or **Save** on the **File** menu from applications such as Notepad. From the path entry box, users can browse the network. From the **Open/Save File** dialog box, users can enter UNC paths, such as \\localhost, and then browse the shares for the local server. By using the UP ARROW to get to the parent object, the user can browse either the domain or the network. Although users might be able to see server and share names, they are still restricted by share-level and NTFS-level permissions. If you need to prevent users from viewing server or share names, the following options are available:

1. Use the RestrictAnonymous registry value in conjunction with share and NTFS permissions to restrict access. For more information, see Knowledge Base article 246261, "How to Use the RestrictAnonymous Registry Value in Windows 2000" at http://go.microsoft.com/fwlink/?LinkId=18396.
2. Hide a share name by adding a trailing "$" to the end of the share name. For more information, Knowledge Base article 90929, "Share Names With a "$" Character at the End Are Hidden" at http://go.microsoft.com/fwlink/?LinkId=18403.
3. Configure computers to not send announcements to browsers on the domain. This can be accomplished by adding the following registry value or executing the following command:

   From the registry:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters

   Value name: Hidden

   Data type: REG_DWORD

   Value data: 1

   The registry setting can be deployed by means of logon scripts (executing regedit /s addressbar.reg) or by using a custom ADM file.

   From the command line:

   ```
   "net config server /hidden:yes"
   ```

For more information, see Knowledge Base article 321710, "HOW TO: Hide a Windows 2000 -Based Computer from the Browser List" at http://go.microsoft.com/fwlink/?LinkId=18397

# Additional Restrictions

## Software Restriction Policies

Software restriction policies are a new feature in Microsoft Windows XP and Windows Server 2003. This important feature provides administrators with a policy-driven mechanism for identifying software programs running on computers in a domain, and it controls the ability of those programs to execute. Policies can be used to block malicious scripts, help lock down a computer, or prevent unwanted applications from running.

For additional information about Software Restriction Policies, see the whitepaper, "Using Software Restriction Policies to Protect Against Unauthorized Software," at http://go.microsoft.com/fwlink/?LinkId=17299 and Knowledge Base article 324036, "HOW TO: Use Software Restriction Policies in Windows Server 2003," at http://go.microsoft.com/fwlink/?LinkId=18400.

## Internet Explorer in Kiosk Mode

Administrators can replace the standard Windows Explorer user interface with Internet Explorer in Kiosk mode. When you run Internet Explorer in Kiosk mode, the Internet Explorer title bar, menus, toolbars, and status bar are not displayed, and Internet Explorer runs in Full Screen mode. Only Web pages are displayed. Internet Explorer in Kiosk mode can be enabled by enabling the following policy:

**[User Configuration\Administrative Templates\System]**

- Custom user interface

  Recommended setting: **Enabled**

  Interface file name: "%ProgramFiles%\Internet Explorer\IExplore.exe" –K

If Internet Explorer in Kiosk mode is used as the user interface, it is strongly recommend reviewing and enabling Internet Explorer restrictive policies under the following sections:

**[Computer Configuration\Administrative Templates\Windows Components\Internet Explorer]**

**[User Configuration\Administrative Templates\Windows Components\Internet Explorer]**

## Summary

Windows Server 2003 is a feature-rich platform that can provide the functionality of Terminal Server to a wide variety of environments. These deployments require various degrees of control and manageability. Using Active Directory, you can quickly and easily configure Terminal Server to integrate with diverse environments, providing controlled desktop functionality and managed access to applications.

## Related Links

See the following resources for further information:

- Microsoft Windows Server 2003 Terminal Server Overview at http://go.microsoft.com/fwlink/?LinkId=17300
- Microsoft Windows Server 2003 Active Directory Overview at http://go.microsoft.com/fwlink/?LinkId=18540
- Securing Windows 2000 Terminal Services at http://go.microsoft.com/fwlink/?LinkId=18404.
- How to Use the RestrictAnonymous Registry Value in Windows 2000at http://go.microsoft.com/fwlink/?LinkId=18396

  Knowledge Base article 90929 "Share Names With a "$" Character at the End Are Hidden" at http://go.microsoft.com/fwlink/?LinkId=18403
- .
- Knowledge Base article 321710, "HOW TO: Hide a Windows 2000 -Based Computer from the Browser List" at http://go.microsoft.com/fwlink/?LinkId=18397
- Using Software Restriction Policies to Protect Against Unauthorized Software at http://go.microsoft.com/fwlink/?LinkId=17299
- Knowledge Base article 324036 "HOW TO: Use Software Restriction Policies in Windows Server 2003," at http://go.microsoft.com/fwlink/?LinkId=18400
- Windows 2003 Server Web site at http://go.microsoft.com/fwlink/?LinkId=18405