Active Directory Group Policy

Administrator

Reference

Group Policy Administrator Reference for Administrative Templates

All policies are listed alphabetically by: policy node, policy path, and policy name.

For policy node:

- Computer Configuration / Administrative Templates policies are listed under COMPUTER.
- User Configuration / Administrative Templates policies are listed under USER.

For example, if you wanted to find the computer configuration policies for Administrative Templates\Component Updates, you would look under COMPUTER, Administrative Templates\Component Updates.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Code Download	Code Download		
COMPUTER	Administrative Templates\Component Updates	Help Menu > About Internet Explorer		
COMPUTER	Administrative Templates\Component Updates	Periodic check for updates to Internet Explorer and Internet Tools		
COMPUTER	Administrative Templates\Network	Sets how often a DFS Client discovers DC's	At least Microsoft Windows XP Professional or Windows Server 2003 family	Allows you to configure how often a Distributed File System (DFS) client attempts to discover domain controllers on their network. By default, a DFS client attempts to discover domain controllers every 15 minutes. If you enable this setting, you can configure how often a DFS client attempts to discover domain controllers. This value is specified in minutes. If you disable this setting or do not configure it, the default value of 15 minutes applies. Note: The minimum value you can select is 15 minutes. If you try to set this setting to a value less then 15 minutes, the default value of 15 minutes is applied.
COMPUTER	Administrative Templates\Network\Background Intelligent Transfer Service	Timeout (days) for inactive jobs	Windows XP or Windows Server 2003, or computers with BITS 1.5 installed.	The number of days a pending BITS job can remain inactive before being considered abandoned by the requestor. Once a job is determined to be abandoned, it is removed by the system and any downloaded files pertaining to the job are deleted from the disk. Any property changes for the job or any successful download action resets this timer. If the computer remains offline for a long period of time, no activity for the job will be recorded. You might want to increase this value if computers tend to stay offline for a longer period of time and still have pending jobs. You might want to decrease this value if you are concerned about orphaned jobs occupying disk space. If you enable this setting, you can configure the inactive job time-out to specified number of days. If you disable or do not configure this setting, the default value of 90 (days) will be used for the inactive job time-out.
COMPUTER	Administrative Templates\Network\Background Intelligent Transfer Service	Maximum network bandwith that BITS uses	Windows XP SP2 or Windows Server 2003 SP1, or computers with BITS 2.0 installed.	Limits the network bandwidth that BITS uses for background transfers (this policy does not affect foreground transfers). Specify a limit to use during a specific time interval and a limit to use at all other times. For example, limit the use of network bandwidth to 10 Kbps from 8AM to 5PM, and use all available unused bandwidth the rest of the time.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Specify the limit in kilobits per second (Kbps). Base the limit on the size of the network link, not the computer's network interface card (NIC). BITS uses approximately two kilobits if you specify a value less than two kilobits. To prevent BITS transfers from occurring, specify a limit of 0. If you disable or do not configure this policy, BITS uses all available unused bandwidth. Typically, you use this policy to prevent BITS transfers from competing for network bandwidth when the client has a fast network card (10Mbs), but is connected to the network via a slow link (56Kbs).
COMPUTER	Administrative Templates\Network\DNS Client	Connection-Specific DNS Suffix	Only works on Microsoft Windows XP Professional	Specifies a connection-specific DNS suffix. This setting supersedes the connection-specific DNS suffixes set on the computers to which this setting is applied, those configured locally and those configured using DHCP. Warning: A connection-specific DNS suffix specified in this setting is applied to all the network connections used by multihomed computers to which this setting is applied. To use this setting, click Enable, and then enter a string value representing the DNS suffix in the available field. If this setting is not configured, it is not applied to any computers, and computers use their local or DHCP-configuration parameters.
COMPUTER	Administrative Templates\Network\DNS Client	DNS Servers	Only works on Microsoft Windows XP Professional	Defines the DNS servers to which a computer sends queries when it attempts to resolve names. Warning: The list of the DNS servers defined in this setting supersedes DNS servers configured locally and those configured using DHCP. The list of DNS servers is applied to all network connections of multihomed computers to which this setting is applied. To use this setting, click Enable, and then enter a space-delimited list of IP addresses (in dotted decimal format) in the available field. If you enable this setting, you must enter at least one IP address. If this setting is not configured, it is not applied to any computers, and computers use their local or DHCP-configured parameters.
COMPUTER	Administrative Templates\Network\DNS Client	Primary DNS Suffix	At least Microsoft Windows 2000	Specifies the primary Domain Name System (DNS) suffix for all affected computers. The primary DNS suffix is used in DNS name registration and DNS name resolution. This setting lets you specify a primary DNS suffix for a group of computers and prevents users, including administrators, from changing it. If you disable this setting or do not configure it, each computer uses its local primary DNS suffix, which is usually the DNS name of Active Directory domain to which it is joined. However, administrators can use System in Control Panel to change the primary DNS suffix of a computer. To use this setting, in the text box

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				provided, type the entire primary DNS suffix you want to assign. For example, microsoft.com. This setting does not disable the DNS Suffix and NetBIOS Computer Name dialog box that administrators use to change the primary DNS suffix of a computer. However, if administrators enter a suffix, that suffix is ignored while this setting is enabled. Important: To make changes to this setting effective, you must restart Windows on all computers affected by the setting. Note: To change the primary DNS suffix of a computer without setting a setting, click System in Control Panel, click the Network Identification tab, click Properties, click More, and then enter a suffix in the Primary DNS suffix of this computer box. For more information about DNS, see Domain Name System (DNS) in Help.
COMPUTER	Administrative Templates\Network\DNS Client	Register DNS records with connection-specific DNS suffix	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines if a computer performing dynamic registration may register A and PTR resource records with a concatenation of its Computer Name and a connection-specific DNS suffix, in addition to registering these records with a concatenation of its Computer Name and the Primary DNS suffix. Warning: Enabling of this group setting is applied to all the network connections of multihomed computers to which this setting is applied. By default, a DNS client performing dynamic DNS registration registers A and PTR resource records with a concatenation of its Computer Name and the primary DNS suffix. For example, a concatenation of a Computer Name, such as mycomputer, and the primary DNS suffix, such as microsoft.com, would result in mycomputer.microsoft.com. If this setting were enabled, a computer would register A and PTR resource records with its connection-specific DNS suffix in addition to registering A and PTR resource records with the primary DNS suffix. For example, a concatenation of a Computer Name mycomputer and the connection specific DNS suffix VPNconnection would be used when registering A and PTR resource records, resulting in mycomputer.VPNconnection. Notice that if dynamic DNS registration is disabled on a computer to which this setting is applied, then, regardless of this setting's settings, a computer does not attempt dynamic DNS registration of A and PTR records containing a concatenation of its Computer Name and a connection-specific DNS suffix. If dynamic DNS registration is disabled on a specific network connection of a computer to which this setting is applied, then, regardless of this setting's settings, a computer does not attempt dynamic DNS registration of A and PTR records containing a concatenation of its Computer Name and a connection-specific DNS

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				suffix on that network connection. If this setting is disabled, a DNS client does not register A and PTR resource records with its connection-specific DNS suffix. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\Network\DNS Client	Register PTR Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether the registration of PTR resource records is enabled for the computers to which this policy is applied. By default, DNS clients configured to perform dynamic DNS registration attempt PTR resource record registration only if they successfully registered the corresponding A resource record. A resource records map a host DNS name to the host IP address, and PTR resource records map the host IP address to the host DNS name. To enable this setting, click Enable, and then select one of the following values: Do not register - computers never attempt PTR resource records registration. Register - computers attempt PTR resource records registration regardless of the success of the A records registration. Register only if A record registration succeeds - computers attempt PTR resource records registration only if they successfully registered the corresponding A resource records. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\Network\DNS Client	Dynamic Update	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines if dynamic update is enabled. Computers configured for dynamic update automatically register and update their DNS resource records with a DNS server. If you enable this setting, the computers to which this setting is applied may use dynamic DNS registration on each of their network connections, depending on the configuration of each individual network connection. For a dynamic DNS registration to be enabled on a specific network connection, it is necessary and sufficient that both computer-specific and connection-specific configurations allow dynamic DNS registration. This setting controls the computer-specific property controlling dynamic DNS registration. If you enable this setting, you allow dynamic update to be set individually for each of the network connections. If you disable this setting, the computers to which this setting is applied may not use dynamic DNS registration for any of their network connections, regardless of the configuration for individual network connections. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\Network\DNS Client	Replace Addresses In Conflicts	Only works on Microsoft Windows XP Professional	Determines whether a DNS client that attempts to register its A resource record should overwrite an existing A resource record or records containing conflicting IP addresses. This setting is designed for

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				computers that register A resource records in DNS zones that do not support Secure Dynamic Update. Secure Dynamic Update preserves ownership of resource records and does not allow a DNS client to overwrite records that are registered by other computers. During dynamic update of a zone that does not use Secure Dynamic Update, a DNS client may discover that an existing A resource record associates the client's host DNS name with an IP address of a different computer. According to the default configuration, the DNS client attempts to replace the existing A resource record with an A resource record associating the DNS name with the client's IP address. If you enable this setting, DNS clients attempt to replace conflicting A resource records during dynamic update. If you disable this setting, the DNS client still performs the dynamic update of A resource records, but if the DNS client attempts to update A resource records containing conflicts, this attempt fails and an error is recorded in the Event Viewer log. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\Network\DNS Client	Registration Refresh Interval	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the Registration Refresh Interval of A and PTR resource records for computers to which this setting is applied. This setting may be applied to computers using dynamic update only. Computers running Windows 2000 Professional and Windows XP Professional, and configured to perform dynamic DNS registration of A and PTR resource records, periodically reregister their records with DNS servers, even if their records' data has not changed. This reregistration is required to indicate to DNS servers configured to automatically remove (scavenge) stale records that these records are current and should be preserved in the database. Warning: If the DNS resource records are registered in zones with scavenging enabled, the value of this setting should never be longer than the Refresh Interval configured for these zones. Setting the Registration Refresh Interval to longer than the Refresh Interval of the DNS zones might result in the undesired deletion of A and PTR resource records. To specify the Registration Refresh Interval, click Enable, and then enter a value larger than 1800. Remember, this value specifies the Registration Refresh Interval in seconds, for example, 1800 seconds is 30 minutes. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\Network\DNS Client	TTL Set in the A and PTR records	At least Microsoft Windows XP Professional or	Specifies the value for the Time-To-Live (TTL) field in A and PTR resource records registered by the computers to which this setting is applied. To specify the TTL, click Enable, and then enter a value in

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			Windows Server 2003 family	seconds (for example, the value 900 is 15 minutes). If this setting is not configured, it is not applied to any computer.
COMPUTER	Administrative Templates\Network\DNS Client	DNS Suffix Search List	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines the DNS suffixes to attach to an unqualified single-label name before submission of a DNS query for that name. An unqualified single-label name contains no dots, such as example. This is different from a fully qualified domain name, such as example.microsoft.com.. With this setting enabled, when a user submits a query for a single-label name, such as example, a local DNS client attaches a suffix, such as microsoft.com, resulting in the query example.microsoft.com, before sending the query to a DNS server. If you enable this setting, you can specify the DNS suffixes to attach before submission of a query for an unqualified single-label name. The values of the DNS suffixes in this setting may be set using comma-separated strings, such as microsoft.com,serverua.microsoft.com,office.microsoft.com. One DNS suffix is attached for each submission of a query. If a query is unsuccessful, a new DNS suffix is added in place of the failed suffix, and this new query is submitted. The values are used in the order they appear in the string, starting with the leftmost value and preceding to the right. If you enable this setting, you must specify at least one suffix. If you disable this setting, the primary DNS suffix and network connection-specific DNS suffixes are appended to the unqualified queries. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\Network\DNS Client	Update Security Level	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether the computers to which this setting is applied use secure dynamic update or standard dynamic update for registration of DNS records. To enable this setting, click Enable, and then choose one of the following values. Unsecure followed by secure - if this option is chosen, computers send secure dynamic updates only when nonsecure dynamic updates are refused. Only Unsecure - if this option is chosen, computers send only nonsecure dynamic updates. Only Secure - if this option is chosen, computers send only secure dynamic updates. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\Network\DNS Client	Update Top Level Domain Zones	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether the computers to which this setting is applied may send dynamic updates to the zones named with a single label name, also known as top-level domain zones, for example, com. By default, a DNS client configured to perform dynamic DNS update sends dynamic updates to the DNS zone that is authoritative for its DNS resource

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				records, unless the authoritative zone is a top-level domain and root zone. If this setting is enabled, computers to which this policy is applied send dynamic updates to any zone that is authoritative for the resource records that the computer needs to update, except the root zone. If this setting is disabled, computers to which this policy is applied do not send dynamic updates to the root and/or top-level domain zones that are authoritative for the resource records that the computer needs to update. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\Network\DNS Client	Primary DNS Suffix Devolution	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether the DNS client performs primary DNS suffix devolution in a name resolution process. When a user submits a query for a single-label name, such as example, a local DNS client attaches a suffix, such as microsoft.com, resulting in the query example.microsoft.com, before sending the query to a DNS server. If a DNS Suffix Search List is not specified, the DNS client attaches the Primary DNS Suffix to a single-label name, and, if this query fails, the Connection-Specific DNS suffix is attached for a new query. If none of these queries are resolved, the client devolves the Primary DNS Suffix of the computer (drops the leftmost label of the Primary DNS Suffix), attaches this devolved Primary DNS suffix to the single-label name, and submits this new query to a DNS server. For example, if the primary DNS suffix ooo.aaa.microsoft.com is attached to the non-dot-terminated single-label name example, and the DNS query for example.ooo.aaa.microsoft.com fails, the DNS client devolves the primary DNS suffix (drops the leftmost label), and submits a query for example.aaa.microsoft.com. If this query fails, the primary DNS suffix is devolved further and the query example.microsoft.com is submitted. If this query fails, devolution continues and the query example.microsoft.com is submitted. The primary DNS suffix would not be devolved further because the DNS suffix has two labels, microsoft.com. The primary DNS suffix cannot be devolved to less than two labels. If this setting is enabled, DNS clients on the computers to which this setting is applied attempt to resolve names that are concatenations of the single-label name to be resolved and the devolved Primary DNS Suffix. If this setting is disabled, DNS clients on the computers to which this setting is applied donot attempt to resolve names that are concatenations of the single-label name to be resolved and the devolved Primary DNS Suffix. If this setting is not configured, it is not applied to any computers, and computers use their local

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				configuration.
COMPUTER	Administrative Templates\Network\DNS Client			
COMPUTER	Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services	Turn off Microsoft Peer-to-Peer Networking Services	At least Microsoft Windows XP Professional with SP2	Allows configuration of components of the operating system used by a client computer to connect to a network. This includes DNS settings and Offline Files.
COMPUTER	Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services\Peer Name Resolution Protocol\Global Clouds	Turn off Multicast Bootstrap	At least Microsoft Windows XP Professional with SP2	
COMPUTER	Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services\Peer Name Resolution Protocol\Global Clouds	Set the Seed Server	At least Microsoft Windows XP Professional with SP2	The Peer Name Resolution Protocol (PNRP) allows for distributed resolution of a name to an IPV6 address and port number. The protocol operates in the context of clouds; a cloud is a set of peers that can communicate with each other using the same IPv6 scope. There are three types of clouds - global, site-local and link-local: a) If a computer is connected to the Internet, it is part of a global cloud. b) If a computer is connected to one or more local area networks, individual link-local clouds are available for each link. c) If your organization has been configured to support IPv6 sites, individual site-local clouds are available for each specific site. PNRP needs to be bootstrapped before it can participate in a cloud. There are three ways in which this can be done: 1. If the computer has participated in the peer to peer cloud previously, the protocol can use cached information to bootstrap itself. 2. If step 1 does not work, the computer sends a local SSDP multicast message on the subnet to see if there are other online computers that can help bootstrap it. 3. If step 2 does not work, the computer sends a message to well known node (called a seed server) hosted on the Internet; alternatively, this can be configured using policy to point to a node within the corporation as well.
COMPUTER	Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services\Peer Name Resolution Protocol\Link-Local Clouds	Turn off Multicast Bootstrap	At least Microsoft Windows XP Professional with SP2	

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services\Peer Name Resolution Protocol\Link-Local Clouds	Set the Seed Server	At least Microsoft Windows XP Professional with SP2	
COMPUTER	Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services\Peer Name Resolution Protocol\Site-Local Clouds	Turn off Multicast Bootstrap	At least Microsoft Windows XP Professional with SP2	
COMPUTER	Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services\Peer Name Resolution Protocol\Site-Local Clouds	Set the Seed Server	At least Microsoft Windows XP Professional with SP2	
COMPUTER	Administrative Templates\Network\Network Connections	IEEE 802.1x Certificate Authority for Machine Authentication	At least Microsoft Windows XP Professional or Windows Server 2003 family	If you want to use IEEE 802.1x machine authentication, configure this setting. If you enable this setting, it configures the Certificate Authority to be used on the client for authentication. To allow successful authentication, enable this setting and indicate the thumbprint or hash for your Certificate Authority. If you disable or do not configure this setting, the Certificate Authority for IEEE 802.1x machine authentication will not be configured on your client. This might cause machine authentication to fail. Note: The Certificate Authority that is configured by this setting only applies to machine authentication, and not to user authentication.
COMPUTER	Administrative Templates\Network\Network Connections	Prohibit installation and configuration of Network Bridge on your DNS domain network	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether a user can install and configure the Network Bridge. Important: This settings is location aware. It only applies when a computer is connected to the same DNS domain network it was connected to when the setting was refreshed on that computer. If a computer is connected to a DNS domain network other than the one it was connected to when the setting was refreshed, this setting does not apply. The Network Bridge allows users to create a layer 2 MAC bridge, enabling them to connect two or more network segements together. This connection appears in the Network Connections folder. If you disable this setting or do not configure it, the user will be able to create and modify the configuration of a Network Bridge. Enabling this setting does not remove an existing Network Bridge from the user's computer.
COMPUTER	Administrative	Prohibit use of Internet	At least Microsoft	Prohibits use of Internet Connection Firewall on your DNS domain

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Templates\Network\Network Connections	Connection Firewall on your DNS domain network	Windows XP Professional or Windows Server 2003 family	network. Determines whether users can enable the Internet Connection Firewall feature on a connection, and if the Internet Connection Firewall service can run on a computer. Important: This setting is location aware. It only applies when a computer is connected to the same DNS domain network it was connected to when the setting was refreshed on that computer. If a computer is connected to a DNS domain network other than the one it was connected to when the setting was refreshed, this setting does not apply. The Internet Connection Firewall is a stateful packet filter for home and small office users to protect them from Internet network security threats. If you enable this setting, Internet Connection Firewall cannot be enabled or configured by users (including administrators), and the Internet Connection Firewall service cannot run on the computer. The option to enable the Internet Connection Firewall through the Advanced tab is removed. In addition, the Internet Connection Firewall is not enabled for remote access connections created through the Make New Connection Wizard. The Network Setup Wizard is disabled. Note: If you enable the Windows Firewall: Protect all network connections policy setting, the Prohibit use of Internet Connection Firewall on your DNS domain network policy setting has no effect on computers that are running Windows Firewall, which replaces Internet Connection Firewall when you install Windows XP Service Pack 2. If you disable this setting or do not configure it, the Internet Connection Firewall is disabled when a LAN Connection or VPN connection is created, but users can use the Advanced tab in the connection properties to enable it. The Internet Connection Firewall is enabled by default on the connection for which Internet Connection Sharing is enabled. In addition, remote access connections created through the Make New Connection Wizard have the Internet Connection Firewall enabled.
COMPUTER	Administrative Templates\Network\Network Connections	Prohibit use of Internet Connection Sharing on your DNS domain network	At least Microsoft Windows 2000 Service Pack 1	Determines whether administrators can enable and configure the Internet Connection Sharing (ICS) feature of an Internet connection and if the ICS service can run on the computer. Important: This setting is location aware. It only applies when a computer is connected to the same DNS domain network it was connected to when the setting was refreshed on that computer. If a computer is connected to a DNS domain network other than the one it was connected to when the setting was refreshed, this setting does not apply. ICS lets administrators configure their system as an Internet gateway for a small network and provides network services, such as name resolution and addressing through

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				DHCP, to the local private network. If you enable this setting, ICS cannot be enabled or configured by administrators, and the ICS service cannot run on the computer. The Advanced tab in the Properties dialog box for a LAN or remote access connection is removed. The Internet Connection Sharing page is removed from the New Connection Wizard. The Network Setup Wizard is disabled. If you disable this setting or do not configure it and have two or more connections, administrators can enable ICS. The Advanced tab in the properties dialog box for a LAN or remote access connection is available. In addition, the user is presented with the option to enable Internet Connection Sharing in the Network Setup Wizard and Make New Connection Wizard. (The Network Setup Wizard is available only in Windows XP Professional.) By default, ICS is disabled when you create a remote access connection, but administrators can use the Advanced tab to enable it. When running the New Connection Wizard or Network Setup Wizard, administrators can choose to enable ICS. Note: Internet Connection Sharing is only available when two or more network connections are present. Note: When the Prohibit access to properties of a LAN connection, Ability to change properties of an all user remote access connection, or Prohibit changing properties of a private remote access connection settings are set to deny access to the Connection Properties dialog box, the Advanced tab for the connection is blocked. Note: Nonadministrators are already prohibited from configuring Internet Connection Sharing, regardless of this setting.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall	Windows Firewall: Allow authenticated IPSec bypass	At least Microsoft Windows XP Professional with SP2	Allows unsolicited incoming messages from specified systems that authenticate using the IPSec transport. If you enable this policy setting, you can view and change a list of computers or groups of computers. If a computer on that list authenticates using IPSec, Windows Firewall does not block its unsolicited messages. This policy setting overrides other policy settings that would block those messages. If you disable or do not configure this policy setting, Windows Firewall makes no exception for messages sent by computers that authenticate using IPSec. If you enable this policy setting and add systems to the list, upon disabling this policy, Windows Firewall deletes the list. Note: You define entries in this list by using Security Descriptor Definition Language (SDDL) strings. For more information about the SDDL format, see Security Descriptor String Format at the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=25131).
COMPUTER	Administrative	Windows Firewall:	At least Microsoft	Allows you to view and change a list of programs and specify whether

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Templates\Network\Network Connections\Windows Firewall\Domain Profile	Define program exceptions	Windows XP Professional with SP2	each program is allowed to receive unsolicited incoming messages. Windows Firewall manages two such lists: the first is defined by Group Policy settings, and the second is defined by the actions of local computer administrators. Windows Firewall ignores the second list unless you enable the Windows Firewall: Allow local program exceptions policy setting. If you enable this policy setting, you can view and change the list of program exceptions defined by Group Policy settings. If you add a program to this list and set its status to Enabled, that program can receive unsolicited incoming messages on any port it asks Windows Firewall to open, even if that port is blocked by using the Windows Firewall: Define port exceptions policy setting. To view the program list, enable the policy setting and then click the Show button. To add a program, enable the policy setting, note the syntax in the shaded area below, click the Show button, click the Add button, and then type a definition string that uses the syntax format. To remove a program, click its definition, and then click the Remove button. To edit a definition, remove the current definition from the list and add a new one with different parameters. To allow local computer administrators to add programs to the list, enable this policy setting and the Windows Firewall: Allow local program exceptions policy setting. If you disable this policy setting, the program exceptions list defined by Group Policy is deleted, and the one defined by local computer administrators is ignored. If you do not configure this policy setting, Windows Firewall will only use the list defined by local computer administrators. Notes: If you type an invalid definition string, Windows Firewall adds it to the list without checking for errors. This allows you to add programs that you have not installed yet, but be aware that you can accidentally create multiple entries for the same program with conflicting Scope or Status values. Scope parameters are combined for multiple entries. If the Status parameter of a definition string is set to disabled, Windows Firewall prohibits incoming messages to this program. If entries have different Status values, then any definition with the Status set to disabled overrides all definitions with the Status set to enabled, and the program does not receive the messages. Therefore, if you set the Status to disabled, you can prevent local computer administrators from enabling the program. Windows Firewall opens ports for the program only when the program is running and listening for incoming messages. If the program is not running, or is running but not listening for those messages, Windows Firewall does not open its ports.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow local program exceptions	At least Microsoft Windows XP Professional with SP2	Allows you to specify that local computer administrators can supplement Windows Firewall: Define program exceptions list. If you enable this policy setting, and you define a program exceptions list by using the Windows Firewall: Define program exceptions policy setting, local computer administrators can add definitions to the list. If you disable or do not configure this policy setting, local computer administrators cannot add definitions to the list defined by the Windows Firewall: Define program exceptions policy setting.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow remote administration exception	At least Microsoft Windows XP Professional with SP2	Allows remote administration of this computer using administrative tools like the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure (RPC) calls and Dynamic COM (DCOM). In effect, Windows Firewall adds SVCHOST.EXE and LSASS.EXE to the program exceptions list: it allows hosted services to open additional, dynamically-assigned ports, typically in the range of 1024 to 1034. If you enable this policy setting, Windows Firewall allows the computer to receive the unsolicited incoming messages associated with remote administration. You must specify whether those messages are allowed from computers anywhere on the network or only from computers on the local subnet. If you disable or do not configure this policy setting, Windows Firewall blocks port 135 and does not open 445. Also, in effect, it adds SVCHOST.EXE and LSASS.EXE to the program exceptions list with the Status of disabled. Because disabling this policy setting does not block TCP port 445, it does not conflict with the Windows Firewall: Allow file and printer sharing exception policy setting. Note: Malicious users often attempt to attack networks and computers using RPC and DCOM. We recommend that you contact the manufacturers of your critical programs to determine if they require RPC and DCOM communication. If they do not, then do not enable this policy setting.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Protect all network connections	At least Microsoft Windows XP Professional with SP2	Turns on Windows Firewall, which replaces Internet Connection Firewall on all computers that are running Windows XP Service Pack 2. If you enable this policy setting, Windows Firewall runs and ignores the Prohibit use of Internet Connection Firewall on your DNS domain network policy setting. If you do not configure this policy setting, Windows Firewall runs unless you enable the Computer Configuration\Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Firewall on your DNS domain network policy setting. If you

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				disable this policy setting, Windows Firewall does not run. This is the only way to ensure that Windows Firewall does not run and local computer administrators cannot start it.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Do not allow exceptions	At least Microsoft Windows XP Professional with SP2	Specifies that Windows Firewall blocks all unsolicited incoming messages. This policy setting overrides all other Windows Firewall policy settings that allow such messages. If you enable this policy setting, you should also enable the Windows Firewall: Protect all network connections policy setting; otherwise, local computer administrators can work around the Windows Firewall: Do not allow exceptions policy setting by turning off the firewall. If you disable or do not configure this policy setting, Windows Firewall applies other policy settings that allow unsolicited incoming messages.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow file and printer sharing exception	At least Microsoft Windows XP Professional with SP2	Allows file and printer sharing. To do this, Windows Firewall opens UDP ports 137 and 138, and TCP ports 139 and 445. If you enable this policy setting, Windows Firewall allows this computer to receive the unsolicited incoming messages generated by computers that attempt to send print jobs or access shared files. You must specify whether these messages are allowed from computers anywhere on the network or only from computers on the local subnet. If you disable this policy setting, Windows Firewall blocks these ports and prohibits the Server service from receiving incoming messages. As a result, shared files and printers on this computer will be unavailable from other computers. If you do not configure this policy setting, Windows Firewall does not block these ports or prohibit the Server service from receiving incoming messages, but neither does it open the ports or enable the Server service. In most cases, if you do not configure this policy setting, the result is the same as disabling the policy setting: shared files and printers on this computer will be unavailable from other computers.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow ICMP exceptions	At least Microsoft Windows XP Professional with SP2	Defines the set of Internet Control Message Protocol (ICMP) messages that are enabled. Utilities can use ICMP messages to determine the status of other computers. For example, Ping uses the echo request. If you do not enable the Allow inbound echo request message type, Windows Firewall blocks echo request messages sent by Ping running on other computers, but it does not block outbound echo request messages sent by Ping running on this computer. If you enable this policy setting, you must specify which ICMP message types Windows Firewall allows this computer to send or receive. If you disable or do not configure this policy setting, Windows Firewall blocks all incoming and

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				outgoing ICMP message types shown in the list. As a result, utilities that use ICMP messages might not be able to send those messages to or from this computer. If you enable this policy setting and allow certain message types, then later disable this policy setting, Windows Firewall deletes the list of message types that you had enabled. Notes: If any policy setting opens TCP port 445, Windows Firewall allows inbound echo requests, even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow file and printer sharing exception, Windows Firewall: Allow remote administration exception, and Windows Firewall: Define port exceptions. Other Windows Firewall policy settings affect only incoming messages, but several of the options of the Windows Firewall: Allow ICMP exceptions policy setting affect outgoing communication.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow logging	At least Microsoft Windows XP Professional with SP2	Allows Windows Firewall to record information about the unsolicited incoming messages that it receives. If you enable this policy setting, Windows Firewall writes the information to a log file. You must provide the name, location, and maximum size of the log file. The location can contain environment variables. You must also specify whether to record information about incoming messages that the firewall blocks (drops), and information about successful incoming and outgoing connections. Windows Firewall does not provide an option to log successful incoming messages. If you disable or do not configure this policy setting, Windows Firewall does not record information in the log file. If you enable this policy setting, and Windows Firewall creates the log file and adds information, then upon disabling this policy setting, Windows Firewall leaves the log file intact.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Prohibit notifications	At least Microsoft Windows XP Professional with SP2	Prevents Windows Firewall from displaying notifications to the user when a program requests that Windows Firewall add the program to the program exceptions list. If you enable this policy setting, Windows Firewall prevents the display of these notifications. If you disable or do not configure this policy setting, Windows Firewall allows the display of these notifications.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Define port exceptions	At least Microsoft Windows XP Professional with SP2	Allows you to define a port exceptions list that Windows Firewall uses to open or block ports. Windows Firewall manages two such lists: the first is defined by Group Policy settings, and the second is defined by the actions of local computer administrators. Windows Firewall ignores the second list unless you enable the Windows Firewall: Allow local port

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				exceptions policy setting. If you enable this policy setting, you can view and change the port exceptions list defined by Group Policy settings. To view the list, enable the policy setting and then click the Show button. To add a port, enable the policy setting, note the syntax in the shaded area below, click the Show button, click the Add button, and then type a definition string that uses the syntax format. To remove a port, click its definition, and then click the Remove button. To edit a definition, remove the current definition from the list and add a new one with different parameters. The Scope parameter of a definition string specifies which set of computers can send messages intended for this program: * allows messages from all computers on the network; localsubnet allows messages only from computers on the same subnet as this computer. If you disable this policy setting, Windows Firewall blocks all ports in the exceptions list defined by Group Policy, except those opened by other policy settings. Windows Firewall ignores the list defined by local computer administrators. If you enable this policy setting and later disable it, Windows Firewall deletes the port exceptions list specified by Group Policy. If you do not configure this policy setting, other policy settings can open ports. Windows Firewall ignores entries in the port exceptions list defined by this policy setting, but uses the list defined by local computer administrators. Notes: Windows Firewall does not check the definition string for syntax errors. If you type an invalid definition string, Windows Firewall adds the invalid definition to the list without displaying a warning or error message. If you type multiple entries for the same port, and any entry disables a port, it overrides all entries that enable that port. If multiple entries for the same port have different scopes, the scopes are additive. To allow local computer administrators to open additional ports, enable this policy setting and the Windows Firewall: Allow local port exceptions policy setting.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow local port exceptions	At least Microsoft Windows XP Professional with SP2	Allows you to distribute a port exceptions list with entries that local computer administrators cannot override, but that they can supplement with other opened or blocked ports. If you enable this policy setting, and define a port exceptions list by using the Windows Firewall: Define port exceptions policy setting, local computer administrators can add definitions to that list. If you disable or do not configure this policy setting, local computer administrators cannot add definitions to that list.
COMPUTER	Administrative Templates\Network\Network Connections\Windows	Windows Firewall: Allow Remote Desktop exception	At least Microsoft Windows XP Professional with	Allows this computer to receive the unsolicited incoming messages created by Remote Desktop requests sent from another computer. To do this, Windows Firewall opens TCP port 3389. If you enable this policy

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Firewall\Domain Profile		SP2	setting, you must specify whether the incoming Remote Desktop requests to this computer are permitted from computers anywhere on the network or only from computers on the local subnet. If you disable or do not configure this policy setting, Windows Firewall blocks TCP port 3389, which prevents access to Remote Desktop.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Prohibit unicast response to multicast or broadcast requests	At least Microsoft Windows XP Professional with SP2	Prevents this computer from receiving unicast responses to its outgoing multicast or broadcast messages. If you enable this policy setting, and this computer sends multicast or broadcast messages to other computers, Windows Firewall blocks the unicast responses sent by those other computers. If you disable or do not configure this policy setting, and this computer sends a multicast or broadcast message to other computers, Windows Firewall waits as long as three seconds for unicast responses from the other computers, and then blocks all later responses. Note: This policy setting has no effect if the unicast message is a response to a Dynamic Host Configuration Protocol (DHCP) multicast message sent by this computer. Windows Firewall always permits those DHCP unicast responses. However, this policy setting can interfere with the NetBIOS messages that detect name conflicts.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow UPnP framework exception	At least Microsoft Windows XP Professional with SP2	Opens the ports required to allow this computer to receive unsolicited Plug and Play messages sent by network devices, such as routers with built-in firewalls. To do this, Windows Firewall opens TCP port 2869, and UDP port 1900. If you enable this policy setting, Windows Firewall opens these ports and allows the computer to receive Plug and Play messages. You must specify whether the incoming Plug and Play messages to this computer are permitted from devices anywhere on the network or only from devices on the local subnet. If you disable this policy setting, Windows Firewall blocks these ports, which prevents the computer from receiving Plug and Play messages. If you do not configure this policy setting, Windows Firewall does not block or open these ports. In most cases, this has the same effect as disabling this policy setting: it prevents the computer from receiving Plug and Play messages.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Define program exceptions	At least Microsoft Windows XP Professional with SP2	Allows you to view and change a list of programs and specify whether each program is allowed to receive unsolicited incoming messages. Windows Firewall manages two such lists: the first is defined by Group Policy settings, and the second is defined by the actions of local computer administrators. Windows Firewall ignores the second list unless you enable the Windows Firewall: Allow local program exceptions

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				policy setting. If you enable this policy setting, you can view and change the list of program exceptions defined by Group Policy settings. If you add a program to this list and set its status to Enabled, that program can receive unsolicited incoming messages on any port it asks Windows Firewall to open, even if that port is blocked by using the Windows Firewall: Define port exceptions policy setting. To view the program list, enable the policy setting and then click the Show button. To add a program, enable the policy setting, note the syntax in the shaded area below, click the Show button, click the Add button, and then type a definition string that uses the syntax format. To remove a program, click its definition, and then click the Remove button. To edit a definition, remove the current definition from the list and add a new one with different parameters. To allow local computer administrators to add programs to the list, enable this policy setting and the Windows Firewall: Allow local program exceptions policy setting. If you disable this policy setting, the program exceptions list defined by Group Policy is deleted, and the one defined by local computer administrators is ignored. If you do not configure this policy setting, Windows Firewall will only use the list defined by local computer administrators. Notes: If you type an invalid definition string, Windows Firewall adds it to the list without checking for errors. This allows you to add programs that you have not installed yet, but be aware that you can accidentally create multiple entries for the same program with conflicting Scope or Status values. Scope parameters are combined for multiple entries. If the Status parameter of a definition string is set to disabled, Windows Firewall prohibits incoming messages to this program. If entries have different Status values, then any definition with the Status set to disabled overrides all definitions with the Status set to enabled, and the program does not receive the messages. Therefore, if you set the Status to disabled, you can prevent local computer administrators from enabling the program. Windows Firewall opens ports for the program only when the program is running and listening for incoming messages. If the program is not running, or is running but not listening for those messages, Windows Firewall does not open its ports.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Allow local program exceptions	At least Microsoft Windows XP Professional with SP2	Allows you to specify that local computer administrators can supplement Windows Firewall: Define program exceptions list. If you enable this policy setting, and you define a program exceptions list by using the Windows Firewall: Define program exceptions policy setting, local computer administrators can add definitions to the list. If you disable or

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				do not configure this policy setting, local computer administrators cannot add definitions to the list defined by the Windows Firewall: Define program exceptions policy setting.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Allow remote administration exception	At least Microsoft Windows XP Professional with SP2	Allows remote administration of this computer using administrative tools like the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure (RPC) calls and Dynamic COM (DCOM). In effect, Windows Firewall adds SVCHOST.EXE and LSASS.EXE to the program exceptions list: it allows hosted services to open additional, dynamically-assigned ports, typically in the range of 1024 to 1034. If you enable this policy setting, Windows Firewall allows the computer to receive the unsolicited incoming messages associated with remote administration. You must specify whether those messages are allowed from computers anywhere on the network or only from computers on the local subnet. If you disable or do not configure this policy setting, Windows Firewall blocks port 135 and does not open 445. Also, in effect, it adds SVCHOST.EXE and LSASS.EXE to the program exceptions list with the Status of disabled. Because disabling this policy setting does not block TCP port 445, it does not conflict with the Windows Firewall: Allow file and printer sharing exception policy setting. Note: Malicious users often attempt to attack networks and computers using RPC and DCOM. We recommend that you contact the manufacturers of your critical programs to determine if they require RPC and DCOM communication. If they do not, then do not enable this policy setting.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Protect all network connections	At least Microsoft Windows XP Professional with SP2	Turns on Windows Firewall, which replaces Internet Connection Firewall on all computers that are running Windows XP Service Pack 2. If you enable this policy setting, Windows Firewall runs and ignores the Prohibit use of Internet Connection Firewall on your DNS domain network policy setting. If you do not configure this policy setting, Windows Firewall runs unless you enable the Computer Configuration\Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Firewall on your DNS domain network policy setting. If you disable this policy setting, Windows Firewall does not run. This is the only way to ensure that Windows Firewall does not run and local computer administrators cannot start it.
COMPUTER	Administrative	Windows Firewall: Do	At least Microsoft	Specifies that Windows Firewall blocks all unsolicited incoming

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Templates\Network\Network Connections\Windows Firewall\Standard Profile	not allow exceptions	Windows XP Professional with SP2	messages. This policy setting overrides all other Windows Firewall policy settings that allow such messages. If you enable this policy setting, you should also enable the Windows Firewall: Protect all network connections policy setting; otherwise, local computer administrators can work around the Windows Firewall: Do not allow exceptions policy setting by turning off the firewall. If you disable or do not configure this policy setting, Windows Firewall applies other policy settings that allow unsolicited incoming messages.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Allow file and printer sharing exception	At least Microsoft Windows XP Professional with SP2	Allows file and printer sharing. To do this, Windows Firewall opens UDP ports 137 and 138, and TCP ports 139 and 445. If you enable this policy setting, Windows Firewall allows this computer to receive the unsolicited incoming messages generated by computers that attempt to send print jobs or access shared files. You must specify whether these messages are allowed from computers anywhere on the network or only from computers on the local subnet. If you disable this policy setting, Windows Firewall blocks these ports and prohibits the Server service from receiving incoming messages. As a result, shared files and printers on this computer will be unavailable from other computers. If you do not configure this policy setting, Windows Firewall does not block these ports or prohibit the Server service from receiving incoming messages, but neither does it open the ports or enable the Server service. In most cases, if you do not configure this policy setting, the result is the same as disabling the policy setting: shared files and printers on this computer will be unavailable from other computers.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Allow ICMP exceptions	At least Microsoft Windows XP Professional with SP2	Defines the set of Internet Control Message Protocol (ICMP) messages that are enabled. Utilities can use ICMP messages to determine the status of other computers. For example, Ping uses the echo request. If you do not enable the Allow inbound echo request message type, Windows Firewall blocks echo request messages sent by Ping running on other computers, but it does not block outbound echo request messages sent by Ping running on this computer. If you enable this policy setting, you must specify which ICMP message types Windows Firewall allows this computer to send or receive. If you disable or do not configure this policy setting, Windows Firewall blocks all incoming and outgoing ICMP message types shown in the list. As a result, utilities that use ICMP messages might not be able to send those messages to or from this computer. If you enable this policy setting and allow certain message types, then later disable this policy setting, Windows Firewall deletes the list of message types that you had enabled. Notes: If any

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				policy setting opens TCP port 445, Windows Firewall allows inbound echo requests, even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow file and printer sharing exception, Windows Firewall: Allow remote administration exception, and Windows Firewall: Define port exceptions. Other Windows Firewall policy settings affect only incoming messages, but several of the options of the Windows Firewall: Allow ICMP exceptions policy setting affect outgoing communication.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Allow logging	At least Microsoft Windows XP Professional with SP2	Allows Windows Firewall to record information about the unsolicited incoming messages that it receives. If you enable this policy setting, Windows Firewall writes the information to a log file. You must provide the name, location, and maximum size of the log file. The location can contain environment variables. You must also specify whether to record information about incoming messages that the firewall blocks (drops), and information about successful incoming and outgoing connections. Windows Firewall does not provide an option to log successful incoming messages. If you disable or do not configure this policy setting, Windows Firewall does not record information in the log file. If you enable this policy setting, and Windows Firewall creates the log file and adds information, then upon disabling this policy setting, Windows Firewall leaves the log file intact.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Prohibit notifications	At least Microsoft Windows XP Professional with SP2	Prevents Windows Firewall from displaying notifications to the user when a program requests that Windows Firewall add the program to the program exceptions list. If you enable this policy setting, Windows Firewall prevents the display of these notifications. If you disable or do not configure this policy setting, Windows Firewall allows the display of these notifications.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Define port exceptions	At least Microsoft Windows XP Professional with SP2	Allows you to define a port exceptions list that Windows Firewall uses to open or block ports. Windows Firewall manages two such lists: the first is defined by Group Policy settings, and the second is defined by the actions of local computer administrators. Windows Firewall ignores the second list unless you enable the Windows Firewall: Allow local port exceptions policy setting. If you enable this policy setting, you can view and change the port exceptions list defined by Group Policy settings. To view the list, enable the policy setting and then click the Show button. To add a port, enable the policy setting, note the syntax in the shaded area below, click the Show button, click the Add button, and then type a

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				definition string that uses the syntax format. To remove a port, click its definition, and then click the Remove button. To edit a definition, remove the current definition from the list and add a new one with different parameters. The Scope parameter of a definition string specifies which set of computers can send messages intended for this program: * allows messages from all computers on the network; localsubnet allows messages only from computers on the same subnet as this computer. If you disable this policy setting, Windows Firewall blocks all ports in the exceptions list defined by Group Policy, except those opened by other policy settings. Windows Firewall ignores the list defined by local computer administrators. If you enable this policy setting and later disable it, Windows Firewall deletes the port exceptions list specified by Group Policy. If you do not configure this policy setting, other policy settings can open ports. Windows Firewall ignores entries in the port exceptions list defined by this policy setting, but uses the list defined by local computer administrators. Notes: Windows Firewall does not check the definition string for syntax errors. If you type an invalid definition string, Windows Firewall adds the invalid definition to the list without displaying a warning or error message. If you type multiple entries for the same port, and any entry disables a port, it overrides all entries that enable that port. If multiple entries for the same port have different scopes, the scopes are additive. To allow local computer administrators to open additional ports, enable this policy setting and the Windows Firewall: Allow local port exceptions policy setting.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Allow local port exceptions	At least Microsoft Windows XP Professional with SP2	Allows you to distribute a port exceptions list with entries that local computer administrators cannot override, but that they can supplement with other opened or blocked ports. If you enable this policy setting, and define a port exceptions list by using the Windows Firewall: Define port exceptions policy setting, local computer administrators can add definitions to that list. If you disable or do not configure this policy setting, local computer administrators cannot add definitions to that list.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Allow Remote Desktop exception	At least Microsoft Windows XP Professional with SP2	Allows this computer to receive the unsolicited incoming messages created by Remote Desktop requests sent from another computer. To do this, Windows Firewall opens TCP port 3389. If you enable this policy setting, you must specify whether the incoming Remote Desktop requests to this computer are permitted from computers anywhere on the network or only from computers on the local subnet. If you disable or do not configure this policy setting, Windows Firewall blocks TCP port 3389, which prevents access to Remote Desktop.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Prohibit unicast response to multicast or broadcast requests	At least Microsoft Windows XP Professional with SP2	Prevents this computer from receiving unicast responses to its outgoing multicast or broadcast messages. If you enable this policy setting, and this computer sends multicast or broadcast messages to other computers, Windows Firewall blocks the unicast responses sent by those other computers. If you disable or do not configure this policy setting, and this computer sends a multicast or broadcast message to other computers, Windows Firewall waits as long as three seconds for unicast responses from the other computers, and then blocks all later responses. Note: This policy setting has no effect if the unicast message is a response to a Dynamic Host Configuration Protocol (DHCP) multicast message sent by this computer. Windows Firewall always permits those DHCP unicast responses. However, this policy setting can interfere with the NetBIOS messages that detect name conflicts.
COMPUTER	Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile	Windows Firewall: Allow UPnP framework exception	At least Microsoft Windows XP Professional with SP2	Opens the ports required to allow this computer to receive unsolicited Plug and Play messages sent by network devices, such as routers with built-in firewalls. To do this, Windows Firewall opens TCP port 2869, and UDP port 1900. If you enable this policy setting, Windows Firewall opens these ports and allows the computer to receive Plug and Play messages. You must specify whether the incoming Plug and Play messages to this computer are permitted from devices anywhere on the network or only from devices on the local subnet. If you disable this policy setting, Windows Firewall blocks these ports, which prevents the computer from receiving Plug and Play messages. If you do not configure this policy setting, Windows Firewall does not block or open these ports. In most cases, this has the same effect as disabling this policy setting: it prevents the computer from receiving Plug and Play messages.
COMPUTER	Administrative Templates\Network\Offline Files	Subfolders always available offline	At least Microsoft Windows 2000	Makes subfolders available offline whenever their parent folder is made available offline. This setting automatically extends the make available offline setting to all new and existing subfolders of a folder. Users do not have the option of excluding subfolders. If you enable this setting, when you make a folder available offline, all folders within that folder are also made available offline. Also, new folders that you create within a folder that is available offline are made available offline when the parent folder is synchronized. If you disable this setting or do not configure it, the system asks users whether they want subfolders to be made available offline when they make a parent folder available offline.
COMPUTER	Administrative	Administratively	At least Microsoft	Lists network files and folders that are always available for offline use.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Templates\Network\Offline Files	assigned offline files	Windows 2000	This setting makes the specified files and folders available offline to users of the computer. To assign a folder, click Show, and then click Add. In the Type the name of the item to be added box, type the fully qualified UNC path to the file or folder. Leave the Enter the value of the item to be added field blank. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the settings will be combined and all specified files will be available for offline use.
COMPUTER	Administrative Templates\Network\Offline Files	Non-default server disconnect actions	At least Microsoft Windows 2000	Determines how computers respond when they are disconnected from particular offline file servers. This setting overrides the default response, a user-specified response, and the response specified in the Action on server disconnect setting. To use this setting, click Show, and then click Add. In the Type the name of the item to be added box, type the server's computer name. Then, in the Type the value of the item to be added box, type 0 if users can work offline when they are disconnected from this server, or type 1 if they cannot. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured for a particular server, the setting in Computer Configuration takes precedence over the setting in User Configuration. Both Computer and User configuration take precedence over a user's setting. This setting does not prevent users from setting custom actions through the Offline Files tab. However, users are unable to change any custom actions established via this setting. Tip: To configure this setting without establishing a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click Advanced. This setting corresponds to the settings in the Exception list section.
COMPUTER	Administrative Templates\Network\Offline Files	Default cache size	At least Microsoft Windows 2000	Limits the percentage of the computer's disk space that can be used to store automatically cached offline files. This setting also disables the Amount of disk space to use for temporary offline files option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it. Automatic caching can be set on any network share. When a user opens a file on the share, the system automatically stores a copy of the file on the user's computer. This setting does not limit the disk space available for files that user's make available offline manually. If you enable this setting, you can specify an automatic-cache disk space limit. If you disable this setting, the system limits the space that automatically cached files occupy to 10 percent of the space on the system drive. If you do not configure this setting, disk space for automatically cached files is limited to 10 percent of the system drive by

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				default, but users can change it. Tip: To change the amount of disk space used for automatic caching without specifying a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then use the slider bar associated with the Amount of disk space to use for temporary offline files option.
COMPUTER	Administrative Templates\Network\Offline Files	Allow or Disallow use of the Offline Files feature	At least Microsoft Windows 2000	Determines whether the Offline Files feature is enabled. This setting also disables the Enable Offline Files option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it. Offline Files saves a copy of network files on the user's computer for use when the computer is not connected to the network. If you enable this setting, Offline Files is enabled and users cannot disable it. If you disable this setting, Offline Files is disabled and users cannot enable it. By default, Offline Files is enabled on Windows 2000 Professional and Windows XP Professional and is disabled on Windows 2000 Server and also Windows Server 2003 family. Tip: To enable Offline Files without specifying a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click Enable Offline Files. Note: To make changes to this setting effective, you must restart Windows.
COMPUTER	Administrative Templates\Network\Offline Files	Encrypt the Offline Files cache	At least Microsoft Windows 2000 Service Pack 5, Microsoft Windows XP Professional Service Pack 2 or Microsoft Windows Server 2003 family Service Pack 1	This setting determines whether offline files are encrypted. Offline files reside on a user's hard drive, not the network, and they are stored in a local cache on the computer. Encrypting this cache enhances security on a local computer. If the cache on the local computer is not encrypted, any encrypted files cached from the network will not be encrypted on the local computer. This may pose a security risk in some environments. If you enable this setting, all files in the Offline Files cache are encrypted. This includes existing files as well as files added later. The cached copy on the local computer is affected, but the associated network copy is not. The user cannot unencrypt Offline Files through the user interface. If you disable this setting, all files in the Offline Files cache are unencrypted. This includes existing files as well as files added later. The cached copy on the local computer is affected, but the associated network copy is not. The user cannot encrypt Offline Files through the user interface. If you do not configure this setting, encryption of the Offline Files cache is controlled by the user through the user interface. The current cache state is retained, and if the cache is only partially encrypted, the operation completes so that it is fully encrypted. The cache does not return to the unencrypted state. The user must be an administrator on the local computer to encrypt or decrypt the Offline Files

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				cache. Note: By default, this cache is protected on NTFS partitions by ACLs.
COMPUTER	Administrative Templates\Network\Offline Files	Event logging level	At least Microsoft Windows 2000	Determines which events the Offline Files feature records in the event log. Offline Files records events in the Application log in Event Viewer when it detects errors. By default, Offline Files records an event only when the offline files storage cache is corrupted. However, you can use this setting to specify additional events you want Offline Files to record. To use this setting, in the Enter box, select the number corresponding to the events you want the system to log. The levels are cumulative; that is, each level includes the events in all preceding levels. 0 records an error when the offline storage cache is corrupted. 1 also records an event when the server hosting the offline file is disconnected from the network. 2 also records events when the local computer is connected and disconnected from the network. 3 also records an event when the server hosting the offline file is reconnected to the network. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
COMPUTER	Administrative Templates\Network\Offline Files	Files not cached	At least Microsoft Windows 2000	Lists types of files that cannot be used offline. This setting lets you exclude certain types of files from automatic and manual caching for offline use. The system does not cache files of the type specified in this setting even when they reside on a network share configured for automatic caching. Also, if users try to make a file of this type available offline, the operation will fail and the following message will be displayed in the Synchronization Manager progress dialog box: Files of this type cannot be made available offline. This setting is designed to protect files that cannot be separated, such as database components. To use this setting, type the file name extension in the Extensions box. To type more than one extension, separate the extensions with a semicolon (;). Note: To make changes to this setting effective, you must log off and log on again.
COMPUTER	Administrative Templates\Network\Offline Files	Action on server disconnect	At least Microsoft Windows 2000	Determines whether network files remain available if the computer is suddenly disconnected from the server hosting the files. This setting also disables the When a network connection is lost option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it. If you enable this setting, you can use the Action box to specify how computers in the group respond. -- Work offline indicates that the computer can use local copies of network files while the server is

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				inaccessible. -- Never go offline indicates that network files are not available while the server is inaccessible. If you disable this setting or select the Work offline option, users can work offline if disconnected. If you do not configure this setting, users can work offline by default, but they can change this option. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To configure this setting without establishing a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, click Advanced, and then select an option in the When a network connection is lost section. Also, see the Non-default server disconnect actions setting.
COMPUTER	Administrative Templates\Network\Offline Files	Prevent use of Offline Files folder	At least Microsoft Windows 2000	Disables the Offline Files folder. This setting disables the View Files button on the Offline Files tab. As a result, users cannot use the Offline Files folder to view or open copies of network files stored on their computer. Also, they cannot use the folder to view characteristics of offline files, such as their server status, type, or location. This setting does not prevent users from working offline or from saving local copies of files available offline. Also, it does not prevent them from using other programs, such as Windows Explorer, to view their offline files. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To view the Offline Files Folder, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click View Files.
COMPUTER	Administrative Templates\Network\Offline Files	Prohibit user configuration of Offline Files	At least Microsoft Windows 2000	Prevents users from enabling, disabling, or changing the configuration of Offline Files. This setting removes the Offline Files tab from the Folder Options dialog box. It also removes the Settings item from the Offline Files context menu and disables the Settings button on the Offline Files Status dialog box. As a result, users cannot view or change the options on the Offline Files tab or Offline Files dialog box. This is a comprehensive setting that locks down the configuration you establish by using other settings in this folder. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: This setting provides a quick method for locking down the default settings for Offline Files. To accept the defaults, just enable this setting. You do not have to disable any

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				other settings in this folder.
COMPUTER	Administrative Templates\Network\Offline Files	Remove 'Make Available Offline'	At least Microsoft Windows 2000	Prevents users from making network files and folders available offline. This setting removes the Make Available Offline option from the File menu and from all context menus in Windows Explorer. As a result, users cannot designate files to be saved on their computer for offline use. However, this setting does not prevent the system from saving local copies of files that reside on network shares designated for automatic caching. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
COMPUTER	Administrative Templates\Network\Offline Files	Prohibit 'Make Available Offline' for these file and folders	At least Microsoft Windows XP Professional or Windows Server 2003 family	Prohibits specific network files and folders from being made available for offline use. To prohibit the Make Available Offline option for specific files or folders, enable this setting, click Show, and then click Add. In the Type the name of the item to be added box, type the fully qualified UNC path to the file or folder. Leave the Enter the value of the item to be added field blank. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the settings are combined, and all specified files will not be available for offline use. Note: This setting does not prevent files from being automatically cached if the network share is configured for Automatic Caching. It only affects the availability of the Make Available Offline menu option in the user interface. Note: If the Disable Make Available Offline setting is enabled, this setting has no effect.
COMPUTER	Administrative Templates\Network\Offline Files	Turn off reminder balloons	At least Microsoft Windows 2000	Hides or displays reminder balloons, and prevents users from changing the setting. Reminder balloons appear above the Offline Files icon in the notification area to notify users when they have lost the connection to a networked file and are working on a local copy of the file. Users can then decide how to proceed. If you enable this setting, the system hides the reminder balloons, and prevents users from displaying them. If you disable the setting, the system displays the reminder balloons and prevents users from hiding them. If this setting is not configured, reminder balloons are displayed by default when you enable offline files, but users can change the setting. To prevent users from changing the setting while a setting is in effect, the system disables the Enable reminders option on the Offline Files tab This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				over the setting in User Configuration. Tip: To display or hide reminder balloons without establishing a setting, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This setting corresponds to the Enable reminders check box.
COMPUTER	Administrative Templates\Network\Offline Files	At logoff, delete local copy of user's offline files	At least Microsoft Windows 2000	Deletes local copies of the user's offline files when the user logs off. This setting specifies that automatically and manually cached offline files are retained only while the user is logged on to the computer. When the user logs off, the system deletes all local copies of offline files. If you disable this setting or do not configure it, automatically and manually cached copies are retained on the user's computer for later offline use. Caution: Files are not synchronized before they are deleted. Any changes to local files since the last synchronization are lost.
COMPUTER	Administrative Templates\Network\Offline Files	Reminder balloon frequency	At least Microsoft Windows 2000	Determines how often reminder balloon updates appear. If you enable this setting, you can select how often reminder balloons updates apppear and also prevent users from changing this setting. Reminder balloons appear when the user's connection to a network file is lost or reconnected, and they are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this setting to change the update interval. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To set reminder balloon frequency without establishing a setting, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This setting corresponds to the Display reminder balloons every ... minutes option.
COMPUTER	Administrative Templates\Network\Offline Files	Initial reminder balloon lifetime	At least Microsoft Windows 2000	Determines how long the first reminder balloon for a network status change is displayed. Reminder balloons appear when the user's connection to a network file is lost or reconnected, and they are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this setting to change the duration of the first reminder. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Network\Offline Files	Reminder balloon lifetime	At least Microsoft Windows 2000	Determines how long updated reminder balloons are displayed. Reminder balloons appear when the user's connection to a network file is lost or reconnected, and they are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this setting to change the duration of the update reminder. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
COMPUTER	Administrative Templates\Network\Offline Files	Configure Slow link speed	At least Microsoft Windows XP Professional or Windows Server 2003 family	Configures the threshold value at which Offline Files considers a network connection to be slow. Any network speed below this value is considered to be slow. When a connection is considered slow, Offline Files automatically adjust its behavior to avoid excessive synchronization traffic and will not automatically reconnect to a server when the presence of a server is detected. If you enable this setting, you can configure the threshold value that will be used to determine a slow network connection. If this setting is disabled or not configured, the default threshold value of 64,000 bps is used to determine if a network connection is considered to be slow. Note: Use the following formula when entering the slow link value: [bps / 100]. For example, if you want to set a threshold value of 128,000 bps, enter a value of 1280.
COMPUTER	Administrative Templates\Network\Offline Files	Synchronize all offline files before logging off	At least Microsoft Windows 2000	Determines whether offline files are fully synchronized when users log off. This setting also disables the Synchronize all offline files before logging off option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it. If you enable this setting, offline files are fully synchronized. Full synchronization ensures that offline files are complete and current. If you disable this setting, the system only performs a quick synchronization. Quick synchronization ensures that files are complete, but does not ensure that they are current. If you do not configure this setting, the system performs a quick synchronization by default, but users can change this option. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To change the synchronization method without changing a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then select the Synchronize all offline files before logging off option.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Network\Offline Files	Synchronize all offline files when logging on	At least Microsoft Windows 2000	Determines whether offline files are fully synchronized when users log on. This setting also disables the Synchronize all offline files before logging on option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it. If you enable this setting, offline files are fully synchronized at logon. Full synchronization ensures that offline files are complete and current. Enabling this setting automatically enables logon synchronization in Synchronization Manager. If this setting is disabled and Synchronization Manager is configured for logon synchronization, the system performs only a quick synchronization. Quick synchronization ensures that files are complete but does not ensure that they are current. If you do not configure this setting and Synchronization Manager is configured for logon synchronization, the system performs a quick synchronization by default, but users can change this option. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To change the synchronization method without setting a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then select the Synchronize all offline files before logging on option.
COMPUTER	Administrative Templates\Network\Offline Files	Synchronize offline files before suspend	At least Microsoft Windows 2000	Determines whether offline files are synchonized before a computer is suspended. If you enable this setting, offline files will be synchronized whenever the computer is suspended. Setting the synchronization action to Quick ensures only that all files in the cache are complete. Setting the synchronization action to Full ensures that all cached files and folders are up to date with the most current version. If you disable or do not configuring this setting, a synchronization will not occur when the computer is suspended. Note: If the computer is suspended by closing the display on a portable computer, a synchronization is not performed. If multiple users are logged on to the computer at the time the computer is suspended, a synchronization is not performed.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler	Limit outstanding packets	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the maximum number of outstanding packets permitted on the system. When the number of outstanding packets reaches this limit, the Packet Scheduler postpones all submissions to network adapters until the number falls below this limit. Outstanding packets are packets that the Packet Scheduler has submitted to a network adapter for transmission, but which have not yet been sent. If you enable this setting, you can limit the number of outstanding packets. If you disable this setting or do not configure it, then the setting has no effect on the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				system. Important: If the maximum number of outstanding packets is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler	Limit reservable bandwidth	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines the percentage of connection bandwidth that the system can reserve. This value limits the combined bandwidth reservations of all programs running on the system. By default, the Packet Scheduler limits the system to 20 percent of the bandwidth of a connection, but you can use this setting to override the default. If you enable this setting, you can use the Bandwidth limit box to adjust the amount of bandwidth the system can reserve. If you disable this setting or do not configure it, the system uses the default value of 20 percent of the connection. Important: If a bandwidth limit is set for a particular network adapter in the registry, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler	Set timer resolution	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines the smallest unit of time that the Packet Scheduler uses when scheduling packets for transmission. The Packet Scheduler cannot schedule packets for transmission more frequently than permitted by the value of this entry. If you enable this setting, you can override the default timer resolution established for the system, usually units of 10 microseconds. If you disable this setting or do not configure it, the setting has no effect on the system. Important: If a timer resolution is specified in the registry for a particular network adapter, then this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of conforming packets	Best effort service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Best Effort service type (ServiceTypeBestEffort). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that conform to the flow specification. If you enable this setting, you can change the default DSCP value associated with the Best Effort service type. If you disable this setting, the system uses the default DSCP value of 0. Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of conforming packets	Controlled load service type	At least Microsoft Windows XP Professional or Windows Server	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Controlled Load service type (ServiceTypeControlledLoad). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that conform to the flow specification. If you

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			2003 family	enable this setting, you can change the default DSCP value associated with the Controlled Load service type. If you disable this setting, the system uses the default DSCP value of 24 (0x18). Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of conforming packets	Guaranteed service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Guaranteed service type (ServiceTypeGuaranteed). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that conform to the flow specification. If you enable this setting, you can change the default DSCP value associated with the Guaranteed service type. If you disable this setting, the system uses the default DSCP value of 40 (0x28). Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of conforming packets	Network control service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Network Control service type (ServiceTypeNetworkControl). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that conform to the flow specification. If you enable this setting, you can change the default DSCP value associated with the Network Control service type. If you disable this setting, the system uses the default DSCP value of 48 (0x30). Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of conforming packets	Qualitative service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Qualitative service type (ServiceTypeQualitative). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that conform to the flow specification. If you enable this setting, you can change the default DSCP value associated with the Qualitative service type. If you disable this setting, the system uses the default DSCP value of 0. Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of non-conforming packets	Best effort service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Best Effort service type (ServiceTypeBestEffort). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that do not conform to the flow specification. If you enable this setting, you can change the default DSCP value associated with the Best Effort service type. If you disable this setting, the system uses the default DSCP value of 0. Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of non-conforming packets	Controlled load service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Controlled Load service type (ServiceTypeControlledLoad). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that do not conform to the flow specification. If you enable this setting, you can change the default DSCP value associated with the Controlled Load service type. If you disable this setting, the system uses the default DSCP value of 0. Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of non-conforming packets	Guaranteed service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Guaranteed service type (ServiceTypeGuaranteed). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that do not conform to the flow specification. If you enable this setting, you can change the default DSCP value associated with the Guaranteed service type. If you disable this setting, the system uses the default DSCP value of 0. Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of non-conforming packets	Network control service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Network Control service type (ServiceTypeNetworkControl). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that do not conform to the flow specification. If

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				you enable this setting, you can change the default DSCP value associated with the Network Control service type. If you disable this setting, the system uses the default DSCP value of 0. Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\DSCP value of non-conforming packets	Qualitative service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate Layer-3 Differentiated Services Code Point (DSCP) value for packets with the Qualitative service type (ServiceTypeQualitative). The Packet Scheduler inserts the corresponding DSCP value in the IP header of the packets. This setting applies only to packets that do not conform to the flow specification. If you enable this setting, you can change the default DSCP value associated with the Qualitative service type. If you disable this setting, the system uses the default DSCP value of 0. Important: If the DSCP value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\Layer-2 priority value	Best effort service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate link layer (Layer-2) priority value for packets with the Best Effort service type (ServiceTypeBestEffort). The Packet Scheduler inserts the corresponding priority value in the Layer-2 header of the packets. If you enable this setting, you can change the default priority value associated with the Best Effort service type. If you disable this setting, the system uses the default priority value of 0. Important: If the Layer-2 priority value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\Layer-2 priority value	Controlled load service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate link layer (Layer-2) priority value for packets with the Controlled Load service type (ServiceTypeControlledLoad). The Packet Scheduler inserts the corresponding priority value in the Layer-2 header of the packets. If you enable this setting, you can change the default priority value associated with the Controlled Load service type. If you disable this setting, the system uses the default priority value of 4. Important: If the Layer-2 priority value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet	Guaranteed service type	At least Microsoft Windows XP Professional or	Specifies an alternate link layer (Layer-2) priority value for packets with the Guaranteed service type (ServiceTypeGuaranteed). The Packet Scheduler inserts the corresponding priority value in the Layer-2 header

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Scheduler\Layer-2 priority value		Windows Server 2003 family	of the packets. If you enable this setting, you can change the default priority value associated with the Guaranteed service type. If you disable this setting, the system uses the default priority value of 5. Important: If the Layer-2 priority value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\Layer-2 priority value	Network control service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate link layer (Layer-2) priority value for packets with the Network Control service type (ServiceTypeNetworkControl). The Packet Scheduler inserts the corresponding priority value in the Layer-2 header of the packets. If you enable this setting, you can change the default priority value associated with the Network Control service type. If you disable this setting, the system uses the default priority value of 7. Important: If the Layer-2 priority value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\Layer-2 priority value	Non-conforming packets	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate link layer (Layer-2) priority value for packets that do not conform to the flow specification. The Packet Scheduler inserts the corresponding priority value in the Layer-2 header of the packets. If you enable this setting, you can change the default priority value associated with nonconforming packets. If you disable this setting, the system uses the default priority value of 1. Important: If the Layer-2 priority value for nonconforming packets is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\QoS Packet Scheduler\Layer-2 priority value	Qualitative service type	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate link layer (Layer-2) priority value for packets with the Qualitative service type (ServiceTypeQualitative). The Packet Scheduler inserts the corresponding priority value in the Layer-2 header of the packets. If you enable this setting, you can change the default priority value associated with the Qualitative service type. If you disable this setting, the system uses the default priority value of 0. Important: If the Layer-2 priority value for this service type is specified in the registry for a particular network adapter, this setting is ignored when configuring that network adapter.
COMPUTER	Administrative Templates\Network\SNMP	Communities	At least Microsoft Windows XP Professional or Windows Server	Configures a list of the communities defined to the Simple Network Management Protocol (SNMP) service. SNMP is a protocol designed to give a user the capability to remotely manage a computer network, by polling and setting terminal values and monitoring network events. A valid community is a community recognized by the SNMP service, while

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			2003 family	a community is a group of hosts (servers, workstations, hubs, and routers) that are administered together by SNMP. The SNMP service is a managed network node that receives SNMP packets from the network. If you enable this setting, the SNMP agent only accepts requests from management systems within the communities it recognizes, and only SNMP Read operation is allowed for the community. If you disable or do not configure this setting, the SNMP service takes the Valid Communities configured on the local computer instead. Best Practice: For security purposes, it is recommended to restrict the HKLM\SOFTWARE\Policies\SNMP\Parameters\ValidCommunities key to allow only the local admin group full control. Note: It is good practice to use a cryptic community name. Note: This setting has no effect if the SNMP agent is not installed on the client computer. Also, see the other two SNMP settings: Permitted Managers and Trap Configuration.
COMPUTER	Administrative Templates\Network\SNMP	Permitted Managers	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting determines the permitted list of hosts that can submit a query to the Simple Network Management (SNMP) agent running on the client computer. Simple Network Management Protocol is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events. The manager is located on the host computer on the network. The manager's role is to poll the agents for certain requested information. If you enable this setting, the SNMP agent only accepts requests from the list of Permitted Managers that you configure using this setting. If you disable or do not configure this setting, SNMP service takes the Permitted Managers configured on the local computer instead. Best Practice: For security purposes, it is recommended to restrict the HKLM\SOFTWARE\Policies\SNMP\Parameters\PermittedManagers key to allow only the local admin group full control. Note: This setting has no effect if the SNMP agent is not installed on the client computer. Also, see the other two SNMP settings: Trap Configuration and Community Name.
COMPUTER	Administrative Templates\Network\SNMP	Traps for public community	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting allows Trap configuration for the Simple Network Management Protocol (SNMP) agent. Simple Network Management Protocol is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events. This setting allows you to configure the name of the hosts that receive trap messages for the community sent by the SNMP service. A trap message is an alert or significant event that allows the SNMP agent to notify management systems asynchronously.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				If you enable this setting, the SNMP service sends trap messages to the hosts within the public community. If you disable or do not configure this setting, the SNMP service takes the Trap Configuration configured on the local computer instead. Note: This setting has no effect if the SNMP agent is not installed on the client computer. Also, see the other two SNMP settings: Permitted Managers and Community Name.
COMPUTER	Administrative Templates\Network\System policies update	Remote update		
COMPUTER	Administrative Templates\Printers	Web-based printing	Windows 2000 or later, running IIS. Not supported on Windows Server 2003	Determines whether Internet printing is activated on this server. Internet printing lets you display printers on Web pages so the printers can be viewed, managed, and used across the Internet or an intranet. Internet printing is and extension of the Internet Information Server. IIS must be installed and the printing support must be enabled in order to use Internet Printing as well as this policy. Note: This setting affects the server side of Internet printing only. It does not prevent the print client on the computer from printing across the Internet. Also, see the Custom support URL in the Printers folder's left pane setting in this folder and the Browse a common web site to find printers setting in User Configuration\Administrative Templates\Control Panel\Printers.
COMPUTER	Administrative Templates\Printers	Automatically publish new printers in Active Directory	At least Microsoft Windows 2000	Determines whether the Add Printer Wizard automatically publishes the computer's shared printers in Active Directory. If you enable this setting or do not configure it, the Add Printer Wizard automatically publishes all shared printers. If you disable this setting, the Add Printer Wizard does not automatically publish printers. However, you can publish shared printers manually. The default behavior is to automatically publish shared printers in Active Directory. Note: This setting is ignored if the Allow printers to be published setting is disabled.
COMPUTER	Administrative Templates\Printers	Custom support URL in the Printers folder's left pane	At least Microsoft Windows 2000	Adds a customized Web page link to the Printers folder. By default, the Printers folder includes a link to the Microsoft Support Web page called Get help with printing. It can also include a link to a Web page supplied by the vendor of the currently selected printer. You can use this setting to replace the Get help with printing default link with a link to a Web page customized for your enterprise. If you disable this setting or do not configure it, or if you do not enter an alternate Internet address, the default link will appear in the Printers folder. Note: Web pages links only appear in the Printers folder when Web view is enabled. If Web view is disabled, the setting has no effect. (To enable Web view, open the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Printers folder, and, on the Tools menu, click Folder Options, click the General tab, and then click Enable Web content in folders.) Also, see the Web-based printing setting in this setting folder and the Browse a common web site to find printers setting in User Configuration\Administrative Templates\Control Panel\Printers. Web view is affected by the Turn on Classic Shell and Remove the Folder Options menu item from the Tools menu settings in User Configuration\Administrative Templates\Windows Components\Windows Explorer, and by the Enable Active Desktop setting in User Configuration\Administrative Templates\Desktop\Active Desktop.
COMPUTER	Administrative Templates\Printers	Allow pruning of published printers	At least Microsoft Windows 2000	Determines whether the domain controller can prune (delete from Active Directory) the printers published by this computer. By default, the pruning service on the domain controller prunes printer objects from Active Directory if the computer that published them does not respond to contact requests. When the computer that published the printers restarts, it republishes any deleted printer objects. If you enable this setting or do not configure it, the domain controller prunes this computer's printers when the computer does not respond. If you disable this setting, the domain controller does not prune this computer's printers. This setting is designed to prevent printers from being pruned when the computer is temporarily disconnected from the network. Note: You can use the Directory Pruning Interval and Directory Pruning Retry settings to adjust the contact interval and number of contact attempts.
COMPUTER	Administrative Templates\Printers	Disallow installation of printers using kernel-mode drivers	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether printers using kernel-mode drivers may be installed on the local computer. Kernel-mode drivers have access to system-wide memory, and therefore poorly-written kernel-mode drivers can cause stop errors. If you disable this setting, or do not configure it, then printers using a kernel-mode drivers may be installed on the local computer running Windows XP Home Edition and Windows XP Professional. If you do not configure this setting on Windows Server 2003 family products, the installation of kernel-mode printer drivers will be blocked. If you enable this setting, installation of a printer using a kernel-mode driver will not be allowed. Note: By applying this policy, existing kernel-mode drivers will be disabled upon installation of service packs or reinstallation of the Windows XP operating system. This policy does not affect 64-bit Itanium computers, because kernel-mode drivers cannot be installed on Intel 64-bit Itanium computers.
COMPUTER	Administrative Templates\Printers	Computer location	At least Microsoft	Specifies the default location criteria used when searching for printers.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			Windows 2000	This setting is a component of the Location Tracking feature of Windows printers. To use this setting, enable Location Tracking by enabling the Pre-populate printer search location text setting. When Location Tracking is enabled, the system uses the specified location as a criterion when users search for printers. The value you type here overrides the actual location of the computer conducting the search. Type the location of the user's computer. When users search for printers, the system uses the specified location (and other search criteria) to find a printer nearby. You can also use this setting to direct users to a particular printer or group of printers that you want them to use. If you disable this setting or do not configure it, and the user does not type a location as a search criterion, the system searches for a nearby printer based on the IP address and subnet mask of the user's computer.
COMPUTER	Administrative Templates\Printers	Pre-populate printer search location text	At least Microsoft Windows 2000	Enables the physical Location Tracking support feature of Windows printers. Location tracking lets you design a location scheme for your enterprise and assign computers and printers to locations in your scheme. Location tracking overrides the standard method of locating and associating users and printers, which uses the IP address and subnet mask of a computer to estimate its physical location and proximity to other computers. If you enable Location Tracking, a Browse button appears beside the Location field in the Find Printers dialog box. (To go to the Browse button, click Start, click Search, and click For printers.) The Browse button also appears on the General tab of the Properties dialog box for a printer. It lets users browse for printers by location without their having to know the precise location (or location naming scheme). Also, if you enable the Computer location setting, the default location you type appears in the Location field. If you disable this setting or do not configure it, Location Tracking is disabled. Printer proximity is estimated based on IP address and subnet mask.
COMPUTER	Administrative Templates\Printers	Printer browsing	At least Microsoft Windows 2000	Announces the presence of shared printers to print browse master servers for the domain. On domains with Active Directory, shared printer resources are available in Active Directory and are not announced. If you enable this setting, the print spooler announces shared printers to the print browse master servers. As a result, shared printers appear in the domain list in the Browse for Printer dialog box in the Add Printer Wizard. If you disable this setting, shared printers are not announced to print browse master servers, even if Active Directory is not available. If you do not configure this setting, shared printers are announced to browse master servers only when Active Directory is not available. Note:

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				A client license is used each time a client computer announces a printer to a print browse master on the domain.
COMPUTER	Administrative Templates\Printers	Prune printers that are not automatically republished	At least Microsoft Windows 2000	Determines whether the system prunes (deletes from Active Directory) printers that are not automatically republished. This setting applies to printers running operating systems other than Windows 2000 and to Windows 2000 printers published outside their forest. The Windows pruning service prunes printer objects from Active Directory when the computer that published them does not respond to contact requests. Computers running Windows 2000 Professional detect and republish deleted printer objects when they rejoin the network. However, because non-Windows 2000 computers and computers in other domains cannot republish printers in Active Directory automatically, by default the system never prunes their printer objects. You can enable this setting to change the default behavior. To use this setting, select one of the following options from the Prune non-republishing printers box: -- Never specifies that printer objects that are not automatically republished are never pruned. Never is the default. -- Only if Print Server is found prunes printer objects that are not automatically republished only when the print server responds, but the printer is unavailable. -- Whenever printer is not found prunes printer objects that are not automatically republished whenever the host computer does not respond, just as it does with Windows 2000 printers. Note: This setting applies to printers published by using Active Directory Users and Computers or Pubprn.vbs. It does not apply to printers published by using Printers in Control Panel. Tip: If you disable automatic pruning, remember to delete printer objects manually whenever you remove a printer or print server.
COMPUTER	Administrative Templates\Printers	Directory pruning interval	At least Microsoft Windows 2000	Specifies how often the pruning service on a domain controller contacts computers to verify that their printers are operational. The pruning service periodically contacts computers that have published printers. If a computer does not respond to the contact message (optionally, after repeated attempts), the pruning service prunes (deletes from Active Directory) printer objects the computer has published. By default, the pruning service contacts computers every eight hours and allows two repeated contact attempts before deleting printers from Active Directory. If you enable this setting, you can change the interval between contact attempts. If you do not configure or disable this setting the default values will be used. Note: This setting is used only on domain controllers.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Printers	Directory pruning priority	At least Microsoft Windows 2000	Sets the priority of the pruning thread. The pruning thread, which runs only on domain controllers, deletes printer objects from Active Directory if the printer that published the object does not respond to contact attempts. This process keeps printer information in Active Directory current. The thread priority influences the order in which the thread receives processor time and determines how likely it is to be preempted by higher priority threads. By default, the pruning thread runs at normal priority. However, you can adjust the priority to improve the performance of this service. Note: This setting is used only on domain controllers.
COMPUTER	Administrative Templates\Printers	Directory pruning retry	At least Microsoft Windows 2000	Specifies how many times the pruning service on a domain controller repeats its attempt to contact a computer before pruning the computer's printers. The pruning service periodically contacts computers that have published printers to verify that the printers are still available for use. If a computer does not respond to the contact message, the message is repeated for the specified number of times. If the computer still fails to respond, then the pruning service prunes (deletes from Active Directory) printer objects the computer has published. By default, the pruning service contacts computers every eight hours and allows two retries before deleting printers from Active Directory. You can use this setting to change the number of retries. If you enable this setting, you can change the interval between attempts. If you do not configure or disable this setting, the default values are used. Note: This setting is used only on domain controllers.
COMPUTER	Administrative Templates\Printers	Log directory pruning retry events	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether or not to log events when the pruning service on a domain controller attempts to contact a computer before pruning the computer's printers. The pruning service periodically contacts computers that have published printers to verify that the printers are still available for use. If a computer does not respond to the contact attempt, the attempt is retried a specified number of times, at a specified interval. The Directory pruning retry setting determines the number of times the attempt is retried; the default value is two retries. The Directory Pruning Interval setting determines the time interval between retries; the default value is every eight hours. If the computer has not responded by the last contact attempt, its printers are pruned from the directory. If the Log directory pruning retry events setting is enabled, the contact events are recorded in the event log. If this setting is not configured or is disabled, the contact events are not recorded in the event log. Note: This setting does not affect the logging of pruning events; the actual pruning of a printer is always logged. Note: This setting is used only on domain

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				controllers.
COMPUTER	Administrative Templates\Printers	Allow printers to be published	At least Microsoft Windows 2000	Determines whether the computer's shared printers can be published in Active Directory. If you enable this setting or do not configure it, users can use the List in directory option in the Printer's Properties' Sharing tab to publish shared printers in Active Directory. If you disable this setting, this computer's shared printers cannot be published in Active Directory, and the List in directory option is not available. Note: This settings takes priority over the setting Automatically publish new printers in the Active Directory.
COMPUTER	Administrative Templates\Printers	Allow Print Spooler to accept client connections	At least Microsoft Windows Server 2003	This policy controls whether the print spooler will accept client connections. When the policy is unconfigured, the spooler will not accept client connections until a user shares out a local printer or opens the print queue on a printer connection, at which point spooler will begin accepting client connections automatically. When the policy is enabled, the spooler will always accept client connections. When the policy is disabled, the spooler will not accept client connections nor allow users to share printers. All printers currently shared will continue to be shared. The spooler must be restarted for changes to this policy to take effect.
COMPUTER	Administrative Templates\Printers	Check published state	At least Microsoft Windows 2000	Directs the system to periodically verify that the printers published by this computer still appear in Active Directory. This setting also specifies how often the system repeats the verification. By default, the system only verifies published printers at startup. This setting allows for periodic verification while the computer is operating. To enable this additional verification, enable this setting, and then select a verification interval. To disable verification, disable this setting, or enable this setting and select Never for the verification interval.
COMPUTER	Administrative Templates\Related Sites and Errors	Related Sites		
COMPUTER	Administrative Templates\System	Download missing COM components	At least Microsoft Windows 2000	Directs the system to search Active Directory for missing Component Object Model (COM) components that a program requires. Many Windows programs, such as the MMC snap-ins, use the interfaces provided by the COM. These programs cannot perform all of their functions unless Windows has internally registered the required components. If you enable this setting and a component registration is missing, the system searches for it in Active Directory and if it is found, downloads it. The resulting searches might make some programs start or run slowly. If you disable this setting or do not configure it, the program

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				continues without the registration. As a result, the program might not perform all of its functions, or it might stop. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
COMPUTER	Administrative Templates\System	Turn off Autoplay	At least Microsoft Windows 2000	Turns off the Autoplay feature. Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately. By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives. If you enable this setting, you can also disable Autoplay on CD-ROM drives or disable Autoplay on all drives. This setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default. Note: This setting appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration. Note: This setting does not prevent Autoplay for music CDs.
COMPUTER	Administrative Templates\System	Remove Boot / Shutdown / Logon / Logoff status messages	At least Microsoft Windows 2000	Suppresses system status messages. If you enable this setting, the system does not display a message reminding users to wait while their system starts or shuts down, or while users log on or off.
COMPUTER	Administrative Templates\System	Allow Distributed Link Tracking clients to use domain resources	At least Microsoft Windows Server 2003	Specifies that Distributed Link Tracking clients in this domain may use the Distributed LInk Tracking (DLT) server, which runs on domain controllers. The DLT client enables programs to track linked files that are moved within an NTFS volume, to another NTFS volume on the same computer, or to an NTFS volume on another computer. The DLT client can more reliably track links when allowed to use the DLT server. This policy should not be set unless the DLT server is running on all domain controllers in the domain.
COMPUTER	Administrative Templates\System	Do not display Manage Your Server page at logon	At least Microsoft Windows Server 2003	Specifies whether to turn off the automatic display of the Manage Your Server page. If the status is set to Enabled, the Manage Your Server page does not appear each time an administrator logs on to the server. If the status is set to Disabled or Not Configured, the Manage Your Server page does appear each time an administrator logs on to the server. However, if the administrator has selected the "Don't display this page at logon" check box at the bottom of the Manage Your Server page, the page will not appear. Regardless of this setting's status, the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Manage Your Server page is still available from the Start menu.
COMPUTER	Administrative Templates\System	Do not turn off system power after a Windows system shutdown has occurred.	At least Microsoft Windows XP Professional with SP1 or Windows Server 2003 family	This setting allows you to configure whether power is automatically turned off when Windows shutdown completes. This setting does not effect Windows shutdown behavior when shutdown is manually selected using the Start menu or Task Manager user interfaces. Applications such as UPS software may rely on Windows shutdown behavior. This setting is only applicable when Windows shutdown is initiated by software programs invoking the Windows programming interfaces ExitWindowsEx() or InitiateSystemShutdown(). If you enable this setting, the computer system will be safely shutdown, and remain in a powered state, ready for power to be safely removed. If you disable or do not configure this setting, the computer system will safely shutdown to a fully powered-off state.
COMPUTER	Administrative Templates\System	Turn off Windows Update device driver search prompt	At least Microsoft Windows XP Professional with SP2	Specifies whether the administrator will be prompted about going to Windows Update to search for device drivers using the Internet. Note: This setting only has effect if Turn off Windows Update device driver searching in Administrative Templates/System/Internet Communication Management/Internet Communication settings is disabled or not configured. If this setting is enabled, administrators will not be prompted to search Windows Update. If this setting is disabled or not configured and Turn off Windows Update device driver searching is disabled or not configured, the administrator will be prompted for consent before going to Windows Update to search for device drivers.
COMPUTER	Administrative Templates\System	Enable Persistent Time Stamp	At least Microsoft Windows Server 2003	The Persistent System Timestamp allows the system to detect the time of unexpected shutdowns by writing the current time to disk on a schedule controlled by the Timestamp Interval. If you enable this setting, the Persistent System Timestamp will be refreshed according to the Timestamp Interval. If you disable this setting, the Persistent System Timestamp will be turned off and the timing of unexpected shutdowns will not be detected. If you do not configure this setting, the default behavior will occur. Note: By default, the Persistent System Timestamp is refreshed every 60 seconds on the Windows Server 2003 family. This feature may interfere with power configuration settings that turn off hard disks after a period of inactivity. These power settings may be accessed in the Power Options Control Panel.
COMPUTER	Administrative Templates\System	Restrict potentially unsafe HTML Help functions to specified	At least Internet Explorer 6 Service	With this policy, you can restrict certain HTML Help commands to function only in HTML Help (.chm) files within specified folders and their subfolders. Alternatively, you can disable these commands on the entire

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
		folders	Pack 1	system. It is strongly recommended that only folders requiring administrative privileges be added to this policy. The Shortcut command is used to add a link to a Help topic, and runs executables that are external to the Help file. The WinHelp command is used to add a link to a Help topic, and runs a WinHLP32.exe Help (.hlp) file. When this policy is disabled, or not configured, these commands are fully functional for all Help files. When this policy is enabled, the commands will function only for .chm files in the specified folders and their subfolders. To restrict the commands to one or more folders, enable the policy and enter the desired folders in the text box on the settings tab of the Policy Properties dialog box. Use a semicolon to separate folders. For example, to restrict the commands to only .chm files in the %windir%\help folder and D:\somefolder, add the following string to the edit box: %windir%\help;D:\somefolder. To disallow the Shortcut and WinHelp commands on the entire local system, enable the policy and leave the text box on the settings tab of the Policy Properties dialog box blank. Note: An environment variable may be used, (for example, %windir%), so long as it is defined on the system. For example, %programfiles% is not defined on some early versions of Windows. Note: Only folders on the local computer can be specified in this policy. You cannot use this policy to enable the Shortcut and WinHelp commands for .chm files that are stored on mapped drives or accessed using UNC paths. For additional options, see the Restrict these programs from being launched from Help policy.
COMPUTER	Administrative Templates\System	Do not automatically encrypt files moved to encrypted folders	At least Microsoft Windows 2000	Prevents Windows Explorer from encrypting files that are moved to an encrypted folder. If you disable this setting or do not configure it, Windows Explorer automatically encrypts files that are moved to an encrypted folder. This setting applies only to files moved within a volume. When files are moved to other volumes, or if you create a new file in an encrypted folder, Windows Explorer encrypts those files automatically.
COMPUTER	Administrative Templates\System	Restrict these programs from being launched from Help	At least Microsoft Windows XP Professional or Windows Server 2003 family	Allows you to restrict programs from being run from online Help. If you enable this setting, you can prevent programs that you specify from being allowed to be run from Help. When you enable this setting, enter the list of the programs you want to restrict. Enter the file name of the executable for each application, separated by commas. If you disable or do not configure this setting, users will be able to run applications from online Help. Note: You can also restrict users from running applications by using the Software Restriction settings available in Computer

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Configuration\Security Settings. Note: This setting is available under Computer Configuration and User Comfiguration. If both are set, the list of programs specified in each of these will be restricted.
COMPUTER	Administrative Templates\System	Run		
COMPUTER	Administrative Templates\System	Specify Windows Service Pack installation file location	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate location for Windows Service Pack installation files. To enable this setting, enter the fully qualified path to the new location in the Windows Service Pack Setup file path box. If you disable this setting or do not configure it, the Windows Service Pack Setup source path will be the location used during the last time Windows Service Pack Setup was run on the system.
COMPUTER	Administrative Templates\System	Specify Windows installation file location	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate location for Windows installation files. To enable this setting, and enter the fully qualified path to the new location in the Windows Setup file path box. If you disable this setting or do not configure it, the Windows Setup source path will be the location used during the last time Windows Setup was run on the system.
COMPUTER	Administrative Templates\System	Activate Shutdown Event Tracker System State Data feature	At least Microsoft Windows Server 2003	Defines when the Shutdown Event Tracker System State Data feature is activated. The system state data file contains information about the basic system state as well as the state of all running processes. If you enable this setting, the System State Data feature is activated when the user indicates that the shutdown or restart is unplanned. If you disable this setting, the System State Data feature is never activated. If you do not configure this setting, the default behavior for the System State Data feature occurs. Note: By default, the System State Data feature is always enabled on the Windows Server 2003 family.
COMPUTER	Administrative Templates\System	Display Shutdown Event Tracker	At least Microsoft Windows XP Professional or Windows Server 2003 family	The Shutdown Event Tracker can be displayed when you shut down a workstation or server. This is an extra set of questions that is displayed when you invoke a shutdown to collect information related to why you are shutting down the computer. If you enable this setting and choose Always from the drop-down menu, the Shutdown Event Tracker is displayed when you shut down. If you enable this setting and choose Server Only from the drop-down menu, the Shutdown Event Tracker is displayed when you shut down a Windows Server 2003 family computer. If you enable this setting and choose Workstation Only from the drop-down menu, the Shutdown Event Tracker is displayed when you shut down a Windows XP Professional workstation. If you disable this setting, the Shutdown Event Tracker is not displayed when you shut down. If you do not configure this setting, the default behavior for the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Shutdown Event Tracker occurs. Note: By default, the Shutdown Event Tracker is not displayed on Windows XP Professional and is displayed by default on the Windows Server 2003 family.
COMPUTER	Administrative Templates\System	Verbose vs normal status messages	At least Microsoft Windows 2000	Directs the system to display highly detailed status messages. If you enable this setting, the system displays status messages that reflect each step in the process of starting, shutting down, logging on, or logging off the system. This setting is designed for sophisticated users that require this information. Note: This setting is ignored if the Remove Boot / Shutdown / Logon / Logoff status messages setting is enabled.
COMPUTER	Administrative Templates\System\Disk Quotas	Enable disk quotas	At least Microsoft Windows 2000	Enables and disables disk quota management on all NTFS volumes of the computer, and prevents users from changing the setting. If you enable this setting, disk quota management is enabled, and users cannot disable it. If you disable the setting, disk quota management is disabled, and users cannot enable it. If this setting is not configured, disk quota management is disabled by default, but administrators can enable it. To prevent users from changing the setting while a setting is in effect, the system disables the Enable quota management option on the Quota tab of NTFS volumes. Note: This setting enables disk quota management but does not establish or enforce a particular disk quota limit. To specify a disk quota limit, use the Default quota limit and warning level setting. Otherwise, the system uses the physical space on the volume as the quota limit. Note: To enable or disable disk quota management without specifying a setting, in My Computer, right-click the name of an NTFS volume, click Properties, click the Quota tab, and then click the Enable quota management option.
COMPUTER	Administrative Templates\System\Disk Quotas	Enforce disk quota limit	At least Microsoft Windows 2000	Determines whether disk quota limits are enforced and prevents users from changing the setting. If you enable this setting, disk quota limits are enforced. If you disable this setting, disk quota limits are not enforced. When you enable or disable the setting, the system disables the Deny disk space to users exceeding quota limit option on the Quota tab so administrators cannot make changes while the setting is in effect. If the setting is not configured, the disk quota limit is not enforced by default, but administrators change the setting. Enforcement is optional. When users reach an enforced disk quota limit, the system responds as though the physical space on the volume were exhausted. When users reach an unenforced limit, their status in the Quota Entries window changes, but they can continue to write to the volume as long as physical space is available. Note: This setting overrides user settings that enable or

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				disable quota enforcement on their volumes. Note: To specify a disk quota limit, use the Default quota limit and warning level setting. Otherwise, the system uses the physical space on the volume as the quota limit.
COMPUTER	Administrative Templates\System\Disk Quotas	Default quota limit and warning level	At least Microsoft Windows 2000	Specifies the default disk quota limit and warning level for new users of the volume. This setting determines how much disk space can be used by each user on each of the NTFS file system volumes on a computer. It also specifies the warning level, the point at which the user's status in the Quota Entries window changes to indicate that the user is approaching the disk quota limit. This setting overrides new users' settings for the disk quota limit and warning level on their volumes, and it disables the corresponding options in the Select the default quota limit for new users of this volume section on the Quota tab. This setting applies to all new users as soon as they write to the volume. It does not affect disk quota limits for current users or affect customized limits and warning levels set for particular users (on the Quota tab in Volume Properties). If you disable this setting or do not configure it, the disk space available to users is not limited. The disk quota management feature uses the physical space on each volume as its quota limit and warning level. When you select a limit, remember that the same limit applies to all users on all volumes, regardless of actual volume size. Be sure to set the limit and warning level so that it is reasonable for the range of volumes in the group. This setting is effective only when disk quota management is enabled on the volume. Also, if disk quotas are not enforced, users can exceed the quota limit you set. When users reach the quota limit, their status in the Quota Entries window changes, but users can continue to write to the volume.
COMPUTER	Administrative Templates\System\Disk Quotas	Log event when quota limit exceeded	At least Microsoft Windows 2000	Determines whether the system records an event in the local Application log when users reach their disk quota limit on a volume, and prevents users from changing the logging setting. If you enable this setting, the system records an event when the user reaches their limit. If you disable this setting, no event is recorded. Also, when you enable or disable this setting, the system disables the Log event when a user exceeds their quota limit option on the Quota tab, so administrators cannot change the setting while a setting is in effect. If the setting is not configured, no events are recorded, but administrators can use the Quota tab option to change the setting. This setting is independent of the enforcement settings for disk quotas. As a result, you can direct the system to log an event, regardless of whether or not you choose to enforce the disk quota

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				limit. Also, this setting does not affect the Quota Entries window on the Quota tab. Even without the logged event, users can detect that they have reached their limit, because their status in the Quota Entries window changes. Note: To find the logging option, in My Computer, right-click the name of an NTFS file system volume, click Properties, and then click the Quota tab.
COMPUTER	Administrative Templates\System\Disk Quotas	Log event when quota warning level exceeded	At least Microsoft Windows 2000	Determines whether the system records an event in the Application log when users reach their disk quota warning level on a volume. If you enable this setting, the system records an event. If you disable this setting, no event is recorded. When you enable or disable the setting, the system disables the corresponding Log event when a user exceeds their warning level option on the Quota tab, so that administrators cannot change logging while a setting is in effect. If the setting is not configured, no event is recorded, but administrators can use the Quota tab option to change the logging setting. This setting does not affect the Quota Entries window on the Quota tab. Even without the logged event, users can detect that they have reached their warning level because their status in the Quota Entries window changes. Note: To find the logging option, in My Computer, right-click the name of an NTFS file system volume, click Properties, and then click the Quota tab.
COMPUTER	Administrative Templates\System\Disk Quotas	Apply policy to removable media	At least Microsoft Windows 2000	Extends the disk quota policies in this folder to NTFS file system volumes on removable media. If you disable this setting or do not configure it, the disk quota policies established in this folder apply to fixed-media NTFS volumes only. Note: When this setting is applied, the computer will apply the disk quota to both fixed and removable media.
COMPUTER	Administrative Templates\System\Error Reporting	Configure Error Reporting	At least Microsoft Windows XP Professional or Windows Server 2003 family	Configures how errors are reported and what information is sent when Error Reporting is enabled. This Policy will not enable or disable Error Reporting, to do so use the Turn off Windows Error Reporting policy in Computer Configuration/Administrative Templates/System/Internet Communication Management/Internet Communication settings. If this setting is enabled, it will override any settings made via the control panel for error reporting, and default values will be used for any error reporting policies that are not configured (even if settings were adjusted via the control panel). If this setting is not configured, the user will be able to adjust the setting via the control panel, which is set to 'enable reporting' by default on Windows XP and to `report to Queue' on Windows Server 2003. If this setting is disabled, configuration settings will be set to the default (unchecked for check boxes and empty for text boxes). - Do not

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				display links to any Microsoft `More information' Web sites: Select this if you do not want error dialogs to display links to Microsoft Web sites. - Do not collect additional files: Select this if you do not want additional files to be collected and included in the error reports. - Do not collect additional machine data: Select this if you do not want additional information about the computer to be collected and included in the error reports. - Force queue mode for application errors: Select this if you do not want users to report errors. When this is selected, the errors are placed in a queue directory, and the next administrator to log onto the machine will be able to report the error. - Corporate file path: Type a UNC path to enable Corporate Error Reporting. All errors will be stored at the specified location instead of being sent directly to Microsoft, and the next administrator to log onto the machine will be able to report the error. - Replace instances of the word `Microsoft' with: Use this to customize error report dialogs. The word Microsoft will be replaced with the specified text. Also, see the Display Error Notification settings in this same folder and Turn off Windows Error Reporting in Computer Configuration/Administrative Templates/System/Internet Communication Management/Internet Communication settings. Important: If Turn off Windows Error Reporting is not configured, then Control Panel settings will override these settings.
COMPUTER	Administrative Templates\System\Error Reporting	Display Error Notification	At least Microsoft Windows XP Professional or Windows Server 2003 family	Use this setting to control whether or not a user is given the choice to report an error. When Display Error Notification is enabled, the user will be notified that an error has occurred and will be given access to details about the error. If the Configure Error Reporting setting is also enabled, the user will also be given the choice of whether to report the error. When Display Error Notification is not enabled, the user will not be given the choice of whether to report the error. If the Configure Error Reporting setting is enabled, the error will be automatically reported, but the user will not be notified that an error has occurred. Disabling this setting is useful for server machines that do not have interactive users. If you do not configure this setting, the user will be able to adjust the setting via the control panel, which is set to 'enable notification' by default on Windows XP Personal and Windows XP Professional machines and 'disable notification' on servers. Also, see the Configure Error Reporting policy.
COMPUTER	Administrative Templates\System\Error Reporting\Advanced Error Reporting	Default application reporting settings	At least Microsoft Windows XP Professional or	This setting controls whether or not errors in general applications are included when error reporting is enabled. When this setting is enabled, The 'Default' dropdown list allows you to choose whether or not to report

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	settings		Windows Server 2003 family	all application errors or no application errors by default. When the 'Report all errors in Microsoft applications' checkbox is checked, all errors in Microsoft applications will be reported, regardless of the setting in the 'Default' dropdown list. When the 'Report all errors in Windows components' checkbox is checked, all errors in Windows applications will be reported, regardless of the setting in the 'Default' dropdown list. If this setting is disabled, or not configured, the user will be able to adjust this setting via the control panel, which is set to 'upload all applications' by default. This setting is ignored if the 'Configure Error Reporting' setting is disabled or not configured. Also see the 'Configure Error Reporting' and 'Report Operating System Errors' policies.
COMPUTER	Administrative Templates\System\Error Reporting\Advanced Error Reporting settings	List of applications to never report errors for	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting controls error reporting for errors in general applications when error reporting is enabled. The Default dropdown list allows you to choose whether or not to report all application errors or no application errors by default. To create a list of applications that error reporting will report for, click the Show button next to Report errors for applications on this list and edit the list of application filenames (example: notepad.exe). Errors generated by applications in this list will be reported, even if Default is set to report no application errors. You may use the Report all errors in Microsoft applications and Report all errors in Windows components checkboxes to implicitly add applications in these categories to the include list. Note that the Microsoft applications category includes the Windows components category. To create a list of applications that error reporting will exclude from reporting, click the Show button next to Exclude errors for applications on this list. Errors generated by applications in this list will never be reported, even if the default is set to report all application errors. The exclude list has priority, so if an application is listed in the include list and exclude list the application will be excluded. You may also use the exclude list to exclude specific Microsoft applications or Windows components if you implicitly included these categories in the include list via the two checkboxes. If you disable this setting or do not configure it, the user will be able to adjust this setting via the control panel, which is set to 'upload all applications' by default.
COMPUTER	Administrative Templates\System\Error Reporting\Advanced Error Reporting settings	List of applications to always report errors for	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting specifies the applications that are always included in error reporting. When this setting is enabled, You can create a list of applications that are always included in error reporting: click the 'Show' button, and edit the list of application file names. The file names must include the .exe file name extension (for example, 'notepad.exe'). Errors

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				generated by applications on this list will be reported, even if the Default dropdown in the Default Application Reporting setting is set to report no application errors. If the 'Report all errors in Microsoft applications' or 'Report all errors in Windows components' checkbox in the Default Application Reporting setting is checked, error reporting will report errors as though all applications in these categories were added to this list. (Note: The 'Microsoft applications' category includes the 'Windows components' category. When this setting is disabled or not configured, no list of explicitly included files will be used, though the two checkboxes mentioned above will still be honored. Also see the Default Application Reporting and Application Exclusion List policies. This setting will be ignored if the 'Configure Error Reporting' setting is disabled or not configured.
COMPUTER	Administrative Templates\System\Error Reporting\Advanced Error Reporting settings	Report operating system errors	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting controls whether or not errors in the operating system are included when error reporting is enabled. When this setting is enabled, error reporting will include operating system errors. When this setting is disabled, operating system errors will not be included in error reporting. If you do not configure this setting, the user will be able to adjust this setting via the control panel, which is set to 'upload operating system errors' by default Also see the 'Configure Error Reporting' setting.
COMPUTER	Administrative Templates\System\Error Reporting\Advanced Error Reporting settings	Report unplanned shutdown events	At least Microsoft Windows Server 2003	This setting controls whether or not unplanned shutdown events can be reported when error reporting is enabled. When this setting is enabled, error reporting will include unplanned shutdown events. When this setting is disabled, unplanned shutdown events will not be included in error reporting. If you do not configure this setting, the user will be able to adjust this setting via the control panel, which is set to 'upload unplanned shutdown events' by default. Also see the 'Configure Error Reporting' setting.
COMPUTER	Administrative Templates\System\Group Policy	Allow Cross-Forest User Policy and Roaming User Profiles	At least Microsoft Windows Server 2003	Allows User based policy processing, Roaming User Profiles and User Object logon scripts for cross forest interactive logons. This setting affects all user accounts interactively logging on to a computer in a different forest when a Cross Forest or 2-Way Forest trust exists. When this setting is Not Configured: - No user based policy settings are applied from the user's forest - User will not receive their roaming profiles, they will receive a local profile on the computer from the local forest. A warning message will be shown to the user, and an Event Log message (1529) will be posted. - Loopback Group Policy processing will be applied, using the Group Policy Objects scoped to the machine. - An

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Event Log message (1109) will be posted stating that Loopback was invoked in replace mode. When this setting is Enabled, the behavior is exactly the same as with Windows 2000 Server Family, User policy is applied and a roaming user profile is allowed from the trusted forest. When this setting is Disabled, the behavior is the same as Not Configured.
COMPUTER	Administrative Templates\System\Group Policy	Software Installation policy processing	At least Microsoft Windows 2000	Determines when software installation policies are updated. This setting affects all policies that use the software installation component of Group Policy, such as policies in Software Settings\Software Installation. You can set software installation policy only for Group Policy objects stored in Active Directory, not for Group Policy objects on the local computer. This policy overrides customized settings that the program implementing the software installation policy set when it was installed. If you enable this setting, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Allow processing across a slow network connection option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	Disk Quota policy processing	At least Microsoft Windows 2000	Determines when disk quota policies are updated. This setting affects all policies that use the disk quota component of Group Policy, such as those in Computer Configuration\Administrative Templates\System\Disk Quotas. It overrides customized settings that the program implementing the disk quota policy set when it was installed. If you enable this setting, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Allow processing across a slow network connection option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays. The Do not apply during periodic background processing option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data. The Process

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				even if the Group Policy objects have not changed option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	EFS recovery policy processing	At least Microsoft Windows 2000	Determines when encryption policies are updated. This setting affects all policies that use the encryption component of Group Policy, such as policies related to encryption in Windows Settings\Security Settings. It overrides customized settings that the program implementing the encryption policy set when it was installed. If you enable this setting, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Allow processing across a slow network connection option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays. The Do not apply during periodic background processing option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	Folder Redirection policy processing	At least Microsoft Windows 2000	Determines when folder redirection policies are updated. This setting affects all policies that use the folder redirection component of Group Policy, such as those in WindowsSettings\Folder Redirection. You can only set folder redirection policy for Group Policy objects, stored in Active Directory, not for Group Policy objects on the local computer. This setting overrides customized settings that the program implementing the folder redirection policy set when it was installed. If you enable this setting, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Allow processing across a slow network connection option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays. The Process even if the Group Policy objects have not changed option updates and reapplies the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	Internet Explorer Maintenance policy processing	At least Microsoft Windows 2000	Determines when Internet Explorer Maintenance policies are updated. This setting affects all policies that use the Internet Explorer Maintenance component of Group Policy, such as those in Windows Settings\Internet Explorer Maintenance. It overrides customized settings that the program implementing the Internet Explorer Maintenance policy set when it was installed. If you enable this setting, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Allow processing across a slow network connection option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays. The Do not apply during periodic background processing option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	IP Security policy processing	At least Microsoft Windows 2000	Determines when IP security policies are updated. This setting affects all policies that use the IP security component of Group Policy, such as policies in Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Local Machine. It overrides customized settings that the program implementing the IP security policy set when it was installed. If you enable this setting, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Allow processing across a slow network connection option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays. The Do not apply during periodic background processing option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				cause a program to stop or operate abnormally, and, in rare cases, damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	Registry policy processing	At least Microsoft Windows 2000	Determines when registry policies are updated. This setting affects all policies in the Administrative Templates folder and any other policies that store values in the registry. It overrides customized settings that the program implementing a registry policy set when it was installed. If you enable this setting, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Do not apply during periodic background processing option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	Scripts policy processing	At least Microsoft Windows 2000	Determines when policies that assign shared scripts are updated. This setting affects all policies that use the scripts component of Group Policy, such as those in WindowsSettings\Scripts. It overrides customized settings that the program implementing the scripts policy set when it was installed. If you enable this policy, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Allow processing across a slow network connection option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays. The Do not apply during periodic background processing option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	Security policy processing	At least Microsoft Windows 2000	Determines when security policies are updated. This setting affects all policies that use the security component of Group Policy, such as those in Windows Settings\Security Settings. It overrides customized settings that the program implementing the security policy set when it was installed. If you enable this setting, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Do not apply during periodic background processing option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and in rare cases, damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they be updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	Wireless policy processing	At least Microsoft Windows 2000	Determines when policies that assign wireless network settings are updated. This setting affects all policies that use the wireless network component of Group Policy, such as those in WindowsSettings\Wireless Network Policies. It overrides customized settings that the program implementing the wireless network set when it was installed. If you enable this policy, you can use the check boxes provided to change the options. If you disable this setting or do not configure it, it has no effect on the system. The Allow processing across a slow network connection option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays. The Do not apply during periodic background processing option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				reapplying a desired setting in case a user has changed it.
COMPUTER	Administrative Templates\System\Group Policy	Disallow Interactive Users from generating Resultant Set of Policy data	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting controls the ability of users to view their Resultant Set of Policy (RSoP) data. By default, interactively logged on users can view their own Resultant Set of Policy (RSoP) data. If this setting is enabled, interactive users cannot generate RSoP data. If this setting is not configured or disabled, interactive Users can generate RSoP. Note: This setting does not affect administrators. If this setting is enabled or disabled, by default, administrators can view RSoP data. Note: To view RSoP data on a client computer, use the RSoP snap-in for the Microsoft Management Console. You can launch the RSoP snap-in from the command line by typing RSOP.msc Note: This setting exists as both a User Configuration and Computer Configuration setting. Also, see the Turn off Resultant set of Policy Logging setting in Computer Configuration\Administrative Templates\System\GroupPolicy.
COMPUTER	Administrative Templates\System\Group Policy	Turn off background refresh of Group Policy	At least Microsoft Windows 2000	Prevents Group Policy from being updated while the computer is in use. This setting applies to Group Policy for computers, users, and domain controllers. If you enable this setting, the system waits until the current user logs off the system before updating the computer and user settings. If you disable this setting, updates can be applied while users are working. The frequency of updates is determined by the Group Policy refresh interval for computers and Group Policy refresh interval for users settings. Note: If you make changes to this setting, you must restart your computer for it to take effect.
COMPUTER	Administrative Templates\System\Group Policy	Remove users ability to invoke machine policy refresh	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting allows you to control a user's ability to invoke a computer policy refresh. If you enable this setting, users may not invoke a refresh of computer policy. Computer policy will still be applied at startup or when an official policy refresh occurs. If you disable or do not configure this setting, the default behavior applies. By default, computer policy is applied when the computer starts up. It also applies at a specified refresh interval or when manually invoked by the user. Note: This setting only applies to non-administrators. Administrators can still invoke a refresh of computer policy at any time, no matter how this policy is configured. Also, see the Group Policy refresh interval for computers setting to change the policy refresh interval. Note: If you make changes to this setting, you must restart your computer for it to take effect.
COMPUTER	Administrative Templates\System\Group Policy	Group Policy slow link detection	At least Microsoft Windows 2000	Defines a slow connection for purposes of applying and updating Group Policy. If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				the rate specified by this setting, the system considers the connection to be slow. The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, the policy processing settings in this folder lets you override the programs' specified responses to slow links. To use this setting, in the Connection speed box, type a decimal number between 0 and 4,294,967,200 (0xFFFFFFA0), indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast. If you disable this setting or do not configure it, the system uses the default value of 500 kilobits per second. This setting appears in the Computer Configuration and User Configuration folders. The setting in Computer Configuration defines a slow link for policies in the Computer Configuration folder. The setting in User Configuration defines a slow link for settings in the User Configuration folder. Also, see the Do not detect slow network connections and related policies in Computer Configuration\Administrative Templates\System\User Profile. Note: If the profile server has IP connectivity, the connection speed setting is used. If the profile server does not have IP connectivity, the SMB timing is used.
COMPUTER	Administrative Templates\System\Group Policy	Group Policy refresh interval for computers	At least Microsoft Windows 2000	Specifies how often Group Policy for computers is updated while the computer is in use (in the background). This setting specifies a background update rate only for Group Policies in the Computer Configuration folder. In addition to background updates, Group Policy for the computer is always updated when the system starts. By default, computer Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes. You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations. If you disable this setting, Group Policy is updated every 90 minutes (the default). To specify that Group Policy should never be updated while the computer is in use, select the Turn off background refresh of Group Policy policy. The Group Policy refresh interval for computers policy also lets you specify how much the actual update interval varies. To prevent clients with the same update interval from requesting updates simultaneously, the system varies the update interval for each client by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that client requests overlap. However, updates might be delayed significantly. This setting establishes the update rate for computer Group Policy. To set an update rate for user policies, use the Group Policy refresh interval for users setting (located in User Configuration\Administrative Templates\System\Group Policy). This setting is only used when the Turn off background refresh of Group Policy setting is not enabled. Note: Consider notifying users that their policy is updated periodically so that they recognize the signs of a policy update. When Group Policy is updated, the Windows desktop is refreshed; it flickers briefly and closes open menus. Also, restrictions imposed by Group Policies, such as those that limit the programs users can run, might interfere with tasks in progress.
COMPUTER	Administrative Templates\System\Group Policy	Group Policy refresh interval for domain controllers	At least Microsoft Windows 2000	Specifies how often Group Policy is updated on domain controllers while they are running (in the background). The updates specified by this setting occur in addition to updates performed when the system starts. By default, Group Policy on the domain controllers is updated every five minutes. You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the domain controller tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations. If you disable this setting, the domain controller updates Group Policy every 5 minutes (the default). To specify that Group Policies for users should never be updated while the computer is in use, select the Turn off background refresh of Group Policy setting. This setting also lets you specify how much the actual update interval varies. To prevent domain controllers with the same update interval from requesting updates simultaneously, the system varies the update interval for each controller by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that update requests overlap. However, updates might be delayed significantly. Note: This setting is used only when you are establishing policy for a domain, site, organizational unit (OU), or customized group. If you are establishing policy for a local computer only, the system ignores this setting.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\System\Group Policy	Always use local ADM files for Group Policy Object Editor	At least Microsoft Windows Server 2003	Always use local ADM files for the Group Policy snap-in. By default, when you edit a Group Policy object (GPO) using the Group Policy Object Editor snap-in, the ADM files are loaded from that GPO into the Group Policy Object Editor snap-in. This enables you to use the same version of the ADM files that were used to create the GPO while editing this GPO. This leads to the following behavior: - If you originally created the GPO with, for example, an English system, the GPO contains English ADM files. - If you later edit the GPO from a different-language system, you get the English ADM files as they were in the GPO. You can change this behavior by using this setting. If you enable this setting, the Group Policy Object Editor snap-in always uses local ADM files in your %windir%\inf directory when editing GPOs. This leads to the following behavior: - If you had originally created the GPO with an English system, and then you edit the GPO with a Japanese system, the Group Policy Object Editor snap-in uses the local Japanese ADM files, and you see the text in Japanese under Administrative Templates. If you disable or do not configure this setting, the Group Policy Object Editor snap-in always loads all ADM files from the actual GPO. Note: If the ADMs that you require are not all available locally in your %windir%\inf directory, you might not be able to see all the settings that have been configured in the GPO that you are editing.
COMPUTER	Administrative Templates\System\Group Policy	Turn off Resultant Set of Policy logging	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting allows you to enable or disable Resultant Set of Policy (RSoP) logging on a client computer. RSoP logs information on Group Policy settings that have been applied to the client. This information includes details such as which Group Policy objects (GPO) were applied, where they came from, and the client-side extension settings that were included. If you enable this setting, RSoP logging is turned off. If you disable or do not configure this setting, RSoP logging is turned on. By default, RSoP logging is always on. Note: To view the RSoP information logged on a client computer, you can use the RSoP snap-in in the Microsoft Management Console (MMC).
COMPUTER	Administrative Templates\System\Group Policy	User Group Policy loopback processing mode	At least Microsoft Windows 2000	Applies alternate user settings when a user logs on to a computer affected by this setting. This setting directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this setting. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user setting based on the computer that is being used. By default, the user's Group Policy objects determine which user settings apply. If this setting is enabled, then, when a user logs on

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				to this computer, the computer's Group Policy objects determine which set of Group Policy objects applies. To use this setting, select one of the following modes from the Mode box: -- Replace indicates that the user settings defined in the computer's Group Policy objects replace the user settings normally applied to the user. -- Merge indicates that the user settings defined in the computer's Group Policy \
COMPUTER	Administrative Templates\System\Internet Communication Management	Restrict Internet communication	At least Microsoft Windows XP Professional with SP2	Specifies whether Windows can access the Internet to accomplish tasks that require Internet resources. If this setting is enabled, the policies that are listed in the Internet Communication Management section of Group Policy are all enabled. If this setting is disabled, or not configured, all of the policies listed in this section will be disabled.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Automatic Root Certificates Update	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Specifies whether to automatically update root certificates using the Window Update Web site. Typically, a certificate is used when you use a secure Web site or when you send and receive secure e-mail. Anyone can issue certificates, but to have transactions that are as secure as possible, certificates must be issued by a trusted certificate authority (CA). Microsoft has included a list in Windows XP and other products of companies and organizations that it considers trusted authorities. If you enable this setting, when you are presented with a certificate issued by an untrusted root authority your computer will not contact the Windows Update web site to, to see if Microsoft has added the CA to its list of trusted authorities. If you disable or do not configure this setting, your computer will contact the Windows Update Web site.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off printing over HTTP	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Specifies whether to allow printing over HTTP from this client. Printing over HTTP allows a client to print to printers on the intranet as well as the Internet. Note: This setting affects the client side of Internet printing only. It does not prevent this machine from acting as an Internet Printing server and making it's shared printers available via HTTP. If you enable this setting, it prevents this client from printing to internet printers over HTTP. If you disable or do not configure this setting, users will be able to choose to print to internet printers over HTTP. Also see the Web-based Printing setting in Computer Configuration/Administrative Templates/Printers.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off downloading of print drivers over HTTP	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family	Specifies whether to allow this client to download print driver packages over HTTP. To setup HTTP printing, non-inbox drivers need to be downloaded over HTTP. Note: This setting does not prevent the client from printing to printers on the Intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally. If you

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			with SP1	enable this setting, print drivers will not be downloaded over HTTP. If you disable this setting or do not configure it, users will be able to download print drivers over HTTP.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Windows Update device driver searching	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	This policy specifies whether Windows searches Windows Update for device drivers when no local drivers for a device are present. If you enable this setting, Windows Update will not be searched when a new device is installed. If you disable this setting, Windows Update will always be searched for drivers when no local drivers are present. If you do not configure this setting, searching Windows Update will be optional when installing a device. Also see Turn off Windows Update device driver search prompt in Administrative Templates/System which governs whether an administrator is prompted before searching Windows Update for device drivers if a driver is not found locally.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Event Viewer Events.asp links	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Specifies whether Events.asp hyperlinks are available for events within the Event Viewer application. The Event Viewer normally makes all HTTP(S) URLs into hot links that activate the Internet browser when clicked. In addition, More Information is placed at the end of the description text if the event is created by a Microsoft component. This text contains a link (URL) that, if clicked, sends information about the event to Microsoft, and allows users to learn more about why that event occurred. If you enable this setting, event description URL links are not activated and the text More Information is not displayed at the end of the description. If you disable or do not configure this setting, the user can click the hyperlink which prompts the user and then sends information about the event over the internet to Microsoft. Also, see Events.asp URL, Events.asp program, and Events.asp Program Command Line Parameters settings in Administrative Templates/Windows Components/Event Viewer.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Help and Support Center Did you know? content	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Specifies whether to show the Did you know? section of Help and Support Center. This content is dynamically updated when users who are connected to the Internet open Help and Support Center, and provides up-to-date information about Windows and the computer. If you enable this setting, the Help and Support Center will no longer retrieve nor display Did you know? content. If you disable not configure this setting, the Help and Support Center will retrieve and display Did you know? content. You might want to enable this setting for users who do not have Internet access, because the content in the Did you know? section will remain static indefinitely without an Internet connection.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Help and Support Center Microsoft Knowledge Base search	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Specifies whether users can perform a Microsoft Knowledge Base search from the Help and Support Center. The Knowledge Base is an online source of technical support information and self-help tools for Microsoft products and is searched as part of all Help and Support Center searches with the default search options. If you enable this setting, it will remove the Knowledge Base section from the Help and Support Center Set search options page and only help content on the local computer will be searched.. If you disable this setting or do not configure it, the Knowledge Base will be searched if the user has a connection to the Internet and has not disabled the Knowledge Base search from the Search Options page.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Windows Movie Maker automatic codec downloads	At least Microsoft Windows XP Professional with SP2	Specifies whether Windows Movie Maker automatically downloads codecs. Windows Movie Maker can be configured so that codecs are downloaded automatically if the required codecs are not installed on the computer. If you enable this setting, Windows Movie Maker will not attempt to download missing codecs for imported audio and video files. If you disable or do not configure this setting, Windows Movie Maker might attempt to download missing codecs for imported audio and video files.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Windows Movie Maker online Web links	At least Microsoft Windows XP Professional with SP2	Specifies whether links to Web sites are available in Windows Movie Maker. These links include the Windows Movie Maker on the Web and Privacy Statement commands that appear on the Help menu, as well as the Learn more about video filters hyperlink in the Options dialog box and the sign up now hyperlink in the The Web saving option in the Save Movie Wizard. The Windows Movie Maker on the Web command lets users go directly to the Windows Movie Maker Web site to get more information, and the Privacy Statement command lets users view information about privacy issues in respect to Windows Movie Maker. The Learn more about video filters hyperlink lets users learn more about video filters and their role in saving movies process in Windows Movie Maker. The sign up now hyperlink lets users sign up with a video hosting provider on the Web. If you enable this setting, the previously mentioned links to Web sites from Windows Movie Maker are disabled and cannot be selected. If you disable or do not configure this setting, the previously mentioned links to Web sites from Windows Movie Maker are enabled and can be selected.
COMPUTER	Administrative Templates\System\Internet	Turn off Windows Movie Maker saving to online	At least Microsoft Windows XP	Specifies whether users can send a final movie to a video hosting provider on the Web by choosing The Web saving option in the Save

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Communication Management\Internet Communication settings	video hosting provider	Professional with SP2	Movie Wizard of Windows Movie Maker. When users create a movie in Windows Movie Maker, they can choose to share it in a variety of ways through the Save Movie Wizard. The Web saving option lets users send their movies to a video hosting provider. If you enable this setting, users cannot choose The Web saving option in the Save Movie Wizard of Windows Movie Maker and cannot send a movie to a video hosting provider on the Web. If you disable or do not configure this setting, users can choose The Web saving option in the Save Movie Wizard of Windows Movie Maker and can send a movie to a video hosting provider on the Web.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Specifies whether the Internet Connection Wizard can connect to Microsoft to download a list of Internet Service Providers (ISPs). If you enable this setting, the Choose a list of Internet Service Providers path in the Internet Connection Wizard will cause the wizard to exit. This prevents users from retrieving the list of ISPs, which resides on Microsoft servers. If you disable or do not configure this setting, users will be able to connect to Microsoft to download a list of ISPs for their area.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Registration if URL connection is referring to Microsoft.com	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Specifies whether the Windows Registration Wizard connects to Microsoft.com for online registration. If you enable this setting, it blocks users from connecting to Microsoft.com for online registration and users cannot register their copy of Windows online. If you disable or do not configure this setting, users can connect to Microsoft.com to complete the online Windows Registration. Note that registration is optional and involves submitting some personal information to Microsoft. However, Windows Product Activation is required but does not involve submitting any personal information (except the country you live in).
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Windows Error Reporting	At least Microsoft Windows XP Professional or Windows Server 2003 family	Controls whether or not errors are reported to Microsoft. Error Reporting is used to report information about a system or application that has failed or has stopped responding and is used to improve the quality of the product. If you enable this setting, users will not be given the option to report errors. If you disable or do not configure this setting, the errors may be reported to Microsoft via the Internet or to a corporate file share. This setting overrides any user setting made from the Control Panel for error reporting. Also see Configure Error Reporting and Display Error Notification settings in Computer Configuration/Administrative Templates/System/Error Reporting.
COMPUTER	Administrative Templates\System\Internet	Turn off access to all Windows Update	At least Microsoft Windows 2000	This setting allows you to remove access to Windows Update. If you enable this setting, all Windows Update features are removed. This

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Communication Management\Internet Communication settings	features	Service Pack 3, Microsoft Windows XP Professional Service Pack 1 or Microsoft Windows Server 2003 family	includes blocking access to the Windows Update Web site at http://windowsupdate.microsoft.com, 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 will neither be notified about nor will you receive critical updates from Windows Update. This setting also prevents Device Manager from automatically installing driver updates from the Windows Update Web site. If you disable or do not configure this setting, users will be able to access the Windows Update Web site and enable automatic updating to receive notifications and critical updates from Windows Update.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Search Companion content file updates	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Specifies whether Search Companion should automatically download content updates during local and Internet searches. When the user searches the local machine or the Internet, Search Companion occasionally connects to Microsoft to download an updated privacy policy and additional content files used to format and display results. If you enable this setting, Search Companion will not download content updates during searches. If you disable or do not configure this setting, Search Companion will download content updates unless the user is using Classic Search. Note: Internet searches will still send the search text and information about the search to Microsoft and the chosen search provider. Choosing Classic Search will turn off the Search Companion feature completely.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Internet File Association service	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether to use the Microsoft Web service for finding an application to open a file with an unhandled file association. When a user opens a file that has an extension that is not associated with any applications on the machine, they are given the choice to choose a local application or use the Web service to find an application. If you enable this setting, the link and the dialog for using the Web service to open an unhandled file association are removed. If you disable or do not configure this setting, the user will be allowed to use the Web service.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Internet download for Web publishing and online ordering wizards	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family	Specifies whether Windows should download a list of providers for the Web publishing and online prdering wizards. These wizards allow users to select from a list of companies that provide services such as online storage and photographic printing. By default, Windows displays providers downloaded from a Windows Web site in addition to providers specified in the registry. If you enable this setting, Windows will not download providers and only the service providers that are cached in the local registry will be displayed. If you disable or do not configure this

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				setting, a list of providers will be downloaded when the user uses the Web publishing or online ordering wizards. See the documentation for the Web publishing and online ordering wizards for more information, including details on specifying service providers in the registry.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off the Order Prints picture task	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family	Specifies whether the Order Prints Online task is available from Picture Tasks in Windows folders. The Order Prints Online Wizard is used to download a list of providers and allow users to order prints online. If you enable this setting, the task Order Prints Online is removed from Picture Tasks in Windows Explorer folders. If you disable or do not configure this setting, the task is displayed.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off the Publish to Web task for files and folders	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family	Specifies whether the tasks Publish this file to the Web, Publish this folder to the Web, and Publish the selected items to the Web, are available from File and Folder Tasks in Windows folders. The Web Publishing Wizard is used to download a list of providers and allow users to publish content to the Web. If you enable this setting, these tasks are removed from the File and Folder tasks in Windows folders. If you disable or do not configure this setting, the tasks will be shown.
COMPUTER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off the Windows Messenger Customer Experience Improvement Program	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family	Specifies whether Windows Messenger collects anonymous information about how Windows Messenger software and service is used. With the Customer Experience Improvement program, users can allow Microsoft to collect anonymous information about how the product is used. This information is used to improve the product in future releases. If you enable this setting, Windows Messenger will not collect usage information and the user settings to enable the collection of usage information will not be shown. If you disable this setting, Windows Messenger will collect anonymous usage information and the setting will not be shown. If you do not configure this setting, users will have the choice to opt-in and allow information to be collected.
COMPUTER	Administrative Templates\System\Logon	Do not process the legacy run list	At least Microsoft Windows 2000	Ignores the customized run list. You can create a customized list of additional programs and documents that the system starts automatically when it runs on Windows XP Professional, Windows 2000 Professional, Windows NT Workstation 4.0 and earlier. These programs are added to the standard run list of programs and services that the system starts. If you enable this setting, the system ignores the run list for Windows NT Workstation 4.0, Windows 2000 Professional, and Windows XP Professional. If you disable or do not configure this setting, Windows 2000 adds any customized run list configured for Windows NT 4.0 and earlier to its run list. This setting appears in the Computer Configuration

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Note: To create a customized run list by using a policy, use the Run these applications at startup setting. The customized run lists for Windows NT 4.0 and earlier are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run and HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run. They can be configured by using the Run setting in System Policy Editor for Windows NT 4.0 and earlier. Also, see the Do not process the run once list setting.
COMPUTER	Administrative Templates\System\Logon	Do not process the run once list	At least Microsoft Windows 2000	Ignores customized run-once lists. You can create a customized list of additional programs and documents that are started automatically the next time the system starts (but not thereafter). These programs are added to the standard list of programs and services that the system starts. If you enable this setting, the system ignores the run-once list. If you disable this setting or do not configure it, the system runs the programs in the run-once list. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Note: Customized run-once lists are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce. Also, see the Do not process the legacy run list setting.
COMPUTER	Administrative Templates\System\Logon	Always use classic logon	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting forces the user to log on to the computer using the classic logon screen. By default, a workgroup is set to use the simple logon screen. This setting only works when the computer is not on a domain.
COMPUTER	Administrative Templates\System\Logon	Don't display the Getting Started welcome screen at logon	Only works on Microsoft Windows 2000	Supresses the welcome screen. This setting hides the welcome screen that is displayed on Windows 2000 Professional and Windows XP Professional each time the user logs on. Users can still display the welcome screen by selecting it on the Start menu or by typing Welcome in the Run dialog box. This setting applies only to Windows 2000 Professional and Windows XP Professional. It does not affect the Configure Your Server on a Windows 2000 Server screen on Windows 2000 Server. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To display the welcome screen, click Start, point to Programs, point to Accessories, point to System Tools, and then click Getting Started. To suppress the welcome screen without specifying a setting, clear the Show this screen at startup check box on the welcome screen.
COMPUTER	Administrative Templates\System\Logon	Run these programs at user logon	At least Microsoft Windows 2000	Specifies additional programs or documents that Windows starts automatically when a user logs on to the system. To use this setting, click Show, click Add, and then, in the text box, type the name of the executable program (.exe) file or document file. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the system starts the programs specified in the Computer Configuration setting just before it starts the programs specified in the User Configuration setting. Also, see the Do not process the legacy run list and the Do not process the run once list settings.
COMPUTER	Administrative Templates\System\Logon	Always wait for the network at computer startup and logon	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether Windows XP waits for the network during computer startup and user logon. By default, Windows XP does not wait for the network to be fully initialized at startup and logon. Existing users are logged on using cached credentials, which results in shorter logon times. Group Policy is applied in the background once the network becomes available. Note that because this is a background refresh, extensions such as Software Installation and Folder Redirection take two logons to apply changes. To be able to operate safely, these extensions require that no users be logged on. Therefore, they must be processed in the foreground before users are actively using the computer. In addition, changes that are made to the user object, such as adding a roaming profile path, home directory, or user object logon script, may take up to two logons to be detected. If a user with a roaming profile, home directory, or user object logon script logs on to a computer, Windows XP always waits for the network to be initialized before logging the user on. If a user has never logged on to this computer before, Windows XP always waits for the network to be initialized. If you enable this setting, logons are performed in the same way as for Windows 2000 clients, in that Windows XP waits for the network to be fully initialized before users are logged on. Group Policy is applied in the foreground, synchronously. If you disable or do not configure this setting, Windows does not wait for the network to be fully initialized and users are logged on with cached

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				credentials. Group Policy is applied asynchronously in the background. Note: If you want to guarantee the application of Folder Redirection, Software Installation, or roaming user profile settings in just one logon, enable this setting to ensure that Windows waits for the network to be available before applying policy. Note: For servers, the startup and logon processing always behaves as if this policy setting is enabled.
COMPUTER	Administrative Templates\System\Net Logon	Contact PDC on logon failure	At least Microsoft Windows XP Professional or Windows Server 2003 family	Defines whether a domain controller (DC) should attempt to verify with the PDC the password provided by a client if the DC failed to validate the password. Contacting the PDC is useful in case the client's password was recently changed and did not propagate to the DC yet. Users may want to disable this feature if the PDC is located over a slow WAN connection. To enable this feature, click Enabled. To disable this feature, click Disabled.
COMPUTER	Administrative Templates\System\Net Logon	Initial DC Discovery Retry Setting for Background Callers	At least Microsoft Windows XP Professional or Windows Server 2003 family	When applications performing periodic searches for domain controllers (DC) are unable to find a DC, the value set in this setting determines the amount of time (in seconds) before the first retry. The default value for this setting is 10 minutes (10*60). The maximum value for this setting is 49 days (0x4294967). The minimum value for this setting is 0. This setting is relevant only to those callers of DsGetDcName that have specified the DS_BACKGROUND_ONLY flag. If the value of this setting is less than the value specified in the NegativeCachePeriod subkey, the value in the NegativeCachePeriod subkey is used. Warning: If the value for this setting is too large, a client will not attempt to find any DCs that were initially unavailable. If the value set in this setting is very small and the DC is not available, the traffic caused by periodic DC discoveries may be excessive.
COMPUTER	Administrative Templates\System\Net Logon	Maximum DC Discovery Retry Interval Setting for Background Callers	At least Microsoft Windows XP Professional or Windows Server 2003 family	When applications performing periodic searches for Domain Controllers (DCs) are unable to find a DC, the value set in this setting determines the maximum retry interval allowed. For example, the retry intervals may be set at 10 minutes, then 20 minutes and then 40 minutes, but when the interval reaches the value set in this setting, that value becomes the retry interval for all subsequent retries until the value set in Final DC Discovery Retry Setting is reached. The default value for this setting is 60 minutes (60*60). The maximum value for this setting is 49 days (0x4294967). The minimum value for this setting is 0. If the value for this setting is smaller than the value specified for the Initial DC Discovery Retry Setting, the Initial DC Discovery Retry Setting is used. Warning: If the value for this setting is too large, a client may take very long periods

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				to try to find a DC. If the value for this setting is too small and the DC is not available, the frequent retries may produce excessive network traffic.
COMPUTER	Administrative Templates\System\Net Logon	Final DC Discovery Retry Setting for Background Callers	At least Microsoft Windows XP Professional or Windows Server 2003 family	When applications performing periodic searches for domain controllers (DC) are unable to find a DC, the value set in this setting determines when retries are no longer allowed. For example, retires may be set to occur according to the Maximum DC Discovery Retry Interval Setting, but when the value set in this setting is reached, no more retries occur. If a value for this setting is smaller than the value in Maximum DC Discovery Retry Interval Setting, the value for Maximum DC Discovery Retry Interval Setting is used. The default value for this setting is to not quit retrying (0). The maximum value for this setting is 49 days (0x4294967). The minimum value for this setting is 0. Warning: If the value for this setting is too small, a client will stop trying to find a DC too soon.
COMPUTER	Administrative Templates\System\Net Logon	Positive Periodic DC Cache Refresh for Background Callers	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines when a successful DC cache entry is refreshed. This setting is applied to caller programs that periodically attempt to locate DCs, and it is applied before the returning the DC information to the caller program. The default value for this setting is infinite (4294967200). The maximum value for this setting is (4294967200), while the maximum that is not treated as infinity is 49 days (4294967). Any larger value is treated as infinity. The minimum value for this setting is to always refresh (0).
COMPUTER	Administrative Templates\System\Net Logon	Log File Debug Output Level	At least Microsoft Windows Server 2003	Specifies the level of debug output for the Net Logon service. The Net Logon service outputs debug information to the log file netlogon.log in the directory %windir%\debug. By default, no debug information is logged. If you enable this setting and specify a non-zero value, debug information will be logged to the file. Higher values result in more verbose logging; the value of 536936447 is commonly used as an optimal setting. If you specify zero for this setting, the default behavior occurs as described above. If you disable this setting or do not configure it, the default behavior occurs as described above.
COMPUTER	Administrative Templates\System\Net Logon	Expected dial-up delay on logon	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the additional time for the computer to wait for the domain controller's (DC) response when logging on to the network. To specify the Expected dial-up delay at logon, click Enable, and then enter the desired value in seconds (for example, the value 60 is 1 minute). If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\System\Net	Maximum Log File Size	At least Microsoft	Specifies the maximum size in bytes of the log file netlogon.log in the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Logon		Windows Server 2003	directory %windir%\debug when logging is enabled. By default, the maximum size of the log file is 20MB. If this policy is enabled, the maximum size of the log file is set to the specified size. Once this size is reached the log file is saved to netlogon.bak and netlogon.log is truncated. A reasonable value based on available storage should be specified. If this policy is disabled or not configured, the default behavior occurs as indicated above.
COMPUTER	Administrative Templates\System\Net Logon	Negative DC Discovery Cache Setting	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the amount of time (in seconds) the DC locator remembers that a domain controller (DC) could not be found in a domain. When a subsequent attempt to locate the DC occurs within the time set in this setting, DC Discovery immediately fails, without attempting to find the DC. The default value for this setting is 45 seconds. The maximum value for this setting is 7 days (7*24*60*60). The minimum value for this setting is 0. Warning: If the value for this setting is too large, a client will not attempt to find any DCs that were initially unavailable. If the value for this setting is too small, clients will attempt to find DCs even when none are available.
COMPUTER	Administrative Templates\System\Net Logon	Netlogon share compatibility	At least Microsoft Windows Server 2003	This setting controls whether or not the Netlogon share created by the Net Logon service on a domain controller (DC) should support compatibility in file sharing semantics with earlier applications. When this setting is enabled, the Netlogon share will honor file sharing semantics that grant requests for exclusive read access to files on the share even when the caller has only read permission. When this setting is disabled or not configured, the Netlogon share will grant shared read access to files on the share when exclusive access is requested and the caller has only read permission. By default, the Netlogon share will grant shared read access to files on the share when exclusive access is requested. Note: The Netlogon share is a share created by the Net Logon service for use by client machines in the domain. The default behavior of the Netlogon share ensures that no application with only read permission to files on the Netlogon share can lock the files by requesting exclusive read access, which might prevent Group Policy settings from being updated on clients in the domain. When this setting is enabled, an application that relies on the ability to lock files on the Netlogon share with only read permission will be able to deny Group Policy clients from reading the files, and in general the availability of the Netlogon share on the domain will be decreased. If this setting is enabled, domain administrators should ensure that the only applications using the exclusive read capability in the domain are those approved by

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				the administrator.
COMPUTER	Administrative Templates\System\Net Logon	Positive Periodic DC Cache Refresh for Non-Background Callers	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines when a successful DC cache entry is refreshed. This setting is applied to caller programs that do not periodically attempt to locate DCs, and it is applied before the returning the DC information to the caller program. This setting is relevant to only those callers of DsGetDcName that have not specified the DS_BACKGROUND_ONLY flag. The default value for this setting is 30 minutes (1800). The maximum value for this setting is (4294967200), while the maximum that is not treated as infinity is 49 days (4294967). Any larger value will be treated as infinity. The minimum value for this setting is to always refresh (0).
COMPUTER	Administrative Templates\System\Net Logon	Scavenge Interval	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines the interval at which Netlogon performs the following scavenging operations: - Checks if a password on a secure channel needs to be modified, and modifies it if necessary. - On the domain controllers (DC), discovers a DC that has not been discovered. - On the PDC, attempts to add the <DomainName>[1B] NetBIOS name if it hasn't already been successfully added. None of these operations are critical. 15 minutes is optimal in all but extreme cases. For instance, if a DC is separated from a trusted domain by an expensive (e.g., ISDN) line, this parameter might be adjusted upward to avoid frequent automatic discovery of DCs in a trusted domain. To enable the setting, click Enabled, and then specify the interval in seconds.
COMPUTER	Administrative Templates\System\Net Logon	Site Name	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the Active Directory site to which computers belong. An Active Directory site is one or more well-connected TCP/IP subnets that allow administrators to configure Active Directory access and replication. To specify the site name for this setting, click Enabled, and then enter the site name. When the site to which a computer belongs is not specified, the computer automatically discovers its site from Active Directory. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon	Sysvol share compatibility	At least Microsoft Windows Server 2003	This setting controls whether or not the Sysvol share created by the Net Logon service on a domain controller (DC) should support compatibility in file sharing semantics with earlier applications. When this setting is enabled, the Sysvol share will honor file sharing semantics that grant requests for exclusive read access to files on the share even when the caller has only read permission. When this setting is disabled or not configured, the Sysvol share will grant shared read access to files on the share when exclusive access is requested and the caller has only read

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				permission. By default, the Sysvol share will grant shared read access to files on the share when exclusive access is requested. Note: The Sysvol share is a share created by the Net Logon service for use by Group Policy clients in the domain. The default behavior of the Sysvol share ensures that no application with only read permission to files on the sysvol share can lock the files by requesting exclusive read access, which might prevent Group Policy settings from being updated on clients in the domain. When this setting is enabled, an application that relies on the ability to lock files on the Sysvol share with only read permission will be able to deny Group Policy clients from reading the files, and in general the availability of the Sysvol share on the domain will be decreased. If this setting is enabled, domain administrators should ensure that the only applications using the exclusive read capability in the domain are those approved by the administrator.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Location of the DCs hosting a domain with single label DNS name	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether the computers to which this setting is applied attempt DNS name resolution of a single-label domain names. By default, when a computer (or the DC Locator running on a computer, to be more specific) needs to locate a domain controller hosting an Active Directory domain specified with a single-label name, the computer exclusively uses NetBIOS name resolution, but not the DNS name resolution, unless the computer is joined to an Active Directory forest in which at least one domain has a single-label DNS name. If this setting is enabled, computers to which this policy is applied will attempt to locate a domain controller hosting an Active Directory domain specified with a single-label name using DNS name resolution. If this setting is disabled, computers to which this setting is applied will attempt to locate a domain controller hosting an Active Directory domain specified with a single-label name only using NetBIOS name resolution, but not the DNS name resolution, unless the computer is searching for a domain with a single label DNS name that exists in the Active Directory forest to which this computer is joined. If this setting is not configured, it is not applied to any computers, and computers use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Automated Site Coverage by the DC Locator DNS SRV Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether domain controllers (DC) will dynamically register DC Locator site-specific SRV records for the closest sites where no DC for the same domain exists (or no Global Catalog for the same forest exists). These DNS records are dynamically registered by the Net Logon service, and they are used to locate the DC. If this setting is enabled, the DCs to which this setting is applied dynamically register DC Locator site-specific DNS SRV records for the closest sites where no DC for the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				same domain, or no Global Catalog for the same forest, exists. If you disable this setting, the DCs will not register site-specific DC Locator DNS SRV records for any other sites but their own. If this setting is not configured, it is not applied to any DCs, and DCs use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	DC Locator DNS records not registered by the DCs	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines which Domain Controller (DC) Locator DNS records are not registered by the Netlogon service. To enable this setting, select Enable and specify a list of space-delimited mnemonics (instructions) for the DC Locator DNS records that will not be registered by the DCs to which this setting is applied. Select the mnemonics from the following list: Mnemonic Type DNS Record LdapIpAddress A <DnsDomainName> Ldap SRV _ldap._tcp.<DnsDomainName> LdapAtSite SRV _ldap._tcp.<SiteName>._sites.<DnsDomainName> Pdc SRV _ldap._tcp.pdc._msdcs.<DnsDomainName> Gc SRV _ldap._tcp.gc._msdcs.<DnsForestName> GcAtSite SRV _ldap._tcp.<SiteName>._sites.gc._msdcs.<DnsForestName> DcByGuid SRV _ldap._tcp.<DomainGuid>.domains._msdcs.<DnsForestName> GcIpAddress A _gc._msdcs.<DnsForestName> DsaCname CNAME <DsaGuid>._msdcs.<DnsForestName> Kdc SRV _kerberos._tcp.dc._msdcs.<DnsDomainName> KdcAtSite SRV _kerberos._tcp.dc._msdcs.<SiteName>._sites.<DnsDomainName> Dc SRV _ldap._tcp.dc._msdcs.<DnsDomainName> DcAtSite SRV _ldap._tcp.<SiteName>._sites.dc._msdcs.<DnsDomainName> Rfc1510Kdc SRV _kerberos._tcp.<DnsDomainName> Rfc1510KdcAtSite SRV _kerberos._tcp.<SiteName>._sites.<DnsDomainName> GenericGc SRV _gc._tcp.<DnsForestName> GenericGcAtSite SRV _gc._tcp.<SiteName>._sites.<DnsForestName> Rfc1510UdpKdc SRV _kerberos._udp.<DnsDomainName> Rfc1510Kpwd SRV _kpasswd._tcp.<DnsDomainName> Rfc1510UdpKpwd SRV _kpasswd._udp.<DnsDomainName> If this setting is disabled, DCs configured to perform dynamic registration of DC Locator DNS records register all DC locator DNS resource records. If this setting is not applied to DCs, DCs use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Refresh Interval of the DC Locator DNS Records	At least Microsoft Windows XP Professional or Windows Server	Specifies the Refresh Interval of the domain controller (DC) Locator DNS resource records for DCs to which this setting is applied. These DNS records are dynamically registered by the Net Logon service and are used by the Locator algorithm to locate the DC. This setting may be

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			2003 family	applied only to DCs using dynamic update. DCs configured to perform dynamic registration of the DC Locator DNS resource records periodically reregister their records with DNS servers, even if their records' data has not changed. If authoritative DNS servers are configured to perform scavenging of the stale records, this reregistration is required to instruct the DNS servers configured to automatically remove (scavenge) stale records that these records are current and should be preserved in the database. Warning: If the DNS resource records are registered in zones with scavenging enabled, the value of this setting should never be longer than the Refresh Interval configured for these zones. Setting the Refresh Interval of the DC Locator DNS records to longer than the Refresh Interval of the DNS zones may result in the undesired deletion of DNS resource records. To specify the Refresh Interval of the DC records, click Enabled, and then enter a value larger than 1800. This value specifies the Refresh Interval of the DC records in seconds (for example, the value 3600 is 60 minutes). If this setting is not configured, it is not applied to any DCs, and DCs use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	TTL Set in the DC Locator DNS Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the value for the Time-To-Live (TTL) field in Net Logon registered SRV resource records. These DNS records are dynamically registered by the Net Logon service, and they are used to locate the domain controller (DC). To specify the TTL for DC Locator DNS records, click Enabled, and then enter a value in seconds (for example, the value 900 is 15 minutes). If this setting is not configured, it is not applied to any DCs, and DCs use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Sites Covered by the GC Locator DNS SRV Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the sites for which the global catalogs (GC) should register site-specific GC locator DNS SRV resource records. These records are registered in addition to the site-specific SRV records registered for the site where the GC resides, and records registered by a GC configured to register GC Locator DNS SRV records for those sites without a GC that are closest to it. The GC Locator DNS records and the site-specific SRV records are dynamically registered by the Net Logon service, and they are used to locate the GC. An Active Directory site is one or more well-connected TCP/IP subnets that allow administrators to configure Active Directory access and replication. A GC is a domain controller that contains a partial replica of every domain in Active Directory. To specify the sites covered by the GC Locator DNS SRV records, click Enabled, and enter the sites' names in a space-delimited format. If this setting is not configured, it is not applied to any GCs, and GCs use their local

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Priority Set in the DC Locator DNS SRV Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the Priority field in the SRV resource records registered by domain controllers (DC) to which this setting is applied. These DNS records are dynamically registered by the Net Logon service and are used to locate the DC. The Priority field in the SRV record sets the preference for target hosts (specified in the SRV record's Target field). DNS clients that query for SRV resource records attempt to contact the first reachable host with the lowest priority number listed. To specify the Priority in the DC Locator DNS SRV resource records, click Enabled, and then enter a value. The range of values is 0 to 65535. If this setting is not configured, it is not applied to any DCs, and DCs use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Weight Set in the DC Locator DNS SRV Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the Weight field in the SRV resource records registered by the domain controllers (DC) to which this setting is applied. These DNS records are dynamically registered by the Net Logon service, and they are used to locate the DC. The Weight field in the SRV record can be used in addition to the Priority value to provide a load-balancing mechanism where multiple servers are specified in the SRV records Target field and are all set to the same priority. The probability with which the DNS client randomly selects the target host to be contacted is proportional to the Weight field value in the SRV record. To specify the Weight in the DC Locator DNS SRV records, click Enabled, and then enter a value. The range of values is 0 to 65535. If this setting is not configured, it is not applied to any DCs, and DCs use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Sites Covered by the Application Directory Partition Locator DNS SRV Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the sites for which the domain controllers (DC) housing application directory partition should register the site-specific, application directory partition-specific DC Locator DNS SRV resource records. These records are registered in addition to the site-specific SRV records registered for the site where the DC resides, and records registered by a DC configured to register DC Locator DNS SRV records for those sites without a DC that are closest to it. The application directory partition locator DNS records and the site-specific SRV records are dynamically registered by the Net Logon service, and they are used to locate the application directory partition-specific DC. An Active Directory site is one or more well-connected TCP/IP subnets that allow administrators to configure Active Directory access and replication. To specify the sites covered by the DC Locator application directory partition-specific DNS

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				SRV records, click Enabled, and then enter the site names in a space-delimited format. If this setting is not configured, it is not applied to any DCs, and DCs use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Sites Covered by the DC Locator DNS SRV Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the sites for which the domain controllers (DC) register the site-specific DC Locator DNS SRV resource records. These records are registered in addition to the site-specific SRV records registered for the site where the DC resides, and records registered by a DC configured to register DC Locator DNS SRV records for those sites without a DC that are closest to it. The DC Locator DNS records are dynamically registered by the Net Logon service, and they are used to locate the DC. An Active Directory site is one or more well-connected TCP/IP subnets that allow administrators to configure Active Directory access and replication. To specify the sites covered by the DC Locator DNS SRV records, click Enabled, and then enter the sites names in a space-delimited format. If this setting is not configured, it is not applied to any DCs, and DCs use their local configuration.
COMPUTER	Administrative Templates\System\Net Logon\DC Locator DNS Records	Dynamic Registration of the DC Locator DNS Records	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines if Dynamic Registration of the domain controller (DC) locator DNS resource records is enabled. These DNS records are dynamically registered by the Net Logon service and are used by the Locator algorithm to locate the DC. If you enable this setting, DCs to which this setting is applied dynamically register DC Locator DNS resource records through dynamic DNS update-enabled network connections. If you disable this setting, DCs will not register DC Locator DNS resource records. If this setting is not configured, it is not applied to any DCs, and DCs use their local configuration.
COMPUTER	Administrative Templates\System\Remote Assistance	Solicited Remote Assistance	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether users can solicit another user's assistance via Remote Assistance. If the status is set to Enabled, a user can create a Remote Assistance invitation that a person ("expert") can use at another computer to connect to the user's computer. If given permission, the expert can view the user's screen, mouse, and keyboard activity in real time. The Permit remote control of this computer setting specifies whether a user on a different computer can control this computer. If a user invites an expert to connect to the computer, and gives permission, the expert can take control of this computer. The expert can only make requests to take control during a Remote Assistance session. The user can stop remote control at any time. The Maximum ticket time setting sets a limit on the amount of time that a Remote Assistance invitation can remain open. The Select the method for sending e-mail invitations

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				setting specifies which e-mail standard to use to send Remote Assistance invitations. Depending on your e-mail program, you can use either the Mailto (the invitation recipient connects through an Internet link) or SMAPI (Simple MAPI) standard (the invitation is attached to your e-mail message). Note: The e-mail program must support the selected e-mail standard. If the status is set to Disabled, users cannot request Remote Assistance and this computer cannot be controlled from another computer. Note: An expert can connect to this computer only with the explicit permission of the user. If Remote Assistance is disabled in this setting or set to "Not Configured" and disabled in Control Panel, the "Offer Remote Assistance" setting will also be disabled. If the status is set to Not Configured, users can enable or disable and configure Remote Assistance themselves in System properties in Control Panel. If the status is set to Not Configured, the default maximum time a Remote Assistance invitation can stay open is determined by the Control Panel setting.
COMPUTER	Administrative Templates\System\Remote Assistance	Offer Remote Assistance	At least Microsoft Windows XP Professional or Windows Server 2003 family	Use this setting to determine whether or not a support person or IT admin (who is termed the expert) can offer remote assistance to this computer without a user explicitly requesting it first via a channel, e-mail, or instant messenger. Using this setting, an expert can offer remote assistance to this computer. Note: The expert cannot connect to the computer unannounced or control it without permission from the user. When the expert tries to connect, the user is still given a chance to accept or deny the connection (giving the expert view-only privileges to the user's desktop), and thereafter the user has to explicitly click a button to give the expert the ability to remotely control the desktop, if remote control is enabled. If you enable this setting, you can offer remote assistance. When you configure this setting, you can make two choices: you can select either Allow helpers to only view the computer or Allow helpers to remotely control the computer. In addition to making this selection, when you configure this setting you also specify the list of users or user groups that will be allowed to offer remote assistance. These are known as helpers. To configure the list of helpers, click Show. This opens a new window where you can enter the names of the helpers. Add each user or group one by one. When you enter the name of the helper user or user groups, use the following format: <Domain Name>\<User Name> or <Domain Name>\<Group Name> If you disable or do not configure this policy setting, users or groups cannot offer unsolicited remote assistance to this computer.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\System\Remote Procedure Call	RPC Endpoint Mapper Client Authentication	At least Microsoft Windows XP Professional with SP2	Enabling this setting directs RPC Clients that need to communicate with the Endpoint Mapper Service to authenticate as long as the RPC call for which the endpoint needs to be resolved has authentication information. Disabling this setting will cause RPC Clients that need to communicate with the Endpoint Mapper Service to not authenticate. The Endpoint Mapper Service on machines running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. This means that enabling this setting on a client machine will prevent that client from communicating with a Windows NT4 server using RPC if endpoint resolution is needed. By default, RPC Clients will not use authentication to communicate with the RPC Server Endpoint Mapper Service when asking for the endpoint of a server.
COMPUTER	Administrative Templates\System\Remote Procedure Call	Propagation of extended error information	At least Microsoft Windows XP Professional or Windows Server 2003 family	Directs the RPC Runtime to generate extended error information when an error occurs. Extended error information includes the local time that the error occurred, the RPC version, and the name of the computer on which the error occurred or was propagated. Programs can retrieve the extended error information by using standard Windows application programming interfaces (APIs). If you disable this setting or do not configure it, the RPC Runtime only generates a status code to indicate an error condition. To use this setting, enable the setting, and then select an error response type in the drop-down box. -- Off disables all extended error information for all processes. RPC only generates an error code. -- On with Exceptions enables extended error information but lets you disable it for selected processes. To disable extended error information for a process while this setting is in effect, the command that starts the process must begin with one of the strings in the Extended Error Information Exception field. -- Off with Exceptions disables extended error information but lets you enable it for selected processes. To enable extended error information for a process while this setting is in effect, the command that starts the process must begin with one of the strings in the Extended Error Information Exception field. -- On enables extended error information for all processes. Note: For information about the Extended Error Information Exception field, see the Windows 2000 Platform Software Development Kit (SDK). Note: Extended error information is formatted to be compatible with other operating systems and older Microsoft operating systems, but only newer Microsoft operating systems can read and respond to the information. Note: The default setting, Off, is designed for systems where extended error information is considered to be sensitive, and it should not be made

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				available remotely.
COMPUTER	Administrative Templates\System\Remote Procedure Call	Ignore Delegation Failure	At least Microsoft Windows Server 2003	Directs the RPC Runtime to ignore delegation failures if delegation was asked for. Windows Server 2003 family includes a new delegation model - constrained delegation. In this model the security system does not report that delegation was enabled on a security context when a client connects to a server. Callers of RPC and COM are encouraged to use the RPC_C_QOS_CAPABILITIES_IGNORE_DELEGATE_FAILURE flag, but some applications written for the traditional delegation model may not use this flag and will encounter RPC_S_SEC_PKG_ERROR when connecting to a server that uses constrained delegation. If you disable this setting, do not configure it or set it to Off, the RPC Runtime will generate RPC_S_SEC_PKG_ERROR errors to applications that ask for delegation and connect to servers using constrained delegation. If you configure this setting to On, the RPC Runtime will accept security contexts that do not support delegation as well as security contexts that do support delegation. -- Off directs the RPC Runtime to generate RPC_S_SEC_PKG_ERROR if the client asks for delegation, but the created security context does not support delegation. -- On directs the RPC Runtime to accept security contexts that do not support delegation even if delegation was asked for.
COMPUTER	Administrative Templates\System\Remote Procedure Call	Minimum Idle Connection Timeout for RPC/HTTP connections	At least Microsoft Windows XP Professional with SP1 or Windows Server 2003 family	Directs the RPC Runtime to assume the specified timeout as the idle connection timeout even if the IIS server running the RPC HTTP proxy is configured with a higher timeout. If the IIS server running the RPC HTTP proxy is configured with a lower idle connection timeout, the timeout on the IIS server is used. The timeout is given in seconds. This setting is useful in cases where a network agent like an HTTP proxy or a router uses a lower idle connection timeout than the IIS server running the RPC HTTP proxy. In such cases RPC over HTTP clients may encounter errors because connections will be timed out faster than expected. Using this setting you can force the RPC Runtime and the RPC Proxy to use a lower connection timeout. This setting is only applicable when the RPC Client, the RPC Server and the RPC HTTP Proxy are all running Windows Server 2003 family/Windows XP SP1 or higher versions. If either the RPC Client or the RPC Server or the RPC HTTP Proxy run on an older version of Windows, this setting will be ignored. The minimum allowed value for this setting is 90 seconds. The maximum is 7200 (2 hours). If you disable this setting or do not configure it, the idle connection timeout on the IIS server running the RPC HTTP proxy will be used.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\System\Remote Procedure Call	Restrictions for Unauthenticated RPC clients	At least Microsoft Windows XP Professional with SP2	If you enable this setting, it directs the RPC Runtime on an RPC server to restrict unauthenticated RPC clients connecting to RPC servers running on a machine. A client will be considered an authenticated client if it uses a named pipe to communicate with the server or if it uses RPC Security. RPC Interfaces that have specifically asked to be accessible by unauthenticated clients may be exempt from this restriction, depending on the selected value for this policy. If you disable this setting or do not configure it, the value of Authenticated will be used for Windows XP and the value of None will be used for Server SKUs that support this policy setting. If you enable it, the following values are available: -- None allows all RPC clients to connect to RPC Servers running on the machine on which the policy is applied. -- Authenticated allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy is applied. Interfaces that have asked to be exempt from this restriction will be granted an exemption. -- Authenticated without exceptions allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy is applied. No exceptions are allowed.
COMPUTER	Administrative Templates\System\Remote Procedure Call	RPC Troubleshooting State Information	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether the RPC Runtime maintains RPC state information for the system, and how much information it maintains. Basic state information, which consists only of the most commonly needed state data, is required for troubleshooting RPC problems. If you enable this setting, you can use the drop-down box to determine which systems maintain RPC state information. If the setting is disabled or not configured, RPC uses the Auto2 setting. -- None indicates that the system does not maintain any RPC state information. Note: Because the basic state information required for troubleshooting has a negligible effect on performance and uses only about 4K of memory, this setting is not recommended for most installations. -- Auto1 directs RPC to maintain basic state information only if the computer has at least 64 MB of memory. -- Auto2 directs RPC to maintain basic state information only if the computer has at least 128 MB of memory and is running Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server. -- Server directs RPC to maintain basic state information on the computer, regardless of its capacity. -- Full directs RPC to maintain complete RPC state information on the system, regardless of its capacity. Because this setting can degrade performance, it is recommended for use only while you are investigating

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				an RPC problem. Note: To retrieve the RPC state information from a system that maintains it, you must use a debugging tool.
COMPUTER	Administrative Templates\System\Scripts	Maximum wait time for Group Policy scripts	At least Microsoft Windows 2000	Determines how long the system waits for scripts applied by Group Policy to run. This setting limits the total time allowed for all logon, startup, and shutdown scripts applied by Group Policy to finish running. If the scripts have not finished running when the specified time expires, the system stops script processing and records an error event. By default, the system lets the combined set of scripts run for up to 600 seconds (10 minutes), but you can use this setting to adjust this interval. To use this setting, in the Seconds box, type a number from 1 to 32,000 for the number of seconds you want the system to wait for the set of scripts to finish. To direct the system to wait until the scripts have finished, no matter how long they take, type 0. This interval is particularly important when other system tasks must wait while the scripts complete. By default, each startup script must complete before the next one runs. Also, you can use the Run logon scripts synchronously setting to direct the system to wait for the logon scripts to complete before loading the desktop. An excessively long interval can delay the system and inconvenience users. However, if the interval is too short, prerequisite tasks might not be done, and the system can appear to be ready prematurely.
COMPUTER	Administrative Templates\System\Scripts	Run logon scripts synchronously	At least Microsoft Windows 2000	Directs the system to wait for the logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop. If you enable this setting, Windows Explorer does not start until the logon scripts have finished running. This setting ensures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop. If you disable this setting or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously. This setting appears in the Computer Configuration and User Configuration folders. The setting set in Computer Configuration takes precedence over the setting set in User Configuration.
COMPUTER	Administrative Templates\System\Scripts	Run shutdown scripts visible	At least Microsoft Windows 2000	Displays the instructions in shutdown scripts as they run. Shutdown scripts are batch files of instructions that run when the user restarts the system or shuts it down. By default, the system does not display the instructions in the shutdown script. If you enable this setting, the system displays each instruction in the shutdown script as it runs. The instructions appear in a command window. If you disable this setting or

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				do not configure it, the instructions are suppressed.
COMPUTER	Administrative Templates\System\Scripts	Run startup scripts asynchronously	At least Microsoft Windows 2000	Lets the system run startup scripts simultaneously. Startup scripts are batch files that run before the user is invited to log on. By default, the system waits for each startup script to complete before it runs the next startup script. If you enable this setting, the system does not coordinate the running of startup scripts. As a result, startup scripts can run simultaneously. If you disable this setting or do not configure it, a startup cannot run until the previous script is complete.
COMPUTER	Administrative Templates\System\Scripts	Run startup scripts visible	At least Microsoft Windows 2000	Displays the instructions in startup scripts as they run. Startup scripts are batch files of instructions that run before the user is invited to log on. By default, the system does not display the instructions in the startup script. If you enable this setting, the system displays each instruction in the startup script as it runs. The instructions appear in a command window. This setting is designed for advanced users. If you disable this setting or do not configure it, the instructions are suppressed.
COMPUTER	Administrative Templates\System\System Restore	Turn off Configuration	Only works on Microsoft Windows XP Professional	Allows you to turn off the Configuration Interface for System Restore. System Restore enables users, in the event of a problem, to restore their computers to a previous state without losing personal data files. The behavior of this setting depends on the Turn off System Restore setting. If you enable this setting, the option to configure System Restore on the Configuration Interface disappears. If the Turn off Configuration setting is disabled, the Configuration Interface is still visible, but all System Restore configuration defaults are enforced. If you do not configure it, the Configuration Interface for System Restore remains, and the user has the ability to configure System Restore. Note: This setting is only available in the Home Edition and Professional versions of Windows. Also, see the Turn off System Restore setting. If the Turn off System Restore setting is enabled, the Turn off Configuration setting is not active. If the Turn off System Restore setting is disabled, and Turn off Configuration is not configured, System Restore cannot be turned off locally, but it can be configured. If the Turn off System Restore setting is not configured, and Turn off Configuration is disabled, System Restore can be turned off locally but not configured.
COMPUTER	Administrative Templates\System\System Restore	Turn off System Restore	Only works on Microsoft Windows XP Professional	Determines whether System Restore is turned on or off. System Restore enables users, in the event of a problem, to restore their computers to a previous state without losing personal data files. By default, System Restore is on. If you enable this setting, System Restore is turned off, and the System Restore Wizard and Configuration

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Interface cannot be accessed. If you disable this setting, System Restore is turned on and enforced. It cannot be turned off in the Configuration Interface, but, depending on the Turn off Configuration settings, it may still be configured. The feature is nonfunctional until the system is rebooted. To turn off the Configuration Interface, see the Turn off Configuration setting. If you do not configure it, the system reverts to the default local setting. Important: This setting only refreshes at boot time. Note: This setting is only available in Windows XP Professional. Also, see the Turn off Configuration setting. If the Turn off System Restore setting is disabled or not configured, the Turn off Configuration setting is used to determine whether the Configuration Interface appears.
COMPUTER	Administrative Templates\System\User Profiles	Add the Administrators security group to roaming user profiles	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting adds the Administrator security group to the roaming user profile share. Once an administrator has configured a users' roaming profile, the profile will be created at the user's next login. The profile is created at the location that is specified by the administrator. For the Windows 2000 Professional and Windows XP Professional operating systems, the default file permissions for the newly generated profile are full control, or read and write access for the user, and no file access for the administrators group. By configuring this setting, you can alter this behavior. If you enable this setting, the administrator group is also given full control to the user's profile folder. If you disable or do not configure it, only the user is given full control of their user profile, and the administrators group has no file system access to this folder. Note: If the setting is enabled after the profile is created, the setting has no effect. Note: The setting must be configured on the client computer, not the server, for it to have any effect, because the client computer sets the file share permissions for the roaming profile at creation time. Note: In the default case, administrators have no file access to the user's profile, but they may still take ownership of this folder to grant themselves file permissions. Note: The behavior when this setting is enabled is exactly the same behavior as in Windows NT 4.0.
COMPUTER	Administrative Templates\System\User Profiles	Do not check for user ownership of Roaming Profile Folders	At least Microsoft Windows 2000 Service Pack 4, Microsoft Windows XP Professional Service Pack 1 or Microsoft Windows	This setting disables the more secure default setting for the user's roaming user profile folder. Once an administrator has configured a users' roaming profile, the profile will be created at the user's next login. The profile is created at the location that is specified by the administrator. For Windows 2000 Professional pre-SP4 and Windows XP pre-SP1 operating systems, the default file permissions for the newly generated profile are full control access for the user and no file access

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			Server 2003 family	for the administrators group. No checks are made for the correct permissions if the profile folder already exists. For Windows Server 2003 family, Windows 2000 Professional SP4 and Windows XP SP1, the default behavior is to check the folder for the correct permissions if the profile folder already exists, and not copy files to or from the roaming folder if the permissions are not correct. By configuring this setting, you can alter this behavior. If you enable this setting Windows will not check the permissions for the folder in the case where the folder exists. If you disable or do not configure this setting AND the roaming profile folder exists AND the user or administrators group not the owner of the folder, Windows will NOT copy files to or from the roaming folder. The user will be shown an error message and an entry will be written to the event log. The user's cached profile will be used, or a temporary profile issued if no cached profile exists. Note: The setting must be configured on the client computer not the server for it to have any effect because the client computer sets the file share permissions for the roaming profile at creation time. Note: The behavior when this setting is enabled is exactly the same behavior as in Windows 2000 Professional pre-SP4 and Windows XP Professional
COMPUTER	Administrative Templates\System\User Profiles	Delete cached copies of roaming profiles	At least Microsoft Windows 2000	Determines whether the system saves a copy of a user's roaming profile on the local computer's hard drive when the user logs off. This setting, and related settings in this folder, together describe a strategy for managing user profiles residing on remote servers. In particular, they tell the system how to respond when a remote profile is slow to load. Roaming profiles reside on a network server. By default, when users with roaming profiles log off, the system also saves a copy of their roaming profile on the hard drive of the computer they are using in case the server that stores the roaming profile is unavailable when the user logs on again. The local copy is also used when the remote copy of the roaming user profile is slow to load. If you enable this setting, any local copies of the user's roaming profile are deleted when the user logs off. The roaming profile still remains on the network server that stores it. Important: Do not enable this setting if you are using the slow link detection feature of Windows 2000 Professional and Windows XP Professional. To respond to a slow link, the system requires a local copy of the user's roaming profile.
COMPUTER	Administrative Templates\System\User Profiles	Do not detect slow network connections	At least Microsoft Windows 2000	Disables the slow link detection feature. Slow link detection measures the speed of the connection between a user's computer and the remote server that stores the roaming user profile. When the system detects a

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				slow link, the related settings in this folder tell the system how to respond. If you enable this setting, the system does not detect slow connections or recognize any connections as being slow. As a result, the system does not respond to slow connections to user profiles, and it ignores the settings that tell the system how to respond to a slow connection. If you disable this setting or do not configure it, slow link detection is enabled. The system measures the speed of the connection between the user's computer and profile server. If the connection is slow (as defined by the Slow network connection timeout for user profiles setting), the system applies the other settings set in this folder to determine how to proceed. By default, when the connection is slow, the system loads the local copy of the user profile.
COMPUTER	Administrative Templates\System\User Profiles	Prompt user when slow link is detected	At least Microsoft Windows 2000	Notifies users when their roaming profile is slow to load. The notice lets users decide whether to use a local copy or to wait for the roaming user profile. If you disable this setting or do not configure it, when a roaming user profile is slow to load, the system does not consult the user. Instead, it loads the local copy of the profile. If you have enabled the Wait for remote user profile setting, the system loads the remote copy without consulting the user. This setting and related settings in this folder together define the system's response when roaming user profiles are slow to load. To adjust the time within which the user must respond to this notice, use the Timeout for dialog boxes setting. Important: If the Do not detect slow network connections setting is enabled, this setting is ignored. Also, if the Delete cached copies of roaming profiles setting is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection.
COMPUTER	Administrative Templates\System\User Profiles	Leave Windows Installer and Group Policy Software Installation Data	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Determines whether the system retains a roaming user's Windows Installer and Group Policy based software installation data on their profile deletion. By default User profile deletes all information related to a roaming user (which includes the user's settings, data, Windows Installer related data etc.) when their profile is deleted. As a result, the next time a roaming user whose profile was previously deleted on that client logs on, they will need to reinstall all apps published via policy at logon increasing logon time. You can use this policy to change this behavior. If you enable this setting, Windows will not delete Windows Installer or Group Policy software installation data for roaming users when profiles are deleted from the machine. This will improve the performance of Group Policy based Software Installation during user logon when a user profile is deleted and that user subsequently logs on

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				to the machine. If you disable or do not configure this policy, Windows will delete the entire profile for roaming users, including the Windows Installer and Group Policy software installation data when those profiles are deleted. Note: If this policy is enabled for a machine, local administrator action is required to remove the Windows Installer or Group Poliy software installation data stored in the registry and file system of roaming users' profiles on the machine.
COMPUTER	Administrative Templates\System\User Profiles	Only allow local user profiles	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting determines if roaming user profiles are available on a particular computer. By default, when roaming profile users log on to a computer, their roaming profile is copied down to the local computer. If they have already logged on to this computer in the past, the roaming profile is merged with the local profile. Similarly, when the user logs off this computer, the local copy of their profile, including any changes they have made, is merged with the server copy of their profile. Using the setting, you can prevent users configured to use roaming profiles from receiving their profile on a specific computer. If you enable this setting, the following occurs on the affected computer: At first logon, the user receives a new local profile, rather than the roaming profile. At logoff, changes are saved to the local profile. All subsequent logons use the local profile. If you disable this setting or do not configure it, the default behavior occurs, as indicated above. If you enable both the Prevent Roaming Profile changes from propagating to the server setting and the Only allow local user profiles setting, roaming profiles are disabled. Note: This setting only affects roaming profile users.
COMPUTER	Administrative Templates\System\User Profiles	Timeout for dialog boxes	At least Microsoft Windows 2000	Determines how long the system waits for a user response before it uses a default value. The default value is applied when the user does not respond to messages explaining that any of the following events has occurred: -- The system detects a slow connection between the user's computer and the server that stores users' roaming user profiles. -- The system cannot access users' server-based profiles when users log on or off. -- Users' local profiles are newer than their server-based profiles. You can use this setting to override the system's default value of 30 seconds. To use this setting, type a decimal number between 0 and 600 for the length of the interval.
COMPUTER	Administrative Templates\System\User Profiles	Log users off when roaming profile fails	At least Microsoft Windows 2000	Logs a user off automatically when the system cannot load the user's roaming user profile. This setting is used when the system cannot find the roaming user profile or the profile contains errors which prevent it from loading correctly. If you disable this setting or do not configure it,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				when the roaming profile fails, the system loads a local copy of the roaming user profile, if one is available. Otherwise, the system loads the default user profile (stored in %Systemroot%\Documents and Settings\Default User). Also, see the Delete cached copies of roaming profiles setting.
COMPUTER	Administrative Templates\System\User Profiles	Maximum retries to unload and update user profile	At least Microsoft Windows 2000	Determines how many times the system tries to unload and update the registry portion of a user profile. When the number of trials specified by this setting is exhausted, the system stops trying. As a result, the user profile might not be current, and local and roaming user profiles might not match. When a user logs off of the computer, the system unloads the user-specific section of the registry (HKEY_CURRENT_USER) into a file (NTUSER.DAT) and updates it. However, if another program or service is reading or editing the registry, the system cannot unload it. The system tries repeatedly (at a rate of once per second) to unload and update the registry settings. By default, the system repeats its periodic attempts 60 times (over the course of one minute). If you enable this setting, you can adjust the number of times the system tries to unload and update the user's registry settings. (You cannot adjust the retry rate.) If you disable this setting or do not configure it, the system repeats its attempt 60 times. If you set the number of retries to 0, the system tries just once to unload and update the user's registry settings. It does not try again. Note: This setting is particularly important to servers running Terminal Services. Because Terminal Services edits the users' registry settings when they log off, the system's first few attempts to unload the user settings are more likely to fail. This setting does not affect the system's attempts to update the files in the user profile. Tip: Consider increasing the number of retries specified in this setting if there are many user profiles stored in the computer's memory. This indicates that the system has not been able to unload the profile. Also, check the Application Log in Event Viewer for events generated by Userenv. The system records an event whenever it tries to unload the registry portion of the user profile. The system also records an event when it fails to update the files in a user profile.
COMPUTER	Administrative Templates\System\User Profiles	Prevent Roaming Profile changes from propagating to the server	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting determines if the changes a user makes to their roaming profile are merged with the server copy of their profile. By default, when a roaming profile user logs on to a computer, their roaming profile is copied down to the local computer. If they have already logged on to this computer in the past, the roaming profile is merged with the local profile. Similiarly, when the user logs off this computer, the local copy of their

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				profile, including any changes they have made, is merged with the server copy of their profile. Using the setting, you can prevent changes made to a roaming profile on a particular computer from being persisted. If you enable this setting, the following occurs on the affected computer: At login, the user receives their roaming profile. But, any changes a user makes to their profile will not be merged to their roaming profile when they log off. If this setting is disabled or not configured, the default behavior occurs, as indicated above. Note: This setting only affects roaming profile users.
COMPUTER	Administrative Templates\System\User Profiles	Wait for remote user profile	At least Microsoft Windows 2000	Directs the system to wait for the remote copy of the roaming user profile to load, even when loading is slow. Also, the system waits for the remote copy when the user is notified about a slow connection, but does not respond in the time allowed. This setting and related settings in this folder together define the system's response when roaming user profiles are slow to load. If you disable this setting or do not configure it, then when a remote profile is slow to load, the system loads the local copy of the roaming user profile. The local copy is also used when the user is consulted (as set in the Prompt user when slow link is detected setting), but does not respond in the time allowed (as set in the Timeout for dialog boxes setting). Waiting for the remote profile is appropriate when users move between computers frequently and the local copy of their profile is not always current. Using the local copy is desirable when quick logging on is a priority. Important: If the Do not detect slow network connections setting is enabled, this setting is ignored. Also, if the Delete cached copies of roaming profiles setting is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection.
COMPUTER	Administrative Templates\System\User Profiles	Slow network connection timeout for user profiles	At least Microsoft Windows 2000	Defines a slow connection for roaming user profiles. If the server on which the user's roaming user profile resides takes longer to respond than the thresholds set by this setting allow, then the system considers the connection to the profile to be slow. This setting and related settings in this folder together define the system's response when roaming user profiles are slow to load. This setting establishes thresholds for two tests. For computers connected to IP networks, the system measures the rate at which the remote server returns data in response to an IP ping message. To set a threshold for this test, in the Connection speed box, type a decimal number between 0 and 4,294,967,200, representing the minimum acceptable transfer rate in kilobits per second. By default, if the server returns fewer than 500 kilobits of data per second, it is considered to be slow. For non-IP computers, the system measures the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				responsiveness of the remote server's file system. To set a threshold for this test, in the Time box, type a decimal number between 0 and 20,000, representing the maximum acceptable delay, in milliseconds. By default, if the server's file system does not respond within 120 milliseconds, it is considered to be slow. Consider increasing this value for clients using DHCP Service-assigned addresses or for computers accessing profiles across dial-up connections. Important: If the Do not detect slow network connections setting is enabled, this setting is ignored. Also, if the Delete cached copies of roaming profiles setting is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection.
COMPUTER	Administrative Templates\System\Windows File Protection	Specify Windows File Protection cache location	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies an alternate location for the Windows File Protection cache. To enable this setting, enter the fully qualified local path to the new location in the Cache file path box. If you disable this setting or do not configure it, the Windows File Protection cache is located in the %Systemroot%\System32\Dllcache directory. Note: Do not put the cache on a network shared directory.
COMPUTER	Administrative Templates\System\Windows File Protection	Limit Windows File Protection cache size	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies the maximum amount of disk space that can be used for the Windows File Protection file cache. Windows File Protection adds protected files to the cache until the cache content reaches the quota. If the quota is greater than 50 MB, Windows File Protection adds other important Windows XP files to the cache until the cache size reaches the quota. To enable this setting, enter the maximum amount of disk space to be used (in MB). To indicate that the cache size is unlimited, select 4294967295 as the maximum amount of disk space. If you disable this setting or do not configure it, the default value is set to 50 MB on Windows XP Professional and is unlimited (4294967295 MB) on Windows Server 2003.
COMPUTER	Administrative Templates\System\Windows File Protection	Set Windows File Protection scanning	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines when Windows File Protection scans protected files. This setting directs Windows File Protection to enumerate and scan all system files for changes. You can use this setting to direct Windows File Protection to scan files more often. By default, files are scanned only during setup. To use this setting, enable the setting, and then select a rate from the Scanning Frequency box. -- Do not scan during startup, the default, scans files only during setup. -- Scan during startup also scans files each time you start Windows XP. This setting delays each startup. Note: This setting affects file scanning only. It does not affect the standard background file change detection that Windows File

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Protection provides.
COMPUTER	Administrative Templates\System\Windows File Protection	Hide the file scan progress window	At least Microsoft Windows XP Professional or Windows Server 2003 family	Hides the file scan progress window. This window provides status information to sophisticated users, but it might confuse novices. If you enable this setting, the file scan window does not appear during file scanning. If you disable this setting or do not configure it, the file scan progress window appears.
COMPUTER	Administrative Templates\System\Windows Time Service	Global Configuration Settings	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies a set of parameters for all time providers installed on your system. There are two sets of parameters: clock discipline parameters, which control how the Windows Time Service processes the time samples it receives from providers, and general parameters. The general parameters allow you to configure the following: whether the time service is discoverable through DsGetDcName, the verbosity of event logging, the reliability of the local CMOS clock, and the minimum and maximum suggested polling intervals for time providers.
COMPUTER	Administrative Templates\System\Windows Time Service\Time Providers	Configure Windows NTP Client	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether the Windows NTP Client synchronizes time from the domain hierarchy or a manually configured NTP server. Specifies whether the client can synchronize time from a source outside its site, how long the Windows NTP Client waits before attempting to re-resolve an unsuccessfully resolved NTP server name, and the verbosity of the NTP Client's event logging.
COMPUTER	Administrative Templates\System\Windows Time Service\Time Providers	Enable Windows NTP Client	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You may want to disable this service if you decide to use a third-party time provider.
COMPUTER	Administrative Templates\System\Windows Time Service\Time Providers	Enable Windows NTP Server	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether the Windows NTP Server is enabled. Enabling the Windows NTP Server allows your computer to service NTP requests from other machines.
COMPUTER	Administrative Templates\Temporary Internet Files (Machine)	Temporary Internet Files (Machine)		
COMPUTER	Administrative Templates\Temporary Internet Files (Machine)	User Profiles		
COMPUTER	Administrative	Windows.adm		The settings in windows.adm are intended for use with Windows 95,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Templates\Unsupported Administrative Templates			Windows 98 and Windows NT 4.0 clients. Their use in Group Policy is not supported.
COMPUTER	Administrative Templates\Unsupported Administrative Templates	Common.adm		The settings in common.adm are intended for use with Windows 95, Windows 98 and Windows NT 4.0 clients. Their use in Group Policy is not supported.
COMPUTER	Administrative Templates\Unsupported Administrative Templates	Winnt.adm		The settings in winnt.adm are intended for use with Windows 95, Windows 98 and Windows NT 4.0 clients. Their use in Group Policy is not supported.
COMPUTER	Administrative Templates\Windows 95 Network\Access control	User-level access control		
COMPUTER	Administrative Templates\Windows 95 Network\Dial-up networking	Disable dial-in		
COMPUTER	Administrative Templates\Windows 95 Network\File and printer sharing	Disable file sharing		
COMPUTER	Administrative Templates\Windows 95 Network\File and printer sharing	Disable printer sharing		
COMPUTER	Administrative Templates\Windows 95 Network\File and Printer Sharing for NetWare Networks	Disable SAP advertising		
COMPUTER	Administrative Templates\Windows 95 Network\Logon	Allow logon without name or password		
COMPUTER	Administrative Templates\Windows 95 Network\Logon	Custom logon banner		
COMPUTER	Administrative Templates\Windows 95 Network\Logon	Require validation by network for Windows access		
COMPUTER	Administrative Templates\Windows 95 Network\Microsoft Client for Windows networks	Alternate workgroup		
COMPUTER	Administrative Templates\Windows 95 Network\Microsoft Client for Windows networks	Log on to Windows NT		

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Windows 95 Network\Microsoft Client for Windows networks	Workgroup		
COMPUTER	Administrative Templates\Windows 95 Network\Microsoft Client Service for NetWare networks	Disable automatic NetWare login		
COMPUTER	Administrative Templates\Windows 95 Network\Microsoft Client Service for NetWare networks	Preferred server		
COMPUTER	Administrative Templates\Windows 95 Network\Microsoft Client Service for NetWare networks	Search mode		
COMPUTER	Administrative Templates\Windows 95 Network\Microsoft Client Service for NetWare networks	Support long filenames		
COMPUTER	Administrative Templates\Windows 95 Network\Passwords	Disable password caching		
COMPUTER	Administrative Templates\Windows 95 Network\Passwords	Hide share passwords with asterisks		
COMPUTER	Administrative Templates\Windows 95 Network\Passwords	Min Windows password length		
COMPUTER	Administrative Templates\Windows 95 Network\Passwords	Require alphanumeric Windows password		
COMPUTER	Administrative Templates\Windows 95 System\Network paths	Network path for Windows setup		
COMPUTER	Administrative Templates\Windows 95 System\Network paths	Network path for Windows tour		
COMPUTER	Administrative Templates\Windows 95 System\Profiles	Enable user profiles		
COMPUTER	Administrative Templates\Windows 95 System\SNMP	Internet MIB (RFC1156)		
COMPUTER	Administrative Templates\Windows	Prevent access to 16-bit	At least Microsoft	Specifies whether to prevent the MS-DOS subsystem (ntvdm.exe) from

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Application Compatibility	applications	Windows Server 2003	running on this computer. This setting affects the launching of 16-bit applications in the operating system. By default, the MS-DOS subsystem runs for all users on this computer. You can use this setting to turn off the MS-DOS subsystem, which will reduce resource usage and prevent users from running 16-bit applications. To run any 16-bit application or any application with 16-bit components, ntvdm.exe must be allowed to run. The MS-DOS subsystem starts when the first 16-bit application is launched. While the MS-DOS subsystem is running, any subsequent 16-bit applications launch faster, but overall resource usage on the system is increased. If the status is set to Enabled, ntvdm.exe is prevented from running, which then prevents any 16-bit applications from running. In addition, any 32-bit applications with 16-bit installers or other 16-bit components cannot run. If the status is set to Disabled, the default setting applies and the MS-DOS subsystem runs for all users on this computer. If the status is set to Not Configured, the default applies and ntvdm.exe runs for all users. However, if an administrator sets the registry DWORD value HKLM\System\CurrentControlSet\Control\WOW\DisallowedPolicyDefault to 1, the default changes to prevent all 16-bit applications from running. Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
COMPUTER	Administrative Templates\Windows Components\Application Compatibility	Remove Program Compatibility Property Page	At least Microsoft Windows Server 2003	This policy controls the visibility of the Program Compatibility property page shell extension. This shell extension is visible on the property context-menu of any program shortcut or executable file. The compatibility property page displays a list of options that can be selected and applied to the application to resolve the most common issues affecting legacy applications. Enabling this policy setting removes the property page from the context-menus, but does not affect previous compatibility settings applied to application using this interface.
COMPUTER	Administrative Templates\Windows Components\Application Compatibility	Turn On Application Help Log Events	At least Microsoft Windows Server 2003	The Application Help features blocks known incompatible applications and displays a dialog to the end-user regarding the problem. This dialog may include links to the web for downloading updates for the application, manual steps to work around an issue, or basic incompatibility information. Enabling this option turns on logging of Application Help events to the Application log.
COMPUTER	Administrative Templates\Windows Components\Application	Turn Off Application Compatibility Engine	At least Microsoft Windows Server	This policy controls the state of the application compatibility engine in the system. The engine is part of the loader and looks through a

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Compatibility		2003	compatibility database every time an application is started on the system. If a match for the application is found it provides either run-time solutions or compatibility fixes, or displays an Application Help message if the application has a know problem. Turning off the application compatibility engine will boost system performance. However, this will degrade the compatibility of many popular legacy applications, and will not block known incompatible applications from installing. (For Instance: This may result in a blue screen if an old anti-virus application is installed.) This option is useful to server administrators who require faster performance and are aware of the compatibility of the applications they are using. It is particularly useful for a web server where applications may be launched several hundred times a second, and the performance of the loader is essential.
COMPUTER	Administrative Templates\Windows Components\Application Compatibility	Turn Off Program Compatibility Wizard	At least Microsoft Windows Server 2003	This policy controls the state of the Program Compatibility Wizard. When enabled, this policy disables the start page of the wizard in the Help and Support Center, and in the Start Menu. These entry points will still exist but the first page of the Help and Support Center wizard will let the user know that this option has been disabled.
COMPUTER	Administrative Templates\Windows Components\Event Viewer	Events.asp program	At least Microsoft Windows XP Professional with SP2	This is the program that will be invoked when the user clicks the events.asp link.
COMPUTER	Administrative Templates\Windows Components\Event Viewer	Events.asp program command line parameters	At least Microsoft Windows XP Professional with SP2	This specifies the command line parameters that will be passed to the events.asp program
COMPUTER	Administrative Templates\Windows Components\Event Viewer	Events.asp URL	At least Microsoft Windows XP Professional with SP2	This is the URL that will be passed to the Description area in the Event Properties dialog box. Change this value if you want to use a different Web server to handle event information requests.
COMPUTER	Administrative Templates\Windows Components\Internet Explorer	Disable Automatic Install of Internet Explorer components	at least Internet Explorer v5.01	Prevents Internet Explorer from automatically installing components. If you enable this policy, it prevents Internet Explorer from downloading a component when users browse to a Web site that needs that component. If you disable this policy or do not configure it, users will be prompted to download and install a component when visiting a Web site that uses that component. This policy is intended to help the administrator control which components the user installs.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Windows Components\Internet Explorer	Disable showing the splash screen	at least Internet Explorer v5.01	Prevents the Internet Explorer splash screen from appearing when users start the browser. If you enable this policy, the splash screen, which displays the program name, licensing, and copyright information, is not displayed. If you disable this policy or do not configure it, the splash screen will be displayed when users start their browsers.
COMPUTER	Administrative Templates\Windows Components\Internet Explorer	Disable Periodic Check for Internet Explorer software updates	at least Internet Explorer v5.01	Prevents Internet Explorer from checking whether a new version of the browser is available. If you enable this policy, it prevents Internet Explorer from checking to see whether it is the latest available browser version and notifying users if a new version is available. If you disable this policy or do not configure it, Internet Explorer checks every 30 days by default, and then notifies users if a new version is available. This policy is intended to help the administrator maintain version control for Internet Explorer by preventing users from being notified about new versions of the browser.
COMPUTER	Administrative Templates\Windows Components\Internet Explorer	Security Zones: Use only machine settings	at least Internet Explorer v5.01	Applies security zone information to all users of the same computer. A security zone is a group of Web sites with the same security level. If you enable this policy, changes that the user makes to a security zone will apply to all users of that computer. If you disable this policy or do not configure it, users of the same computer can establish their own security zone settings. This policy is intended to ensure that security zone settings apply uniformly to the same computer and do not vary from user to user. Also, see the Security zones: Do not allow users to change policies policy.
COMPUTER	Administrative Templates\Windows Components\Internet Explorer	Security Zones: Do not allow users to change policies	at least Internet Explorer v5.01	Prevents users from changing security zone settings. A security zone is a group of Web sites with the same security level. If you enable this policy, the Custom Level button and security-level slider on the Security tab in the Internet Options dialog box are disabled. If you disable this policy or do not configure it, users can change the settings for security zones. This policy prevents users from changing security zone settings established by the administrator. Note: The Disable the Security page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Security tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored. Also, see the Security zones: Use only machine settings policy.
COMPUTER	Administrative Templates\Windows Components\Internet Explorer	Security Zones: Do not allow users to	at least Internet Explorer v5.01	Prevents users from adding or removing sites from security zones. A security zone is a group of Web sites with the same security level. If you

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
		add/delete sites		enable this policy, the site management settings for security zones are disabled. (To see the site management settings for security zones, in the Internet Options dialog box, click the Security tab, and then click the Sites button.) If you disable this policy or do not configure it, users can add Web sites to or remove sites from the Trusted Sites and Restricted Sites zones, and alter settings for the Local Intranet zone. This policy prevents users from changing site management settings for security zones established by the administrator. Note: The Disable the Security page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Security tab from the interface, takes precedence over this policy. If it is enabled, this policy is ignored. Also, see the Security zones: Use only machine settings policy.
COMPUTER	Administrative Templates\Windows Components\Internet Explorer	Disable software update shell notifications on program launch	at least Internet Explorer v5.01	Specifies that programs using the Microsoft Software Distribution Channel will not notify users when they install new components. The Software Distribution Channel is a means of updating software dynamically on users' computers by using Open Software Distribution (.osd) technologies. If you enable this policy, users will not be notified if their programs are updated using Software Distribution Channels. If you disable this policy or do not configure it, users will be notified before their programs are updated. This policy is intended for administrators who want to use Software Distribution Channels to update their users' programs without user intervention.
COMPUTER	Administrative Templates\Windows Components\Internet Explorer	Make proxy settings per-machine (rather than per-user)	at least Internet Explorer v5.01	Applies proxy settings to all users of the same computer. If you enable this policy, users cannot set user-specific proxy settings. They must use the zones created for all users of the computer. If you disable this policy or do not configure it, users of the same computer can establish their own proxy settings. This policy is intended to ensure that proxy settings apply uniformly to the same computer and do not vary from user to user.
COMPUTER	Administrative Templates\Windows Components\Internet Information Services	Prevent IIS installation	At least Microsoft Windows Server 2003	When you enable this setting, it will prevent Internet Information Services (IIS) from being installed, and you will not be able to install Windows components or applications that require IIS. Users installing Windows components or applications that require IIS may not receive a warning that IIS cannot be installed because of this Group Policy. Enabling this setting will not have any effect on IIS if IIS is already installed on the computer.
COMPUTER	Administrative Templates\Windows	Disable remote Desktop		Disables the remote desktop sharing feature of NetMeeting. Users will

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\NetMeeting	Sharing		not be able to set it up or use it for controlling their computers remotely.
COMPUTER	Administrative Templates\Windows Components\Security Center	Turn on Security Center (Domain PCs only)	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether the Security Center is turned on or off on users' computers that are joined to an Active Directory domain. When the Security Center is turned on, it monitors essential security settings (firewall, antivirus, and Automatic Updates), and notifies users when their computers might be at risk. The Security Center Control Panel category view also contains a status section, where users can get recommendations for helping to increase their computer's security. When the Security Center is turned off, neither the notifications nor the Security Center status section are displayed. Note that the Security Center cannot be turned off for computers that are NOT joined to a Windows domain, and this policy setting will have no effect in that case. If this setting is Not Configured, the Security Center is turned off for domain members. When this policy setting is Enabled, the Security Center is turned on for all users. Note that the Security Center will not become available following a change to this policy setting until after a computer is restarted. When this policy is Disabled, the Security Center is turned off for domain members.
COMPUTER	Administrative Templates\Windows Components\Task Scheduler	Prohibit Browse	At least Microsoft Windows 2000	Limits newly scheduled to items on the user's Start menu, and prevents the user from changing the scheduled program for existing tasks. This setting removes the Browse button from the Schedule Task Wizard and from the Task tab of the properties dialog box for a task. Also, users cannot edit the Run box or the Start in box that determine the program and path for a task. As a result, when users create a task, they must select a program from the list in the Scheduled Task Wizard, which displays only the tasks that appear on the Start menu and its submenus. Once a task is created, users cannot change the program a task runs. Important: This setting does not prevent users from creating a new task by pasting or dragging any program into the Scheduled Tasks folder. To prevent this action, use the Prohibit Drag-and-Drop setting. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
COMPUTER	Administrative Templates\Windows Components\Task Scheduler	Hide Advanced Properties Checkbox in Add Scheduled Task Wizard	At least Microsoft Windows 2000	This setting removes the Open advanced properties for this task when I click Finish checkbox from the last page of the Scheduled Task Wizard. This policy is only designed to simplify task creation for beginning users. The checkbox, when checked, instructs Task Scheduler to automatically open the newly created task's property sheet upon completion of the Add

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Scheduled Task wizard. The task's property sheet allows users to change task characteristics such as: the program the task runs, details of its schedule, idle time and power management settings, and its security context. Beginning users will often not be interested or confused by having the property sheet displayed automatically. Note that the checkbox is not checked by default even if this setting is Disabled or Not Configured. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
COMPUTER	Administrative Templates\Windows Components\Task Scheduler	Prohibit Drag-and-Drop	At least Microsoft Windows 2000	Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder. This setting disables the Cut, Copy, Paste, and Paste shortcut items on the context menu and the Edit menu in Scheduled Tasks. It also disables the drag-and-drop features of the Scheduled Tasks folder. As a result, users cannot add new scheduled tasks by dragging, moving, or copying a document or program into the Scheduled tasks folder. This setting does not prevent users from using other methods to create new tasks, and it does not prevent users from deleting tasks. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
COMPUTER	Administrative Templates\Windows Components\Task Scheduler	Prevent Task Run or End	At least Microsoft Windows 2000	Prevents users from starting and stopping tasks manually. This setting removes the Run and End Task items from the context menu that appears when you right-click a task. As a result, users cannot start tasks manually or force tasks to end before they are finished. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
COMPUTER	Administrative Templates\Windows Components\Task Scheduler	Hide Property Pages	At least Microsoft Windows 2000	Prevents users from viewing and changing the properties of an existing task. This setting removes the Properties item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview. This setting prevents users from viewing and changing characteristics such as the program the task runs, its schedule details, idle time and power management settings, and its security context. Note: This setting appears in the Computer Configuration and User

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: This setting affects existing tasks only. To prevent users from changing the properties of newly created tasks, use the Remove Advanced Menu setting.
COMPUTER	Administrative Templates\Windows Components\Task Scheduler	Prohibit New Task Creation	At least Microsoft Windows 2000	Prevents users from creating new tasks. This setting removes the Add Scheduled Task item that starts the New Task Wizard. Also, the system does not respond when users try to move, paste, or drag programs or documents into the Scheduled Tasks folder. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Important: This setting does not prevent administrators of a computer from using At.exe to create new tasks or prevent administrators from submitting tasks from remote computers.
COMPUTER	Administrative Templates\Windows Components\Task Scheduler	Prohibit Task Deletion	At least Microsoft Windows 2000	Prevents users from deleting tasks from the Scheduled Tasks folder. This setting removes the Delete command from the Edit menu in the Scheduled Tasks folder and from the menu that appears when you right-click a task. Also, the system does not respond when users try to cut or drag a task from the Scheduled Tasks folder. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Important: This setting does not prevent administrators of a computer from using At.exe to delete tasks.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Automatic reconnection	At least Microsoft Windows XP Terminal Services	Specifies whether to allow Remote Desktop Connection clients to automatically reconnect to Terminal Services sessions if their network link is temporarily lost. By default, a maximum of twenty reconnection attempts are made at five second intervals. If the status is set to Enabled, automatic reconnection is attempted for all clients running Remote Desktop Connection whenever their network connection is lost. If the status is set to Disabled, automatic reconnection of clients is prohibited. If the status is set to Not Configured, automatic reconnection is not specified at the Group Policy level. However, users can configure automatic reconnection using the Reconnect if connection is dropped checkbox on the Experience tab in Remote Desktop Connection.
COMPUTER	Administrative Templates\Windows	Limit maximum color	At least Microsoft Windows XP	Specifies the maximum color resolution (color depth) for Terminal Services connections. You can use this setting to set a limit on the color

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Terminal Services	depth	Terminal Services	depth of any connection to a terminal server or Remote Desktop. Limiting the color depth can improve connection performance, particularly over slow links, and reduce server load. To use this setting, select the setting from the Color Depth list. To specify that all connections should be at the highest color depth supported by the client, select Client Compatible. The current maximum color depth for Terminal Server and Remote Desktop connections is 24 bit. The default maximum color depth is set to 16 bit for Terminal Server and Remote Desktop on Windows XP Professional. If the status is set to Enabled, the specified color depth is the maximum depth for a user's Terminal Services connection. The actual color depth for the connection is determined by the color support available on the client computer. If the status is set to Disabled or Not Configured, the color depth for connections is the default value for the Terminal Services mode/Windows version running on the computer, unless a lower level is specified by the user at the time of connection.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Allow users to connect remotely using Terminal Services	At least Microsoft Windows XP Terminal Services	Specifies whether to allow users to connect remotely using Terminal Services. You can use this setting to configure Terminal Services remote access for the target computers. If the status is set to Enabled, users can connect to the target computers remotely using Terminal Services. You can limit the number of users who can connect simultaneously by configuring the Limit number of connections setting or the Maximum Connections option on the Network Adapter tab in the Terminal Services Configuration tool. If the status is set to Disabled, the target computers maintain current connections, but will not accept any new incoming connections. If the status is set to Not Configured, Terminal Services uses the Allow users to connect remotely to your computer option on the target computer to determine whether remote connection is allowed. This option is found on the Remote tab in System Properties.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Enforce Removal of Remote Desktop Wallpaper	At least Microsoft Windows XP Terminal Services	Specifies whether desktop wallpaper is displayed to remote clients connecting via Terminal Services. You can use this setting to enforce the removal of wallpaper during a remote session. By default, Windows XP Professional displays wallpaper to remote clients connecting through Remote Desktop, depending on the client configuration (see the Experience tab in the Remote Desktop Connection options for more information). Servers running Windows Server 2003 do not display wallpaper by default to remote sessions. If the status is set to Enabled, wallpaper never appears to a Terminal Services client. If the status is

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				set to Disabled, wallpaper might appear to a Terminal Services client, depending on the client configuration. If the status is set to Not Configured, the default behavior applies.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Deny log off of an administrator logged in to the console session	At least Microsoft Windows Server 2003	Specifies whether to allow an administrator attempting to connect to the console of a server to log off an administrator currently logged on to the console. The console session is also known as Session 0. Console access can be obtained by using the /console switch from Remote Desktop Connection in the computer field name or from the command line. If the status is set to Enabled, logging off the connected administrator is not allowed. If the status is set to Disabled, logging off the connected administrator is allowed. If the status is set to Not Configured, logging off the connected administrator is allowed but can be changed at the local computer policy level. This policy is useful when the currently connected administrator does not want to be logged off by another administrator. If the connected administrator is logged off, any data not previously saved is lost.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Keep-Alive Connections	At least Microsoft Windows XP Terminal Services	Specifies whether persistent connections are allowed. After a terminal server client loses the connection to a terminal server, the session on the terminal server might remain active instead of changing to a disconnected state, even if the client is physically disconnected from the terminal server. If the client logs on to the same terminal server again, a new session might be established (if Terminal Services is configured to allow multiple sessions), and the original session might still be active. You can use this setting to enable keep-alive connections and ensure that the session state is consistent with the client state. By default, keep-alive connections are disabled. To configure keep-alive connections, enable the setting and set the Keep-alive interval. The keep-alive interval determines how often, in minutes, the server checks the session state. If the status is set to Enabled, keep-alive connections are enabled. If the status is set to Disabled, the default behavior is enforced. If the status is set to Not Configured, keep-alive connections remain disabled by default.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Use these License Servers	At least Microsoft Windows Server 2003 with SP1	Determines whether to override the automatic discovery of the Terminal Server License Server. You can select which license servers are to be used. Not configured: If this setting is not configured, you can use the Terminal Services Configuration snap-in or the Windows Components Wizard to select which license servers will be used. Enabled: If you enable this setting, you can add the license server names in the field

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				below. Any computer that this policy is applied to will use the license servers you have specified. Disabled: If you disable this policy for any computer that this policy is applied to, the license servers will be selected automatically and you will not be able to specifically select which license server to use. Note: The Terminal Server License Server must run on Windows Server 2003.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Use these License Servers	At least Microsoft Windows Server 2003 with SP1	Determines whether to override the automatic discovery of the Terminal Server License Server. You can select which license servers are to be used. Not configured: If this setting is not configured, you can use the Terminal Services Configuration snap-in or the Windows Components Wizard to select which license servers will be used. Enabled: If you enable this setting, you can add the license server names in the field below. Any computer that this policy is applied to will use the license servers you have specified. Disabled: If you disable this policy for any computer that this policy is applied to, the license servers will be selected automatically and you will not be able to specifically select which license server to use. Note: The Terminal Server License Server must run on Windows Server 2003.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Limit number of connections	At least Microsoft Windows XP Terminal Services	Specifies whether Terminal Services limits the number of simultaneous connections to the server. You can use this setting to restrict the number of remote sessions that can be active on a server. If this number is exceeded, addtional users who try to connect receive an error message telling them that the server is busy and to try again later. Restricting the number of sessions improves performance because fewer sessions are demanding system resources. By default, terminal servers allow an unlimited number of remote sessions, and Remote Desktop for Administration allows two remote sessions. To use this setting, enter the number of connections you want to specify as the maximum for the server. To specify an unlimited number of connections, type 999999. If the status is set to Enabled, the maximum number of connections is limited to the specified number consistent with the version of Windows and the mode of Terminal Services running on the server. If the status is set to Disabled or Not Configured, limits to the number of connections are not enforced at the Group Policy level. Note: This setting is designed to be used on terminal servers (that is, on servers running Windows with Terminal Server installed).
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Remove Disconnect option from Shut Down	At least Microsoft Windows 2000	Specifies whether to remove the Disconnect option from the Shut Down Windows dialog box on Terminal Services clients. You can use this

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
		dialog	Terminal Services	setting to prevent users from using this familiar method to disconnect their client from a terminal server. If the status is set to Enabled, Disconnect does not appear as an option in the drop-down list in the Shut Down Windows dialog box. If the status is set to Disabled, Disconnect always appears as an option in the drop-down list. If the status is set to Not Configured, the appearance of the Disconnect option is not specified at the Group Policy level. Note: This setting affects the Shut Down Windows dialog box only. It does not prevent users from using other methods of disconnecting from a Terminal Services session. This setting also does not prevent disconnected sessions at the server. See the Do not allow disconnected sessions setting to configure this behavior.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Remove Windows Security item from Start menu	At least Microsoft Windows 2000 Terminal Services	Specifies whether to remove the Windows Security item from the Settings menu on Terminal Services clients. You can use this setting to prevent inexperienced users from logging off from Terminal Services inadvertently. If the status is set to Enabled, Windows Security does not appear in Settings on the Start menu. As a result, users must type a security attention sequence, such as CTRL+ALT+END, to open the Windows Security dialog box on the client computer. If the status is set to Disabled or Not Configured, Windows Security remains in the Settings menu.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Sets rules for remote control of Terminal Services user sessions	At least Microsoft Windows XP Terminal Services	Specifies the level of remote control permitted in a Terminal Services session. Remote control can be established with or without the session user's permission. You can use this setting to select one of two levels of remote control: View Session permits the remote control user to watch a session, Full Control permits the remote control user to interact with the session. If the status is set to Enabled, administrators can remotely interact with a user's Terminal Services session according to the specified rules. To set these rules, select the desired level of control and permission in the Options list. To disable remote control, select No remote control allowed. If the status is set to Disabled or Not Configured, remote control rules are determined by the server administrator using the Terminal Services Configuration tool (tscc.msc). By default, remote control users can have full control with the session user's permission. Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
COMPUTER	Administrative Templates\Windows	Restrict Terminal	At least Microsoft	Specifies whether to restrict users to a single remote Terminal Services

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Terminal Services	Services users to a single remote session	Windows XP Terminal Services	session. If the status is set to Enabled, users who log on remotely via Terminal Services will be restricted to a single session on that server (either active or disconnected). If the user leaves the session in a disconnected state, the user automatically reconnects to that session at next logon. If the status is set to Disabled, users are allowed to make unlimited simultaneous remote connections. If the status is set to Not Configured, behavior is determined by the setting in the Terminal Services Configuration tool (the default is for users to be limited to one remote session).
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Start a program on connection	At least Microsoft Windows XP Terminal Services	Configures Terminal Services to run a specified program automatically upon connection. You can use this setting to specify a program to run automatically when a user logs on to a remote computer. By default, Terminal Services sessions provide access to the full Windows desktop, unless otherwise specified with this setting, by the server administrator, or by the user in configuring the client connection. Enabling this setting overrides the Start Program settings set by the server administrator or user. The Start menu and Windows Desktop are not displayed, and when the user exits the program the session is automatically logged off. To use this setting, in Program path and file name, type the fully qualified path and file name of the executable file to be run when the user logs on. If necessary, in Working Directory, type the fully qualified path to the starting directory for the program. If you leave Working Directory blank, the program runs with its default working directory. If the specified program path, file name, or working directory is not the name of a valid directory, the terminal server connection fails with an error message. If the status is set to Enabled, Terminal Services sessions automatically run the specified program and use the specified Working Directory (or the program default directory, if Working Directory is not specified) as the working directory for the program. If the status is set to Disabled or Not Configured, Terminal Services sessions start with the full desktop, unless the server administrator or user specify otherwise. (See Computer Config\Administrative templates\Windows Components\System\Logon\Run these programs at user logon setting.) Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Do not allow local administrators to customize permissions	At least Microsoft Windows XP Terminal Services	Specifies whether to disable the administrator rights to customize security permissions in the Terminal Services Configuration tool (tscc.msc). You can use this setting to prevent administrators from

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				making changes to the security descriptors for user groups in the TSCC Permissions tab. By default, administrators are able to make such changes. If the status is set to Enabled, the TSCC Permissions tab cannot be used to customize per-connection security descriptors or to change the default security descriptors for an existing group. All of the security descriptors are Read Only. If the status is set to Disabled or Not Configured, server administrators have full Read/Write privileges to the user security descriptors in the TSCC Permissions tab. Note: The preferred method of managing user access is by adding a user to the Remote Desktop Users group.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	TS User Home Directory	At least Microsoft Windows XP Terminal Services	Specifies whether Terminal Services uses the specified network share or local directory path as the root of the user's home directory for a Terminal Services session. To use this setting, select the location for the home directory (network or local) from the Location drop-down list. If you choose to place the directory on a network share, type the Home Dir Root Path in the form \\Computername\Sharename, and then select the drive letter to which you want the network share to be mapped. If you choose to keep the home directory on the local computer, type the Home Dir Root Path in the form Drive:\Path (without quotes), without environment variables or ellipses. Do not specify a placeholder for user alias, because Terminal Services automatically appends this at logon. Note: The Drive Letter field is ignored if you choose to specify a local path. If you choose to specify a local path but then type the name of a network share in Home Dir Root Path, Terminal Services places user home directories in the network location. If the status is set to Enabled, Terminal Services creates the user's home directory in the specified location on the local computer or the network. The home directory path for each user is the specified Home Dir Root Path and the user's alias. If the status is set to Disabled or Not Configured, the user's home directory is as specified at the server.
COMPUTER	Administrative Templates\Windows Components\Terminal Services	Set path for TS Roaming Profiles	At least Microsoft Windows XP Terminal Services	Specifies whether Terminal Services uses the specified network path for roaming user profiles. You can use this setting to specify a network share where the profiles are stored, allowing users to access the same profile for sessions on all terminal servers in the same organizational unit. By default, Terminal Services stores all user profiles locally on the terminal server. To use this setting, type the path to the network share in the form \\Computername\Sharename. Do not specify a placeholder for user alias, because Terminal Services automatically appends this at logon. If the specified network share does not exist, Terminal Services

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				displays an error message at the server and stores the user profiles locally. If the status is set to Enabled, Terminal Services uses the specified path as the root directory for all user profiles. The profiles themselves are contained in subdirectories named for the alias of each user. If the status is set to Disabled or Not Configured, user profiles are stored locally on the server, unless specified otherwise by the server administrator. Note: The roaming profiles specified with this setting apply to Terminal Services connections only; a user might also have a Windows roaming profile, in which case the Terminal Services roaming profile always takes precedence in a Terminal Services session.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client	Do not allow passwords to be saved	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Controls whether passwords can be saved on this computer from Terminal Services clients. If you enable this setting the password saving checkbox in Terminal Services clients will be disabled and users will no longer be able to save passwords. When a user opens an RDP file using the Terminal Services client and saves his settings, any password that previously existed in the RDP file will be deleted. If you disable this setting or leave it not configured, the user will be able to save passwords using the Terminal Services client.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Allow audio redirection	At least Microsoft Windows XP Terminal Services	Specifies whether users can choose where to play the remote computer's audio output during a Terminal Services session (audio redirection). Users can use the Remote computer sound option on the Local Resources tab of Remote Desktop Connection to choose whether to play the remote audio on the remote computer or on the local computer. Users can also choose to disable the audio. By default, users cannot apply audio redirection when connecting via Terminal Services to a server running Windows Server 2003. Users connecting to a computer running Windows XP Professional can apply audio redirection by default. If the status is set to Enabled, users can apply audio redirection. If the status is set to Disabled, users cannot apply audio redirection. If the status is set to Not Configured, audio redirection is not specified at the Group Policy level. However, an administrator can still enable or disable audio redirection by using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Do not allow clipboard redirection	At least Microsoft Windows XP Terminal Services	Specifies whether to prevent the sharing of clipboard contents (clipboard redirection) between a remote computer and a client computer during a Terminal Services session. You can use this setting to prevent users from redirecting clipboard data to and from the remote computer and the local computer. By default, Terminal Services allows this clipboard

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				redirection. If the status is set to Enabled, users cannot redirect clipboard data. If the status is set to Disabled, Terminal Services always allows clipboard redirection. If the status is set to Not Configured, clipboard redirection is not specified at the Group Policy level. However, an administrator can still disable clipboard redirection using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Do not allow COM port redirection	At least Microsoft Windows XP Terminal Services	Specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Terminal Services session. You can use this setting to prevent users from redirecting data to COM port peripherals or mapping local COM ports while they are logged on to a Terminal Services session. By default, Terminal Services allows this COM port redirection. If the status is set to Enabled, users cannot redirect server data to the local COM port. If the status is set to Disabled, Terminal Services always allows COM port redirection. If the status is set to Not Configured, COM port redirection is not specified at the Group Policy level. However, an administrator can still disable COM port redirection using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Do not set default client printer to be default printer in a session	At least Microsoft Windows XP Terminal Services	Specifies whether the client default printer is automatically set as the default printer in a Terminal Services session. By default, Terminal Services automatically designates the client default printer as the default printer in a Terminal Services session. You can use this setting to override this behavior. If the status is set to Enabled, the default printer is the printer specified on the remote computer. If the status is set to Disabled, the terminal server automatically maps the client default printer and sets it as the default printer upon connection. If the status is set to Not Configured, the default printer is not specified at the Group Policy level. However, an administrator can configure the default printer for client sessions by using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Do not allow drive redirection	At least Microsoft Windows XP Terminal Services	Specifies whether to prevent the mapping of client drives in a Terminal Services session (drive redirection). By default, Terminal Services maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or My Computer in the format <driveletter> on <computername>. You can use this setting to override this behavior. If the status is set to Enabled, client drive redirection is not allowed in Terminal Services sessions. If the status is set to Disabled, client drive redirection is always allowed. If the status is set to Not Configured, client drive redirection is not specified at the Group Policy level. However, an administrator can still disable client

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				drive redirection by using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Do not allow LPT port redirection	At least Microsoft Windows XP Terminal Services	Specifies whether to prevent the redirection of data to client LPT ports during a Terminal Services session. You can use this setting to prevent users from mapping local LPT ports and redirecting data from the remote computer to local LPT port peripherals. By default, Terminal Services allows this LPT port redirection. If the status is set to Enabled, users in a Terminal Services session cannot redirect server data to the local LPT port. If the status is set to Disabled, LPT port redirection is always allowed. If the status is set to Not Configured, LPT port redirection is not specified at the Group Policy level. However, an administrator can still disable local LPT port redirection using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Do not allow client printer redirection	At least Microsoft Windows XP Terminal Services	Specifies whether to prevent the mapping of client printers in Terminal Services sessions. You can use this setting to prevent users from redirecting print jobs from the remote computer to a printer attached to their local (client) computer. By default, Terminal Services allows this client printer mapping. If the status is set to Enabled, users cannot redirect print jobs from the remote computer to a local client printer in Terminal Services sessions. If the status is set to Disabled, users can redirect print jobs with client printer mapping. If the status is set to Not Configured, client printer mapping is not specified at the Group Policy level. However, an administrator can still disable client printer mapping using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Terminal Server Fallback Printer Driver Behavior	At least Microsoft Windows Server 2003 with SP1	Specifies the Terminal Server fallback printer driver behavior. By default, Terminal Server fallback printer driver is disabled. If the Terminal Server does not have a printer driver that matches the client's printer, no printer will be available for the terminal server session. If this setting is set to enabled, the Fallback Printer Driver is enabled and the default behavior is for the Terminal Server to find a suitable printer driver. If one is not found, the client's printer is not available. You can choose to change this default behavior. The available options are: Do nothing if one is not found - In the event of a printer driver mismatch, the server will attempt to find a suitable driver, If one is not found, the client's printer is not available. This is the default behavior. Default to PCL if one is not found - If no suitable printer driver can be found, default to the PCL fallback printer driver. Default to PS if one is not found - If no suitable printer driver can be found, default to the PS fallback printer driver. Show both PCL and PS if one is not found - In the event that no suitable

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				driver can be found, show both PS and PCL based fallback printer drivers. If this setting is set to disabled, the Terminal Server fallback driver is disabled and the Terminal Server will not attempt to use the Fallback driver. If this setting is Not configured, the fallback printer driver behavior is off by default. Note: If the Do not allow client printer redirection setting is enabled, this setting is ignored and the fallback driver is disabled.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Terminal Server Fallback Printer Driver Behavior	At least Microsoft Windows Server 2003 with SP1	Specifies the Terminal Server fallback printer driver behavior. By default, Terminal Server fallback printer driver is disabled. If the Terminal Server does not have a printer driver that matches the client's printer, no printer will be available for the terminal server session. If this setting is set to enabled, the Fallback Printer Driver is enabled and the default behavior is for the Terminal Server to find a suitable printer driver. If one is not found, the client's printer is not available. You can choose to change this default behavior. The available options are: Do nothing if one is not found - In the event of a printer driver mismatch, the server will attempt to find a suitable driver, If one is not found, the client's printer is not available. This is the default behavior. Default to PCL if one is not found - If no suitable printer driver can be found, default to the PCL fallback printer driver. Default to PS if one is not found - If no suitable printer driver can be found, default to the PS fallback printer driver. Show both PCL and PS if one is not found - In the event that no suitable driver can be found, show both PS and PCL based fallback printer drivers. If this setting is set to disabled, the Terminal Server fallback driver is disabled and the Terminal Server will not attempt to use the Fallback driver. If this setting is Not configured, the fallback printer driver behavior is off by default. Note: If the Do not allow client printer redirection setting is enabled, this setting is ignored and the fallback driver is disabled.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Do not allow smart card device redirection	At least Microsoft Windows XP Terminal Services	Specifies whether to prevent the mapping of smart card devices (smart card device redirection) in a Terminal Services session. The client computer must be running Windows 2000 server, Windows XP Professional, or Windows Server 2003 family. By default, Terminal Services automatically maps smart card devices on connection. If the status is set to Enabled, Terminal Services users cannot use a smart card to log on to a Terminal Services session. If the status is set to Disabled, smart card device redirection is always allowed. If the status is set to Not Configured, smart card device redirection is not specified at the Group Policy level. However, an administrator can disable local

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				smart card device redirection by using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection	Allow Time Zone Redirection	At least Microsoft Windows XP Terminal Services	Specifies whether to allow the client computer to redirect its time zone settings to the Terminal Services session. By default, the session time zone is the same as the server time zone, and the client computer cannot redirect its time zone information. If the status is set to Enabled, clients that are capable of time zone redirection send their time zone information to the server. The server base time is then used to calculate the current session time (current session time = server base time + client time zone). Currently, Remote Desktop Connection and Windows CE 5.1 are the only clients capable of time zone redirection. Session 0 (the console session) always has the server time zone and settings. To change the system time and time zone, connect to session 0. If the status is set to Disabled, time zone redirection is not possible. If the status is set to Not Configured, time zone redirection is not specified at the Group Policy level and the default behavior is for time zone redirection to be turned off. When an administrator changes this setting, only new connections display the behavior specified by the new setting. Sessions that were initiated before the change must log off and reconnect to be affected by the new setting. Microsoft recommends that all users log off the server after this setting is changed. Note: Time zone redirection is only possible when connecting to a Windows Server 2003 family terminal server.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Encryption and Security	Set client connection encryption level	At least Microsoft Windows XP Terminal Services	Specifies whether to enforce an encryption level for all data sent between the client and the remote computer during a Terminal Services session. Important: If FIPS compliance has already been enabled by the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing Group Policy, you cannot change the encryption level by using this Group Policy or by using Terminal Services Configuration. If the status is set to Enabled, encryption for all connections to the server is set to the level you specify. By default, encryption is set to High. The following encryption levels are available: FIPS Compliant: encrypts data sent from client to server and from server to client to meet the Federal Information Processing Standard 140-1 (FIPS 140-1), a security implementation designed for certifying cryptographic software. Use this level when Terminal Services connections require the highest degree of encryption. FIPS 140-1 validated software is required by the U.S. Government and requested by other prominent institutions. High: encrypts data sent from client to

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				server and from server to client by using strong 128-bit encryption. Use this level when the remote computer is running in an environment containing 128-bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption cannot connect. Client Compatible: encrypts data sent from client to server and from server to client at the maximum key strength supported by the client. Use this level when the remote computer is running in an environment containing mixed or legacy clients. Low: encrypts data sent from the client to the server using 56-bit encryption. Note that data sent from the server to the client is not encrypted when Low is specified. If the status is set to Disabled or Not Configured, the encryption level is not enforced through Group Policy. However, administrators can set the encryption level on the server using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Encryption and Security	Always prompt client for password upon connection	At least Microsoft Windows XP Terminal Services	Specifies whether Terminal Services always prompts the client for a password upon connection. You can use this setting to enforce a password prompt for users logging on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on by entering a password in the Remote Desktop Connection client. If the status is set to Enabled, users cannot automatically log on to Terminal Services by supplying their passwords in the Remote Desktop Connection client. They are prompted for a password to log on. If the status is set to Disabled, users can always log on to Terminal Services automatically by supplying their passwords in the Remote Desktop Connection client. If the status is set to Not Configured, automatic logon is not specified at the Group Policy level. However, an administrator can still enforce password prompting by using the Terminal Services Configuration tool.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Encryption and Security\RPC Security Policy	Secure Server (Require Security)	At least Microsoft Windows Server 2003	Specifies whether a Terminal Server requires secure RPC communication with all clients or allows unsecured communication. You can use this setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. If the status is set to Enabled, the Terminal Server accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients. If the status is set to Disabled, the Terminal Server always requests security for all RPC traffic. However, unsecured communication is allowed for RPC clients that do not respond to the request. If the status is set to Not Configured, unsecured

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				communication is allowed. Note: The RPC interface is used for administering and configuring Terminal Services.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Licensing	License Server Security Group	At least Microsoft Windows XP Terminal Services	Specifies the terminal servers and license servers to which a Terminal Server License Server offers licenses. You can use this setting to control which servers are issued licenses. By default, a Terminal Server License Server issues a license to any computer that requests one. If the status is set to Enabled, a local group called Terminal Services Computers is created. The Terminal Server License Server grants licenses only to computers whose computer accounts are placed in this group. When the target computer is a domain controller, this group is a domain local group. If the status is set to Disabled, the Terminal Server License Server issues a license to any computer that requests one. The Terminal Services Computers group is not deleted or changed in any way. This is the default behavior. If the status is set to Not Configured, the Terminal Server License Server issues a license to any computer that requests one. The Terminal Services Computers group is not deleted or changed in any way. This is the default behavior. Notes: 1. The Terminal Services Computers group is empty by default. The Terminal Server License Server does not grant licenses to any computers unless you explicitly populate this group. 2. The most efficient way to manage Terminal Server computer accounts is to create a global group containing the accounts of all terminal servers and license servers that must receive licenses. Then, place this global group into the local (or domain local) Terminal Services Computers group. This method allows a domain administrator to manage a single list of computer accounts. 3. To add a computer account to a group, open the Computer Management snap-in, navigate to the Properties page of the group, and click Add. On the Select Users, Computers, or Groups dialog box, click Object Types and then check Computers.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Licensing	Prevent License Upgrade	At least Microsoft Windows XP Terminal Services	Specifies how a License Server distributes license upgrades to terminal servers running Windows 2000. A License Server attempts to provide the most appropriate Client Access License (CAL) for a connection. For example, a License Server provides a Windows 2000 Terminal Services (TS) CAL token for clients connecting to a terminal server running Windows 2000 operating system, and a Windows Server 2003 family TS CAL token for a connection to a terminal server running Windows Server 2003. By default, this per-computer setting allows a License Server to supply a Windows Server 2003 family TS CAL token, if available, to a terminal server running Windows 2000 operating system if there is no

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Windows 2000 server TS CAL token available. If the status is set to Enabled, when a terminal server running Windows 2000 server requests a license, but no Windows 2000 server TS CAL token is available, a temporary CAL is issued if the client has not already been issued a temporary CAL. Otherwise, no CAL is issued and the client is refused connection, unless the terminal server is within its grace period. If the status is set to Disabled, the default behavior is enforced. If the status is set to Not Configured, the License Server exhibits the default behavior.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Session Directory	Join Session Directory	Microsoft Windows Server 2003, Enterprise Edition	Specifies whether Terminal Services uses a Session Directory for tracking user sessions, allowing a group of terminal servers to locate and connect a user back to an existing session. If the status is set to Enabled, Terminal Services stores user session information in a Session Directory on the server specified in the Session Directory Server setting. If the status is set to Disabled, session tracking is not performed, and cannot be enabled using either the Terminal Services Configuration tool or the Terminal Services WMI provider. If the status is set to Not Configured, session tracking is not specified at the Group Policy level. However, an administrator can configure servers to participate in a Session Directory with the Terminal Services Configuration tool or via the Terminal Services WMI provider. Note: If you enable this setting, you must enable the Session Directory Server and Session Directory Cluster Name settings. The Session Directory service can only be used when the Terminal Server component is installed on the server.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Session Directory	Session Directory Cluster Name	Microsoft Windows Server 2003, Enterprise Edition	Specifies the Cluster Name for the terminal server, associating it with other servers in the same logical group. If the status is set to Enabled, you can specify the name of the terminal server cluster. If the name is invalid, an error is logged in the event log stating that the specified cluster could not be found. If the status is set to Disabled or Not Configured, Cluster Name is not specified at the Group Policy level, and may be adjusted using the Terminal Services Configuration tool or the Terminal Services WMI provider. Note: Use this setting in combination with Join Session Directory and Session Directory Server settings.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Session Directory	Terminal Server IP Address Redirection	Microsoft Windows Server 2003, Enterprise Edition	Specifies how client devices are directed when reconnecting to an existing terminal server session. If the status is set to Enabled, client devices attempt to reconnect to disconnected sessions using the internal IP addresses of the terminal servers in the Session Directory. Enable this setting if clients can directly connect to an individual terminal server

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				via that terminal server's IP address. If the status is set to Disabled, client devices are redirected to disconnected sessions using the virtual IP address of the cluster. To direct the request to the proper terminal server, terminal server clients and the load balancing hardware must both support the use of routing tokens. This requires configuration and software support in the load balancing device specifically for terminal servers and routing tokens. Disable this setting if the clients only have visibility to the virtual IP address for the terminal server cluster, and cannot connect to an individual terminal server's IP address. If the status is set to Not Configured, the IP address redirection setting in the Terminal Services Configuration tool is used. The default for this setting in the Terminal Services Configuration tool is enabled.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Session Directory	Session Directory Server	Microsoft Windows Server 2003, Enterprise Edition	Specifies whether to configure a server as a Session Directory Server for Terminal Services sessions on your network. A Session Directory Server directs incoming Terminal Services connections for a terminal server cluster. If the status is set to Enabled, you can specify a server and its DNS name, IP address, or fully qualified domain name to act as the Session Directory Server. Terminal Services Session Directory must be running on the specified server for this setting to be effective. If the name specified for the Session Directory Server is not valid, an error is logged in Event Viewer on the target computer indicating that the specified location could not be found. If status is set to Disabled or Not Configured, the Session Directory Server is not specified at the Group Policy level, and can be adjusted using the Terminal Services Configuration tool or the Terminal Services WMI provider. Note: This setting must be used in combination with the Join Session Directory setting.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Sessions	Terminate session when time limits are reached		Specifies whether to terminate a timed-out Terminal Services session instead of disconnecting it. You can use this setting to direct Terminal Services to terminate a session (that is, the user is logged off and the session is deleted from the server) after time limits for active or idle sessions are reached. By default, Terminal Services disconnects sessions that reach their time limits. Time limits are set locally by the server administrator or in Group Policy. See the Sets a time limit for active Terminal Services sessions and Sets a time limit for active but idle Terminal Services sessions settings. If the status is set to Enabled, Terminal Services terminates any session that reaches its time-out limit. If the status is set to Disabled, Terminal Services always disconnects a timed-out session, even if specified otherwise by the server

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				administrator. If the status is set to Not Configured, Terminal Services disconnects a timed-out session, unless specified otherwise in local settings. Note: This setting only applies to time-out limits that are deliberately set (in the Terminal Services Configuration tool or Group Policy Object Editor), not to time-out events that occur due to connectivity or network conditions. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Sessions	Set time limit for disconnected sessions	At least Microsoft Windows XP Terminal Services	Specifies a time limit for disconnected Terminal Services sessions. You can use this setting to specify the maximum amount of time that a disconnected session is kept active on the server. By default, Terminal Services allows users to disconnect from a remote session without logging off and ending the session. When a session is in a disconnected state, running programs are kept active even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server. If the status is set to Enabled, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select Never. If the status is set to Disabled or Not Configured, time limits for disconnected sessions are not specified at the Group Policy level. Note: This setting does not apply to console sessions such as Remote Desktop sessions with computers running Windows XP Professional. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Sessions	Sets a time limit for active but idle Terminal Services sessions	At least Microsoft Windows XP Terminal Services	Specifies a time limit for active but idle Terminal Services sessions. You can use this setting to specify the maximum amount of time that an active session can be idle (that is, no user input) before it is automatically disconnected. By default, Terminal Services allows active sessions to remain idle for an unlimited time. To use this setting, select Enabled, and then select the desired time limit in the Idle session limit drop-down list. If the status is set to Enabled, active but idle sessions are automatically disconnected after the specified amount of time. The user receives a two-minute warning before the session ends, which allows the user to press a key or move the mouse to keep the session active. If the status is set to Disabled or Not Configured, the time limit for active but idle sessions is not specified at the Group Policy level. However, an administrator can specify time limits for idle sessions in the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Terminal Services Configuration tool. Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides. Idle session limits do not apply to the console session. To specify that user sessions are terminated at time-out, enable the Terminate session when time limits are reached setting.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Sessions	Sets a time limit for active Terminal Services sessions	At least Microsoft Windows XP Terminal Services	Specifies a time limit for active Terminal Services sessions. You can use this setting to specify the maximum amount of time a Terminal Services session can be active before it is automatically disconnected. To use this setting, select Enabled, and then select the desired limit in the Active session limit drop-down list. By default, Terminal Services allows sessions to remain active for an unlimited time. If the status is set to Enabled, Terminal Services ends active sessions after the specified amount of time. The user receives a two-minute warning before the Terminal Services session ends, which allows the user to save open files and close programs. If the status is set to Disabled or Not Configured, time limits for active sessions are not specified at the Group Policy level. However, an administrator can specify time limits for active sessions in the Terminal Services Configuration tool. Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides. Active session limits do not apply to the console session. To specify user sessions to be terminated at time-out, enable the Terminate session when time limits are reached setting.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Sessions	Allow reconnection from original client only	At least Microsoft Windows XP Terminal Services	Specifies whether to allow users to reconnect to a disconnected Terminal Services session using a computer other than the original client computer. You can use this setting to prevent Terminal Services users from reconnecting to the disconnected session using a computer other than the client computer from which they originally created the session. By default, Terminal Services allows users to reconnect to disconnected sessions from any client computer. If the status is set to Enabled, users can reconnect to disconnected sessions only from the original client computer. If a user attempts to connect to the disconnected session from another computer, a new session is created instead. If the status is set to Disabled, users can always connect to the disconnected session from any computer. If the status is set to Not Configured, session reconnection from the original client computer is not specified at the Group Policy level. Important: This option is only supported for Citrix ICA clients that provide a serial number when connecting; this setting is

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				ignored if the user is connecting with a Windows client. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Temporary folders	Do not delete temp folder upon exit	At least Microsoft Windows XP Terminal Services	Specifies whether Terminal Services retains a user's per-session temporary folders at logoff. You can use this setting to maintain a user's session-specific temporary folders on a remote computer, even if the user logs off from a session. By default, Terminal Services deletes a user's temporary folders when the user logs off. If the status is set to Enabled, users' per-session temporary folders are retained when the user logs off from a session. If the status is set to Disabled, temporary folders are deleted when a user logs off, even if the administrator specifies otherwise in the Terminal Services Configuration tool. If the status is set to Not Configured, Terminal Services deletes the temporary folders from the remote computer at logoff, unless specified otherwise by the server administrator. Note: This setting only takes effect if per-session temporary folders are in use on the server. That is, if you enable the Do not use temporary folders per session setting, this setting has no effect.
COMPUTER	Administrative Templates\Windows Components\Terminal Services\Temporary folders	Do not use temp folders per session	At least Microsoft Windows XP Terminal Services	Specifies whether to prevent Terminal Services from creating session-specific temporary folders. You can use this setting to disable the creation of separate temporary folders on a remote computer for each session. By default, Terminal Services creates a separate temporary folder for each active session that a user maintains on a remote computer. Unless otherwise specified, these temporary folders are in %USERPROFILE%\Local Settings\Temp\<sessionID>. If the status is set to Enabled, per-session temporary folders are not created. Instead, users' temporary files are stored in a common Temp directory for each user on the server (by default, %USERPROFILE%\Local Settings\Temp). If the status is set to Disabled, per-session temporary folders are always created, even if the administrator specifies otherwise in the Terminal Services Configuration tool. If the status is set to Not Configured, per-session temporary folders are created unless otherwise specified by the server administrator.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Enable user to browse for source while elevated	At least Microsoft Windows 2000	Allows users to search for installation files during privileged installations. This setting enables the Browse button in the Use feature from dialog box. As a result, users can search for installation files, even when the installation program is running with elevated system privileges. By

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				default, only system administrators can browse during installations with elevated privileges, such as installations offered on the desktop or displayed in Add or Remove Programs. Because the installation is running with elevated system privileges, users can browse through directories that their own permissions would not allow. This setting does not affect installations that run in the user's security context. Also, see the Remove browse dialog box for new source setting.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Enable user to use media source while elevated	At least Microsoft Windows 2000	Allows users to install programs from removable media, such as floppy disks and CD-ROMs, during privileged installations. This setting permits all users to install programs from removable media, even when the installation program is running with elevated system privileges. By default, users can install programs from removable media only when the installation runs in the user's security context. During privileged installations, such as those offered on the desktop or displayed in Add or Remove Programs, only system administrators can install from removable media. This setting does not affect installations that run in the user's security context. By default, users can install from removable media when the installation runs in their own security context. Also, see the Prevent removable media source for any install setting in User Configuration\Administrative Templates\Windows Components\Windows Installer.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Enable user to patch elevated products	At least Microsoft Windows 2000	Allows users to upgrade programs during privileged installations. This setting permits all users to install patches, even when the installation program is running with elevated system privileges. Patches are updates or upgrades that replace only those program files that have changed. Because patches can easily be vehicles for malicious programs, some installations prohibit their use. By default, only system administrators can apply patches during installations with elevated privileges, such as installations offered on the desktop or displayed in Add or Remove Programs. This setting does not affect installations that run in the user's security context. By default, users can install patches to programs that run in their own security context. Also, see the Prohibit patching setting.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Always install with elevated privileges	At least Microsoft Windows 2000	Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer. Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Remove browse dialog box for new source	At least Microsoft Windows 2000	Prevents users from searching for installation files when they add features or components to an installed program. This setting disables the Browse button beside the Use feature from list in the Windows Installer dialog box. As a result, users must select an installation file source from the Use features from list that the system administrator configures. This setting applies even when the installation is running in the user's security context. If you disable this setting or do not configure it, the Browse button is enabled when an installation is running in the user's security context. But only system administrators can browse when an installation is running with elevated system privileges, such as installations offered on the desktop or in Add or Remove Programs. This setting affects Windows Installer only. It does not prevent users from selecting other browsers, such as Windows Explorer or My Network Places, to search for installation files. Also, see the Enable user to browse for source while elevated setting.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Disable Windows Installer	At least Microsoft Windows 2000	Disables or restricts the use of Windows Installer. This setting can prevent users from installing software on their systems or permit users to install only those programs offered by a system administrator. If you enable this setting, you can use the options in the Disable Windows Installer box to establish an installation setting. -- The Never option indicates Windows Installer is fully enabled. Users can install and upgrade software. This is the default behavior for Windows Installer on Windows 2000 Professional and Windows XP Professional when the policy is not configured. -- The For non-managed apps only option permits users to install only those programs that a system administrator assigns (offers on the desktop) or publishes (adds them to Add or Remove Programs). This is the default behavior of Windows Installer on Windows Server 2003 family when the policy is not configured. -- The

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Always option indicates that Windows Installer is disabled. This setting affects Windows Installer only. It does not prevent users from using other methods to install and upgrade programs.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Prohibit patching	At least Microsoft Windows 2000	Prevents users from using Windows Installer to install patches. Patches are updates or upgrades that replace only those program files that have changed. Because patches can be easy vehicles for malicious programs, some installations prohibit their use. Note: This setting applies only to installations that run in the user's security context. By default, users who are not system administrators cannot apply patches to installations that run with elevated system privileges, such as those offered on the desktop or in Add or Remove Programs. Also, see the Enable user to patch elevated products setting.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Prohibit rollback	At least Microsoft Windows 2000	Prohibits Windows Installer from generating and saving the files it needs to reverse an interrupted or unsuccessful installation. This setting prevents Windows Installer from recording the original state of the system and sequence of changes it makes during installation. It also prevents Windows Installer from retaining files it intends to delete later. As a result, Windows Installer cannot restore the computer to its original state if the installation does not complete. This setting is designed to reduce the amount of temporary disk space required to install programs. Also, it prevents malicious users from interrupting an installation to gather data about the internal state of the computer or to search secure system files. However, because an incomplete installation can render the system or a program inoperable, do not use this setting unless it is essential. This setting appears in the Computer Configuration and User Configuration folders. If the setting is enabled in either folder, it is considered be enabled, even if it is explicitly disabled in the other folder.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Allow admin to install from Terminal Services session	At least Microsoft Windows 2000	Allows Terminal Services administrators to install and configure programs remotely. By default, system administrators can install programs only when system administrators are logged on to the computer on which the program is being installed. This setting creates a special exception for computers running Terminal Services. This setting affects system administrators only. Other users cannot install programs remotely.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Enable user control over installs	At least Microsoft Windows 2000	Permits users to change installation options that typically are available only to system administrators. This setting bypasses some of the security features of Windows Installer. It permits installations to complete that otherwise would be halted due to a security violation. The security

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user. This setting is designed for less restrictive environments. It can be used to circumvent errors in an installation program that prevents software from being installed.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Prohibit non-administrators from applying vendor signed updates	Windows Installer v3.0	This setting controls the ability of non-administrators to install updates that have been digitally signed by the application vendor. Non-administrator updates provide a mechanism for the author of an application to create digitally signed updates that can be applied by non-privileged users. If you enable this policy setting, only administrators or users with administrative privileges can apply updates to Windows Installer based application. If you disable this policy setting, users without administrative privileges will be able to install non-administrator updates.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Prohibit removal of updates	Windows Installer v3.0	This setting controls the ability for users or administrators to remove Windows Installer based updates. This setting should be used if you need to maintain a tight control over updates. One example is a lockdown environment where you want to ensure that updates once installed cannot be removed by users or administrators. If you enable this policy setting, updates cannot be removed from the computer by a user or an administrator. The Windows Installer can still remove an update that is no longer applicable to the product. If you disable this policy setting, a user can remove an update from the computer only if the user has been granted privileges to remove the update. This can depend on whether the user is an administrator, whether Disable Windows Installer and Always install with elevated privileges policy settings are set, and whether the update was installed in a per-user managed, per-user unmanaged, or per-machine context.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Turn off creation of System Restore Checkpoints	Only works on Microsoft Windows XP Professional	System Restore enables users, in the event of a problem, to restore their computers to a previous state without losing personal data files. By default, the Windows Installer automatically creates a System Restore checkpoint each time an application is installed, so that users can restore their computer to the state it was in before installing the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				application. If you enable this setting, the windows Installer does not generate System Restore checkpoints when installing applications. If you disable this setting or do not configure it, the Windows Installer automatically creates a System Restore checkpoint each time an application is installed. Note: This setting only applies to Windows XP Professional.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Prohibit User Installs	Microsoft Windows XP or Windows 2000 with Windows Installer v2.0	This setting allows you to configure user installs. To configure this setting, set it to enabled and use the drop-down list to select the behavior you want. If this setting is not configured, or if the setting is enabled and Allow User Installs is selected, the installer allows and makes use of products that are installed per user, and products that are installed per computer. If the installer finds a per-user install of an application, this hides a per-computer installation of that same product. If this setting is enabled and Hide User Installs is selected, the installer ignores per-user applications. This causes a per-computer installed application to be visible to users, even if those users have a per-user install of the product registered in their user profile. If this setting is enabled and Prohibit User Installs is selected, the installer prevents applications from being installed per user, and it ignores previously installed per-user applications. An attempt to perform a per-user installation causes the installer to display an error message and stop the installation. This setting is useful in environments where the administrator only wants per-computer applications installed, such as on a kiosk or a Windows Terminal Server.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Enforce upgrade component rules	Windows Installer v3.0	This setting causes the Windows Installer to enforce strict rules for component upgrades - setting this may cause some updates to fail. If you enable this policy setting strict upgrade rules will be enforced by the Windows Installer. Upgrades can fail if they attempt to do one of the following: (1) Remove a component from a feature. This can also occur if you change the GUID of a component. The component identified by the original GUID appears to be removed and the component as identified by the new GUID appears as a new component. (2) Add a new feature to the top or middle of an existing feature tree. The new feature must be added as a new leaf feature to an existing feature tree. If you disable this policy setting, the Windows Installer will use less restrictive rules for component upgrades.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Baseline file cache maximum size	Windows Installer v3.0	This policy controls the percentage of disk space available to the Windows Installer baseline file cache. The Windows Installer uses the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				baseline file cache to save baseline files modified by binary delta difference updates. The cache is used to retrieve the baseline file for future updates. The cache eliminates user prompts for source media when new updates are applied. If you enable this policy setting you can modify the maximum size of the Windows Installer baseline file cache. If you set the baseline cache size to 0, the Windows Installer will stop populating the baseline cache for new updates. The existing cached files will remain on disk and will be deleted when the product is removed. If you set the baseline cache to 100, the Windows Installer will use available free space for the baseline file cache. If you disable this policy setting or if it is not configured the Windows Installer will uses a default value of 10 percent for the baseline file cache maximum size.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Logging	At least Microsoft Windows 2000	Specifies the types of events that Windows Installer records in its transaction log for each installation. The log, Msi.log, appears in the Temp directory of the system volume. When you enable this setting, you can specify the types of events you want Windows Installer to record. To indicate that an event type is recorded, type the letter representing the event type. You can type the letters in any order and list as many or as few event types as you want. To disable logging, delete all of the letters from the box. If you disable this setting or do not configure it, Windows Installer logs the default event types, represented by the letters iweap.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Disable IE security prompt for Windows Installer scripts	At least Microsoft Windows 2000	Allows Web-based programs to install software on the computer without notifying the user. By default, when a script hosted by an Internet browser tries to install a program on the system, the system warns users and allows them to select or refuse the installation. This setting suppresses the warning and allows the installation to proceed. This setting is designed for enterprises that use Web-based tools to distribute programs to their employees. However, because this setting can pose a security risk, it should be applied cautiously.
COMPUTER	Administrative Templates\Windows Components\Windows Installer	Cache transforms in secure location on workstation	At least Microsoft Windows 2000	Saves copies of transform files in a secure location on the local computer. Transform files consist of instructions to modify or customize a program during installation. If you enable this setting, the transform file is saved in a secure location on the user's computer. Because Windows Installer requires the transform file in order to repeat an installation in which the transform file was used, the user must be using the same computer or be connected to the original or identical media to reinstall, remove, or repair the installation. This is the default behavior on Windows Server 2003 family when the policy is not configured. This

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				setting is designed for enterprises to prevent unauthorized or malicious editing of transform files. If you disable this setting, Windows Installer stores transform files in the Application Data directory in the user's profile. When a user reinstalls, removes, or repairs an installation, the transform file is available, even if the user is on a different computer or is not connected to the network. This is the default behavior on Windows 2000 Professional and Windows XP Professional when the policy is not configured.
COMPUTER	Administrative Templates\Windows Components\Windows Media Digital Rights Management	Prevent Windows Media DRM Internet Access	At least Microsoft Windows Server 2003	Prevents Windows Media Digital Rights Management (DRM) from accessing the Internet (or intranet). When enabled, Windows Media DRM is prevented from accessing the Internet (or intranet) for license acquisition and security upgrades. When this policy is enabled, programs are not able to acquire licenses for secure content, upgrade Windows Media DRM security components, or restore backed up content licenses. Secure content that is already licensed to the local computer will continue to play. Users are also able to protect music that they copy from a CD and play this protected content on their computer, since the license is generated locally in this scenario. When this policy is either disabled or not configured, Windows Media DRM functions normally and will connect to the Internet (or intranet) to acquire licenses, download security upgrades, and perform license restoration.
COMPUTER	Administrative Templates\Windows Components\Windows Media Player	Prevent Automatic Updates	Windows Media Player 9 Series and later.	Prevents users from being prompted to update Windows Media Player. This policy prevents the Player from being updated and prevents users with administrator rights from being prompted to update the Player if an updated version is available. The Check for Player Updates command on the Help menu in the Player is not available. In addition, none of the time intervals in the Check for updates section on the Player tab are selected or available. When this policy is not configured or disabled, Check for Player Updates is available only to users with administrator rights and they may be prompted to update the Player if an updated version is available. By default, users with administrator rights can select how frequently updates are checked for. Users without administrator rights do not see Check for Player Updates and are never prompted to update the Player even without this policy.
COMPUTER	Administrative Templates\Windows Components\Windows Media Player	Do Not Show First Use Dialog Boxes	Windows Media Player 9 Series and later.	Do Not Show First Use Dialog Boxes This policy prevents the Privacy Options and Installation Options dialog boxes from being displayed the first time a user starts Windows Media Player. This policy prevents the dialog boxes which allow users to select privacy, file types, and other

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				desktop options from being displayed when the Player is first started. Some of the options can be configured by using other Windows Media Player group policies. When this policy is not configured or disabled, the dialog boxes are displayed when the user starts the Player for the first time.
COMPUTER	Administrative Templates\Windows Components\Windows Media Player	Prevent Video Smoothing	Windows Media Player 9 Series and later.	Prevents video smoothing from occurring. This policy prevents video smoothing, which can improve video playback on computers with limited resources, from occurring. In addition, the Use Video Smoothing check box in the Video Acceleration Settings dialog box in the Player is cleared and is not available. When this policy is disabled, video smoothing can occur if necessary, and the Use Video Smoothing check box is selected and is not available. When this policy is not configured, video smoothing can occur if necessary. Users can change the setting for the Use Video Smoothing check box. Video smoothing is available only on the Windows XP Home Edition and Windows XP Professional operating systems.
COMPUTER	Administrative Templates\Windows Components\Windows Media Player	Prevent Quick Launch Toolbar Shortcut Creation	Windows Media Player 9 Series and later.	This policy prevents a shortcut for the Player from being added to the Quick Launch bar. When this policy is not configured or disabled, the user can choose whether to add the shortcut for the Player to the Quick Launch bar.
COMPUTER	Administrative Templates\Windows Components\Windows Media Player	Prevent Desktop Shortcut Creation	Windows Media Player 9 Series and later.	This policy prevents a shortcut icon for the Player from being added to the user's desktop. When this policy is not configured or disabled, users can choose whether to add the Player shortcut icon to their desktops.
COMPUTER	Administrative Templates\Windows Components\Windows Messenger	Do not automatically start Windows Messenger initially	At least Microsoft Windows XP Professional or Windows Server 2003 family	Windows Messenger is automatically loaded and running when a user logs on to a Windows XP computer. You can use this setting to stop Windows Messenger from automatically being run at logon. If you enable this setting, Windows Messenger will not be loaded automatically when a user logs on. If you disable or do not configure this setting, the Windows Messenger will be loaded automatically at logon. Note: This setting simply prevents Windows Messenger from running intially. If the user invokes and uses Windows Messenger from that point on, Windows Messenger will be loaded. The user can also configure this behavior on the Preferences tab on the Tools menu in the Windows Messenger user interface. Note: If you do not want users to use Windows Messenger, enable the Do not allow Windows Messenger to run setting. Note: This setting is available under both Computer Configuration and User Configuration. If both are present, the Computer Configuration version of

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				this setting takes precedence.
COMPUTER	Administrative Templates\Windows Components\Windows Messenger	Do not allow Windows Messenger to be run	At least Microsoft Windows XP Professional or Windows Server 2003 family	Allows you to disable Windows Messenger. If you enable this setting, Windows Messenger will not run. If you disable or do not configure this setting, Windows Messenger can be used. Note: If you enable this setting, Remote Assistance also cannot use Windows Messenger. Note: This setting is available under both Computer Configuration and User Configuration. If both are present, the Computer Configuration version of this setting takes precedence.
COMPUTER	Administrative Templates\Windows Components\Windows Movie Maker	Do not allow Windows Movie Maker to run	At least Microsoft Windows XP Professional with SP2	Specifies whether Windows Movie Maker can run. Windows Movie Maker is a feature of the Windows XP operating system that can be used to capture, edit, and then save video as a movie to share with others. If you enable this setting, Windows Movie Maker will not run. If you disable or do not configure this setting, Windows Movie Maker can be run.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Configure Automatic Updates	Windows Server 2003, XP SP1, 2000 SP3	Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service. This setting lets you specify if automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting: 2 = Notify before downloading any updates and notify again before installing them. When Windows finds updates that apply to this computer, an icon appears in the status area with a message that updates are ready to be downloaded. Clicking the icon or message provides the option to select the specific updates to download. Windows then downloads the selected updates in the background. When the download is complete, the icon appears in the status area again, with notification that the updates are ready to be installed. Clicking the icon or message provides the option to select which updates to install. 3 = (Default setting) Download the updates automatically and notify when they are ready to be installed Windows finds updates that apply to your computer and downloads these updates in the background (the user is not notified or interrupted during this process). When the download is complete, the icon appears in the status area, with notification that the updates are ready to be installed. Clicking the icon or message provides the option to select which updates to install. 4 = Automatically download updates and install them on the schedule specified below Specify the schedule using the options in the Group Policy Setting. If no schedule is specified, the default schedule for all installations will be everyday at 3:00 AM. If any of the updates require

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				a restart to complete the installation, Windows will restart the computer automatically. (If a user is logged on to the computer when Windows is ready to restart, the user will be notified and given the option to delay the restart.) 5 = Allow local administrators to select the configuration mode that Automatic Updates should notify and install updates With this option, the local administrators will be allowed to use the Automatic Updates control panel to select a configuration option of their choice. For example they can choose their own scheduled installation time. Local administrators will not be allowed to disable Automatic Updates' configuration. To use this setting, click Enabled, and then select one of the options (2, 3, 4 or 5). If you select 4, you can set a recurring schedule (if no schedule is specified, all installations will occur everyday at 3:00 AM). If the status is set to Enabled, Windows recognizes when this computer is online and uses its Internet connection to search the Windows Update Web site for updates that apply to this computer. If the status is set to Disabled, any updates that are available on the Windows Update Web site must be downloaded and installed manually by going to http://windowsupdate.microsoft.com. If the status is set to Not Configured, use of Automatic Updates is not specified at the Group Policy level. However, an administrator can still configure Automatic Updates through Control Panel.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Specify intranet Microsoft update service location	Windows Server 2003, XP SP1, 2000 SP3	Specifies an intranet server to host updates from the Microsoft Update Web sites. You can then use this update service to automatically update computers on your network. This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network. To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server. If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying them. If the status is set to Disabled or Not Configured, and if Automatic Updates is not disabled by policy or user preference, the Automatic Updates client connects directly to the Windows Update site on the Internet. Note: If the Configure Automatic

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Updates policy is disabled, then this policy has no effect.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Automatic Updates detection frequency	Windows Server 2003, XP SP1, 2000 SP3	Specifies the hours that Windows will use to determine how long to wait before checking for available updates. The exact wait time is determined by using the hours specified here minus zero to twenty percent of the hours specified. For example, if this policy is used to specify a 20 hour detection frequency, then all clients to which this policy is applied will check for updates anywhere between 16 and 20 hours. If the status is set to Enabled, Windows will check for available updates at the specified interval. If the status is set to Disabled or Not Configured, Windows will check for available updates at the default interval of 22 hours. Note: The Specify intranet Microsoft update service location setting must be enabled for this policy to have effect. Note: If the Configure Automatic Updates policy is disabled, this policy has no effect.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Allow non-administrators to receive update notifications	Windows Server 2003, XP SP1, 2000 SP3	Specifies whether, when logged on, non-administrative users will receive update notifications based on the configuration settings for Automatic Updates. If Automatic Updates is configured, by policy or locally, to notify the user either before downloading or only before installation, these notifications will be offered to any non-administrator who logs onto the computer. If the status is set to Enabled, Automatic Updates will include non-administrators when determining which logged-on user should receive notification. If the status is set to Disabled or Not Configured, Automatic Updates will notify only logged-on administrators. Note: If the Configure Automatic Updates policy is disabled, this policy has no effect.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Allow Automatic Updates immediate installation	Windows Server 2003, XP SP1, 2000 SP3	Specifies whether Automatic Updates should automatically install certain updates that neither interrupt Windows services nor restart Windows. If the status is set to Enabled, Automatic Updates will immediately install these updates once they are downloaded and ready to install. If the status is set to Disabled, such updates will not be installed immediately. Note: If the Configure Automatic Updates policy is disabled, this policy has no effect.
COMPUTER	Administrative Templates\Windows Components\Windows Update	No auto-restart for scheduled Automatic Updates installations	Windows Server 2003, XP SP1, 2000 SP3	Specifies that to complete a scheduled installation, Automatic Updates will wait for the computer to be restarted by any user who is logged on, instead of causing the computer to restart automatically. If the status is set to Enabled, Automatic Updates will not restart a computer automatically during a scheduled installation if a user is logged in to the computer. Instead, Automatic Updates will notify the user to restart the computer. Be aware that the computer needs to be restarted for the updates to take effect. If the status is set to Disabled or Not Configured,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation. Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the Configure Automatic Updates policy is disabled, this policy has no effect.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Re-prompt for restart with scheduled installations	Windows Server 2003, XP SP1, 2000 SP3	Specifies the amount of time for Automatic Updates to wait before prompting again with a scheduled restart. If the status is set to Enabled, a scheduled restart will occur the specified number of minutes after the previous prompt for restart was postponed. If the status is set to Disabled or Not Configured, the default interval is 10 minutes. Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the Configure Automatic Updates policy is disabled, this policy has no effect.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Delay Restart for scheduled installations	Windows Server 2003, XP SP1, 2000 SP3	Specifies the amount of time for Automatic Updates to wait before proceeding with a scheduled restart. If the status is set to Enabled, a scheduled restart will occur the specified number of minutes after the installation is finished. If the status is set to Disabled or Not Configured, the default wait time is 5 minutes. Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the Configure Automatic Updates policy is disabled, this policy has no effect.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Reschedule Automatic Updates scheduled installations	Windows Server 2003, XP SP1, 2000 SP3	Specifies the amount of time for Automatic Updates to wait, following system startup, before proceeding with a scheduled installation that was missed previously. If the status is set to Enabled, a scheduled installation that did not take place earlier will occur the specified number of minutes after the computer is next started. If the status is set to Disabled, a missed scheduled installation will occur with the next scheduled installation. If the status is set to Not Configured, a missed scheduled installation will occur one minute after the computer is next started. Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the Configure Automatic Updates policy is disabled, this policy has no effect.
COMPUTER	Administrative Templates\Windows Components\Windows Update	Enable client-side targeting	Windows Server 2003, XP SP1, 2000 SP3	Specifies the target group name that should be used to receive updates from an intranet Microsoft update service. If the status is set to Enabled, the specified target group information is sent to the intranet Microsoft update service which uses it to determine which updates should be deployed to this computer. If the status is set to Disabled or Not Configured, no target group information will be sent to the intranet

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Microsoft update service. Note: This policy applies only when the intranet Microsoft update service this computer is directed to is configured to support client-side targeting. If the Specify intranet Microsoft update service location policy is disabled or not configured, this policy has no effect.
COMPUTER	Administrative Templates\Windows NT Network\Sharing	Create hidden drive shares (server)		
COMPUTER	Administrative Templates\Windows NT Network\Sharing	Create hidden drive shares (workstation)		
COMPUTER	Administrative Templates\Windows NT Printers	Beep for error enabled		
COMPUTER	Administrative Templates\Windows NT Printers	Disable browse thread on this computer		
COMPUTER	Administrative Templates\Windows NT Printers	Scheduler priority		
COMPUTER	Administrative Templates\Windows NT Remote Access	Auto Disconnect		
COMPUTER	Administrative Templates\Windows NT Remote Access	Wait interval for callback		
COMPUTER	Administrative Templates\Windows NT Remote Access	Max number of unsuccessful authentication retries		
COMPUTER	Administrative Templates\Windows NT Remote Access	Max time limit for authentication		
COMPUTER	Administrative Templates\Windows NT Shell\Custom shared folders	Custom shared desktop icons		
COMPUTER	Administrative Templates\Windows NT Shell\Custom shared folders	Custom shared Programs folder		
COMPUTER	Administrative Templates\Windows NT Shell\Custom shared folders	Custom shared Start menu		
COMPUTER	Administrative Templates\Windows NT Shell\Custom shared folders	Custom shared Startup folder		

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
COMPUTER	Administrative Templates\Windows NT System\File system	Allow extended characters in 8.3 file names		
COMPUTER	Administrative Templates\Windows NT System\File system	Do not create 8.3 file names for long file names		
COMPUTER	Administrative Templates\Windows NT System\File system	Do not update last access time		
COMPUTER	Administrative Templates\Windows NT System\Logon	Do not display last logged on user name		
COMPUTER	Administrative Templates\Windows NT System\Logon	Logon banner		
COMPUTER	Administrative Templates\Windows NT System\Logon	Run logon scripts synchronously.		
COMPUTER	Administrative Templates\Windows NT System\Logon	Enable shutdown from Authentication dialog box		
COMPUTER	Administrative Templates\Windows NT User Profiles	Choose profile default operation		
COMPUTER	Administrative Templates\Windows NT User Profiles	Delete cached copies of roaming profiles		
COMPUTER	Administrative Templates\Windows NT User Profiles	Automatically detect slow network connections		
COMPUTER	Administrative Templates\Windows NT User Profiles	Timeout for dialog boxes		
COMPUTER	Administrative Templates\Windows NT User Profiles	Slow network default profile operation		
COMPUTER	Administrative Templates\Windows NT User Profiles	Slow network connection timeout		
USER	Administrative Templates\Advanced settings	Browsing		

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Advanced settings	HTTP 1.1 settings		
USER	Administrative Templates\Advanced settings	Internet Connection Wizard Settings		
USER	Administrative Templates\Advanced settings	Microsoft VM		
USER	Administrative Templates\Advanced settings	Connection		
USER	Administrative Templates\Advanced settings	Multimedia		
USER	Administrative Templates\Advanced settings	Printing		
USER	Administrative Templates\Advanced settings	Searching		
USER	Administrative Templates\Advanced settings	Security		
USER	Administrative Templates\Advanced settings	Signup Settings		
USER	Administrative Templates\AutoComplete	AutoComplete Settings		
USER	Administrative Templates\Control Panel	Hide specified Control Panel applets	At least Microsoft Windows 2000	Hides specified Control Panel items and folders. This setting removes Control Panel items (such as Display) and folders (such as Fonts) from the Control Panel window and the Start menu. It can remove Control Panel items you have added to your system, as well as Control Panel items included in Windows 2000 Professional and Windows XP Professional. To hide a Control Panel item, type the file name of the item, such as Ncpa.cpl (for Network). To hide a folder, type the folder name, such as Fonts. This setting affects the Start menu and Control Panel window only. It does not prevent users from running Control Panel items. Also, see the Remove Display in Control Panel setting in User Configuration\Administrative Templates\Control Panel\Display. If both the Hide specified Control Panel applets setting and the Show only specified Control Panel applets setting are enabled, and the same item appears in both lists, the Show only specified Control Panel applets

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				setting is ignored. Note: To find the file name of a Control Panel item, search for files with the .cpl file name extension in the %Systemroot%\System32 directory. Note: To create a list of disallowed Control Panel applets, click Show, click Add, and then enter the Control Panel file name (ends with .cpl) or the name displayed under that item in the Control Panel. (e.g., desk.cpl, powercfg.cpl, Printers and Faxes) Note: This setting does not affect the Categories that are displayed in the new Control Panel Category view in Windows XP. If you want to control which items are displayed in Control Panel, enable the Force classic Control Panel Style setting to remove the Category view, and then use this setting to control which .cpls are not displayed.
USER	Administrative Templates\Control Panel	Force classic Control Panel Style	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting affects the visual style and presentation of the Control Panel. It allows you to disable the new style of Control Panel, which is task-based, and use the Windows 2000 style, referred to as the classic Control Panel. The new Control Panel, referred to as the simple Control Panel, simplifies how users interact with settings by providing easy-to-understand tasks that help users get their work done quickly. The Control Panel allows the users to configure their computer, add or remove programs, and change settings. If you enable this setting, Control Panel sets the classic Control Panel. The user cannot switch to the new simple style. If you disable this setting, Control Panel is set to the task-based style. The user cannot switch to the classic Control Panel style. If you do not configure it, the default is the task-based style, which the user can change.
USER	Administrative Templates\Control Panel	Prohibit access to the Control Panel	At least Microsoft Windows 2000	Disables all Control Panel programs. This setting prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot start Control Panel or run any Control Panel items. This setting also removes Control Panel from the Start menu. (To open Control Panel, click Start, point to Settings, and then click Control Panel.) This setting also removes the Control Panel folder from Windows Explorer. If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action. Also, see the Remove Display in Control Panel and Remove programs on Settings menu settings.
USER	Administrative Templates\Control Panel	Show only specified Control Panel applets	At least Microsoft Windows 2000	Hides all Control Panel items and folders except those specified in this setting. This setting removes all Control Panel items (such as Network) and folders (such as Fonts) from the Control Panel window and the Start menu. It removes Control Panel items you have added to your system,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				as well the Control Panel items included in Windows 2000 and Windows XP Professional. The only items displayed in Control Panel are those you specify in this setting. To display a Control Panel item, type the file name of the item, such as Ncpa.cpl (for Network). To display a folder, type the folder name, such as Fonts. This setting affects the Start menu and Control Panel window only. It does not prevent users from running any Control Panel items. Also, see the Remove Display in Control Panel setting in User Configuration\Administrative Templates\Control Panel\Display. If both the Hide specified Control Panel applets setting and the Show only specified Control Panel applets setting are enabled, the Show only specified Control Panel applets setting is ignored. Tip: To find the file name of a Control Panel item, search for files with the .cpl file name extension in the %Systemroot%\System32 directory.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Specify default category for Add New Programs	At least Microsoft Windows 2000	Specifies the category of programs that appears when users open the Add New Programs page. If you enable this setting, only the programs in the category you specify are displayed when the Add New Programs page opens. Users can use the Category box on the Add New Programs page to display programs in other categories. To use this setting, type the name of a category in the Category box for this setting. You must enter a category that is already defined in Add or Remove Programs. To define a category, use Software Installation. If you disable this setting or do not configure it, all programs (Category: All) are displayed when the Add New Programs page opens. You can use this setting to direct users to the programs they are most likely to need. Note: This setting is ignored if either the Remove Add or Remove Programs setting or the Hide Add New Programs page setting is enabled.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Hide the Add a program from CD-ROM or floppy disk option	At least Microsoft Windows 2000	Removes the Add a program from CD-ROM or floppy disk section from the Add New Programs page. This prevents users from using Add or Remove Programs to install programs from removable media. If you disable this setting or do not configure it, the Add a program from CD-ROM or floppy disk option is available to all users. This setting does not prevent users from using other tools and methods to add or remove program components. Note: If the Hide Add New Programs page setting is enabled, this setting is ignored. Also, if the Prevent removable media source for any install setting (located in User Configuration\Administrative Templates\Windows Components\Windows Installer) is enabled, users cannot add programs from removable media, regardless of this setting.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Control Panel\Add or Remove Programs	Hide the Add programs from Microsoft option	At least Microsoft Windows 2000	Removes the Add programs from Microsoft section from the Add New Programs page. This setting prevents users from using Add or Remove Programs to connect to Windows Update. If you disable this setting or do not configure it, Add programs from Microsoft is available to all users. This setting does not prevent users from using other tools and methods to connect to Windows Update. Note: If the Hide Add New Programs page setting is enabled, this setting is ignored.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Hide the Add programs from your network option	At least Microsoft Windows 2000	Prevents users from viewing or installing published programs. This setting removes the Add programs from your network section from the Add New Programs page. The Add programs from your network section lists published programs and provides an easy way to install them. Published programs are those programs that the system administrator has explicitly made available to the user with a tool such as Windows Installer. Typically, system administrators publish programs to notify users that the programs are available, to recommend their use, or to enable users to install them without having to search for installation files. If you enable this setting, users cannot tell which programs have been published by the system administrator, and they cannot use Add or Remove Programs to install published programs. However, they can still install programs by using other methods, and they can view and install assigned (partially installed) programs that are offered on the desktop or on the Start menu. If you disable this setting or do not configure it, Add programs from your network is available to all users. Note: If the Hide Add New Programs page setting is enabled, this setting is ignored.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Hide Add New Programs page	At least Microsoft Windows 2000	Removes the Add New Programs button from the Add or Remove Programs bar. As a result, users cannot view or change the attached page. The Add New Programs button lets users install programs published or assigned by a system administrator. If you disable this setting or do not configure it, the Add New Programs button is available to all users. This setting does not prevent users from using other tools and methods to install programs.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Remove Add or Remove Programs	At least Microsoft Windows 2000	Prevents users from using Add or Remove Programs. This setting removes Add or Remove Programs from Control Panel and removes the Add or Remove Programs item from menus. Add or Remove Programs lets users install, uninstall, repair, add, and remove features and components of Windows 2000 Professional and a wide variety of Windows programs. Programs published or assigned to the user appear in Add or Remove Programs. If you disable this setting or do not

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				configure it, Add or Remove Programs is available to all users. When enabled, this setting takes precedence over the other settings in this folder. This setting does not prevent users from using other tools and methods to install or uninstall programs.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Hide the Set Program Access and Defaults page	At least Microsoft Windows 2000 Service Pack 3 or Microsoft Windows XP Professional Service Pack 1	Removes the Set Program Access and Defaults button from the Add or Remove Programs bar. As a result, users cannot view or change the associated page. The Set Program Access and Defaults button lets administrators specify default programs for certain activities, such as Web browsing or sending e-mail, as well as which programs are accessible from the Start menu, desktop, and other locations. If you disable this setting or do not configure it, the Set Program Access and Defaults button is available to all users. This setting does not prevent users from using other tools and methods to change program access or defaults. This setting does not prevent the Set Program Access and Defaults icon from appearing on the Start menu. See the Remove Set Program Access and Defaults from Start menu setting.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Hide Change or Remove Programs page	At least Microsoft Windows 2000	Removes the Change or Remove Programs button from the Add or Remove Programs bar. As a result, users cannot view or change the attached page. The Change or Remove Programs button lets users uninstall, repair, add, or remove features of installed programs. If you disable this setting or do not configure it, the Change or Remove Programs page is available to all users. This setting does not prevent users from using other tools and methods to delete or uninstall programs.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Go directly to Components Wizard	At least Microsoft Windows 2000	Prevents users from using Add or Remove Programs to configure installed services. This setting removes the Set up services section of the Add/Remove Windows Components page. The Set up services section lists system services that have not been configured and offers users easy access to the configuration tools. If you disable this setting or do not configure it, Set up services appears only when there are unconfigured system services. If you enable this setting, Set up services never appears. This setting does not prevent users from using other methods to configure services. Note: When Set up services does not appear, clicking the Add/Remove Windows Components button starts the Windows Component Wizard immediately. Because the only remaining option on the Add/Remove Windows Components page starts the wizard, that option is selected automatically, and the page is bypassed. To remove Set up services and prevent the Windows

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Component Wizard from starting, enable the Hide Add/Remove Windows Components page setting. If the Hide Add/Remove Windows Components page setting is enabled, this setting is ignored.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Remove Support Information	At least Microsoft Windows 2000	Removes links to the Support Info dialog box from programs on the Change or Remove Programs page. Programs listed on the Change or Remove Programs page can include a Click here for support information hyperlink. When clicked, the hyperlink opens a dialog box that displays troubleshooting information, including a link to the installation files and data that users need to obtain product support, such as the Product ID and version number of the program. The dialog box also includes a hyperlink to support information on the Internet, such as the Microsoft Product Support Services Web page. If you disable this setting or do not configure it, the Support Info hyperlink appears. Note: Not all programs provide a support information hyperlink.
USER	Administrative Templates\Control Panel\Add or Remove Programs	Hide Add/Remove Windows Components page	At least Microsoft Windows 2000	Removes the Add/Remove Windows Components button from the Add or Remove Programs bar. As a result, users cannot view or change the associated page. The Add/Remove Windows Components button lets users configure installed services and use the Windows Component Wizard to add, remove, and configure components of Windows from the installation files. If you disable this setting or do not configure it, the Add/Remove Windows Components button is available to all users. This setting does not prevent users from using other tools and methods to configure services or add or remove program components. However, this setting blocks user access to the Windows Component Wizard.
USER	Administrative Templates\Control Panel\Display	Remove Display in Control Panel	At least Microsoft Windows 2000	Disables Display in Control Panel. If you enable this setting, Display in Control Panel does not run. When users try to start Display, a message appears explaining that a setting prevents the action. Also, see the Prohibit access to the Control Panel (User Configuration\Administrative Templates\Control Panel) and Remove programs on Settings menu (User Configuration\Administrative Templates\Start Menu & Taskbar) settings.
USER	Administrative Templates\Control Panel\Display	Hide Appearance and Themes tab	At least Microsoft Windows 2000	Removes the Appearance and Themes tabs from Display in Control Panel. When this setting is enabled, it removes the desktop color selection option from the Desktop tab. This setting prevents users from using Control Panel to change the colors or color scheme of the desktop and windows. If this setting is disabled or not configured, the Appearance and Themes tabs are available in Display in Control Panel.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Control Panel\Display	Hide Desktop tab	At least Microsoft Windows 2000	Removes the Desktop tab from Display in Control Panel. This setting prevents users from using Control Panel to change the pattern and wallpaper on the desktop. Enabling this setting also prevents the user from customizing the desktop by changing icons or adding new Web content through Control Panel.
USER	Administrative Templates\Control Panel\Display	Hide Screen Saver tab	At least Microsoft Windows 2000	Removes the Screen Saver tab from Display in Control Panel. This setting prevents users from using Control Panel to add, configure, or change the screen saver on the computer.
USER	Administrative Templates\Control Panel\Display	Hide Settings tab	At least Microsoft Windows 2000	Removes the Settings tab from Display in Control Panel. This setting prevents users from using Control Panel to add, configure, or change the display settings on the computer.
USER	Administrative Templates\Control Panel\Display	Restrict display		
USER	Administrative Templates\Control Panel\Display	Screen Saver	At least Microsoft Windows 2000 Service Pack 1	Enables desktop screen savers. If you disable this setting, screen savers do not run. Also, this setting disables the Screen Saver section of the Screen Saver tab in Display in Control Panel. As a result, users cannot change the screen saver options. If you do not configure it, this setting has no effect on the system. If you enable it, a screen saver runs, provided the following two conditions hold: First, a valid screensaver on the client is specified through the Screensaver executable name setting or through Control Panel on the client computer. Second, the screensaver timeout is set to a nonzero value through the setting or Control Panel. Also, see the Hide Screen Saver tab setting.
USER	Administrative Templates\Control Panel\Display	Screen Saver executable name	At least Microsoft Windows 2000 Service Pack 1	Specifies the screen saver for the user's desktop. If you enable this setting, the system displays the specified screen saver on the user's desktop. Also, this setting disables the drop-down list of screen savers on the Screen Saver tab in Display in Control Panel, which prevents users from changing the screen saver. If you disable this setting or do not configure it, users can select any screen saver. If you enable this setting, type the name of the file that contains the screen saver, including the .scr file name extension. If the screen saver file is not in the %Systemroot%\System32 directory, type the fully qualified path to the file. If the specified screen saver is not installed on a computer to which this setting applies, the setting is ignored. Note: This setting can be superseded by the Screen Saver setting. If the Screen Saver setting is disabled, this setting is ignored, and screen savers do not run.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Control Panel\Display	Password protect the screen saver	At least Microsoft Windows 2000 Service Pack 1	Determines whether screen savers used on the computer are password protected. If you enable this setting, all screen savers are password protected. If you disable this setting, password protection cannot be set on any screen saver. This setting also disables the Password protected check box on the Screen Saver tab in Display in Control Panel, preventing users from changing the password protection setting. If you do not configure this setting, users can choose whether or not to set password protection on each screen saver. To ensure that a computer will be password protected, also enable the Screen Saver setting and specify a timeout via the Screen Saver timeout setting. Note: To remove the Screen Saver tab, use the Hide Screen Saver tab setting.
USER	Administrative Templates\Control Panel\Display	Screen Saver timeout	At least Microsoft Windows 2000 Service Pack 1	Specifies how much user idle time must elapse before the screen saver is launched. When configured, this idle time can be set from a minimum of 1 second to a maximum of 86,400 seconds, or 24 hours. If set to zero, the screen saver will not be started. This setting has no effect under any of the following circumstances: - The setting is disabled or not configured. - The wait time is set to zero. - The No screen saver setting is enabled. - Neither the Screen saver executable name setting nor the Screen Saver tab of the client computer's Display Properties dialog box specifies a valid existing screensaver program on the client. When not configured, whatever wait time is set on the client through the Screen Saver tab of the Display Properties dialog box is used. The default is 15 minutes.
USER	Administrative Templates\Control Panel\Display	Prevent changing wallpaper	At least Microsoft Windows 2000	Prevents users from adding or changing the background design of the desktop. By default, users can use the Desktop tab of Display in Control Panel to add a background design (wallpaper) to their desktop. If you enable this setting, the Desktop tab still appears, but all options on the tab are disabled. To remove the Desktop tab, use the Hide Desktop tab setting. To specify wallpaper for a group, use the Active Desktop Wallpaper setting. Also, see the Allow only bitmapped wallpaper setting.
USER	Administrative Templates\Control Panel\Display\Desktop Themes	Prohibit Theme color selection	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting forces the theme color to be the default color scheme. If you enable this setting, a user cannot change the color scheme of the current desktop theme. If you disable or do not configure this setting, a user may change the color scheme of the current desktop theme.
USER	Administrative Templates\Control Panel\Display\Desktop Themes	Remove Theme option	At least Microsoft Windows XP	This setting effects the Themes tab that controls the overall appearance of windows. It is accessed through the Display icon in Control Panel.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			Professional or Windows Server 2003 family	Using the options under the Themes tab, users can configure the theme for their desktop. If you enable this setting, it removes the Themes tab. If you disable or do not configure this setting, there is no effect. Note: If you enable this setting but do not set a theme, the theme defaults to whatever the user previously set.
USER	Administrative Templates\Control Panel\Display\Desktop Themes	Prevent selection of windows and buttons styles	At least Microsoft Windows XP Professional or Windows Server 2003 family	Prevents users from changing the visual style of the windows and buttons displayed on their screens. When enabled, this setting disables the Windows and buttons drop-down list on the Appearance tab in Display Properties.
USER	Administrative Templates\Control Panel\Display\Desktop Themes	Load a specific visual style file or force Windows Classic	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting allows you to load a specific visual style file by entering the path (location) of the visual style file. This can be a local computer visual style (Luna.msstyles), or a file located on a remote server using a UNC path (\\Server\Share\luna.msstyles). If you enable this setting, the visual style file that you specify will be used. Also, a user may not choose to use a different visual style. If you disable or do not configure this setting, the users can select the visual style that they want to use for their desktop. Note: If this setting is enabled and the file is not available at user logon, the default visual style is loaded. Note: When running Windows XP, you can select the Luna visual style by typing %windir%\resources\Themes\Luna\Luna.msstyles Note: To select the Windows Classic visual style, leave the box blank beside Path to Visual Style: and enable this setting.
USER	Administrative Templates\Control Panel\Display\Desktop Themes	Prohibit selection of font size	At least Microsoft Windows XP Professional or Windows Server 2003 family	Prevents users from changing the size of the font in the windows and buttons displayed on their screens. If this setting is enabled, the Font size drop-down list on the Appearance tab in Display Properties is disabled. If you disable or do not configure this setting, a user may change the font size using the Font size drop-down list on the Appearance tab.
USER	Administrative Templates\Control Panel\Printers	Browse the network to find printers	At least Microsoft Windows 2000	Allows users to use the Add Printer Wizard to search the network for shared printers. If you enable this setting or do not configure it, when users choose to add a network printer by selecting the A network printer, or a printer attached to another computer radio button on Add Printer Wizard's page 2, and also check the Connect to this printer (or to browse for a printer, select this option and click Next) radio button on Add Printer Wizard's page 3, and do not specify a printer name in the adjacent Name edit box, then Add Printer Wizard displays the list of shared printers on the network and invites to choose a printer from the shown list. If you

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				disable this setting, the network printer browse page is removed from within the Add Printer Wizard, and users cannot search the network but must type a printer name. Note: This setting affects the Add Printer Wizard only. It does not prevent users from using other programs to search for shared printers or to connect to network printers.
USER	Administrative Templates\Control Panel\Printers	Browse a common web site to find printers	At least Microsoft Windows 2000	Adds a link to an Internet or intranet Web page to the Add Printer Wizard. You can use this setting to direct users to a Web page from which they can install printers. If you enable this setting and type an Internet or intranet address in the text box, the system adds a Browse button to the Specify a Printer page in the Add Printer Wizard. The Browse button appears beside the Connect to a printer on the Interner or on a home or office network option. When users click Browse, the system opens an Internet browser and navigates to the specified URL address to display the available printers. This setting makes it easy for users to find the printers you want them to add. Also, see the Custom support URL in the Printers folder's left pane and Web-based printing settings in Computer Configuration\Administrative Templates\Printers.
USER	Administrative Templates\Control Panel\Printers	Prevent addition of printers	At least Microsoft Windows 2000	Prevents users from using familiar methods to add local and network printers. This setting removes the Add Printer option from the Start menu. (To find the Add Printer option, click Start, click Printers, and then click Add Printer.) This setting also removes Add Printer from the Printers folder in Control Panel. Also, users cannot add printers by dragging a printer icon into the Printers folder. If they try, a message appears explaining that the setting prevents the action. However, this setting does not prevent users from using the Add Hardware Wizard to add a printer. Nor does it prevent users from running other programs to add printers. This setting does not delete printers that users have already added. However, if users have not added a printer when this setting is applied, they cannot print. Note: You can use printer permissions to restrict the use of printers without specifying a setting. In the Printers folder, right-click a printer, click Properties, and then click the Security tab.
USER	Administrative Templates\Control Panel\Printers	Prevent deletion of printers	At least Microsoft Windows 2000	Prevents users from deleting local and network printers. If a user tries to delete a printer, such as by using the Delete option in Printers in Control Panel, a message appears explaining that a setting prevents the action. This setting does not prevent users from running other programs to delete a printer.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Control Panel\Printers	Point and Print Restrictions	At least Microsoft Windows XP Professional with SP1 or Windows Server 2003 family	This policy setting restricts the servers that a client can connect to for point and print. The policy setting applies only to non Print Administrators clients, and only to machines that are members of a domain. When the policy setting is enabled, the client can be restricted to only point and print to a server within its own forest, and/or to a list of explicitly trusted servers. When the policy setting is not-configured, it defaults to allowing point and print only within the client's forest. When the policy setting is disabled, client machines can point and print to any server.
USER	Administrative Templates\Control Panel\Printers	Default Active Directory path when searching for printers	At least Microsoft Windows 2000	Specifies the Active Directory location where searches for printers begin. The Add Printer Wizard gives users the option of searching Active Directory for a shared printer. If you enable this setting, these searches begin at the location you specify in the Default Active Directory path box. Otherwise, searches begin at the root of Active Directory. This setting only provides a starting point for Active Directory searches for printers. It does not restrict user searches through Active Directory.
USER	Administrative Templates\Control Panel\Regional and Language Options	Restrict selection of Windows menus and dialogs language	At least Microsoft Windows 2000	This setting restricts users to the specified language by disabling the menus and dialog box controls in the Regional and Language Options Control Panel. If the specified language is not installed on the target computer, the language selection defaults to English.
USER	Administrative Templates\Desktop	Color scheme		
USER	Administrative Templates\Desktop	Prohibit user from changing My Documents path	At least Microsoft Windows 2000	Prevents users from changing the path to the My Documents folder. By default, a user can change the location of the My Documents folder by typing a new path in the Target box of the My Documents Properties dialog box. If you enable this setting, users are unable to type a new location in the Target box.
USER	Administrative Templates\Desktop	Hide and disable all items on the desktop	At least Microsoft Windows 2000	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. Also, see Items displayed in Places Bar in User Configuration\Administrative Templates\Windows Components\Common Open File Dialog to remove the Desktop icon from the Places Bar. This will help prevent users from saving data to the Desktop.
USER	Administrative Templates\Desktop	Remove the Desktop Cleanup Wizard	At least Microsoft Windows XP Professional or	Prevents users from using the Desktop Cleanup Wizard. If you enable this setting, the Desktop Cleanup wizard does not automatically run on a users workstation every 60 days. The user will also not be able to access

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			Windows Server 2003 family	the Desktop Cleanup Wizard. If you disable this setting or do not configure it, the default behavior of the Desktop Clean Wizard running every 60 days occurs. Note: When this setting is not enabled, users can run the Desktop Cleanup Wizard, or have it run automatically every 60 days from Display, by clicking the Desktop tab and then clicking the Customize Desktop button.
USER	Administrative Templates\Desktop	Hide Internet Explorer icon on desktop	At least Microsoft Windows 2000	Removes the Internet Explorer icon from the desktop and from the Quick Launch bar on the taskbar. This setting does not prevent the user from starting Internet Explorer by using other methods.
USER	Administrative Templates\Desktop	Remove My Computer icon on the desktop	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting 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 via the Up button while this setting is enabled, they view an empty My Computer folder. This setting allows administrators to restrict their users from seeing My Computer in the shell namespace, allowing them to present their users with a simpler desktop environment. If you enable this setting, My Computer is hidden on the desktop, the new Start menu, the Explorer folder tree pane, and the Explorer Web views. If the user manages to navigate to My Computer, the folder will be empty. If you disable this setting, My Computer is displayed as usual, appearing as normal on the desktop, Start menu, folder tree pane, and Web views, unless restricted by another setting. If you do not configure this setting, the default is to display My Computer as usual. 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	Administrative Templates\Desktop	Remove My Documents icon on the desktop	At least Microsoft Windows 2000	Removes most occurrences of the My Documents icon. This setting removes the My Documents icon from the desktop, from Windows Explorer, from programs that use the Windows Explorer windows, and from the standard Open dialog box. This setting does not prevent the user from using other methods to gain access to the contents of the My Documents folder. This setting does not remove the My Documents icon from the Start menu. To do so, use the Remove My Documents icon from Start Menu setting. Note: To make changes to this setting effective, you must log off from and log back on to Windows 2000 Professional.
USER	Administrative Templates\Desktop	Hide My Network	At least Microsoft	Removes the My Network Places icon from the desktop. This setting only affects the desktop icon. It does not prevent users from connecting

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
		Places icon on desktop	Windows 2000	to the network or browsing for shared computers on the network.
USER	Administrative Templates\Desktop	Remove Properties from the My Computer context menu	At least Microsoft Windows 2000 Service Pack 3	This setting hides Properties on the context menu for My Computer. If you enable this setting, the Properties option will not be present when the user right-clicks My Computer or clicks My Computer and then goes to the File menu. Likewise, Alt-Enter does nothing when My Computer is selected. If you disable or do not configure this setting, the Properties option is displayed as usual.
USER	Administrative Templates\Desktop	Remove Properties from the My Documents context menu	At least Microsoft Windows 2000 Service Pack 3	This setting hides Properties for the context menu on My Documents. If you enable this setting, the Properties option will not be present when the user right-clicks My Documents or clicks My Documents and then goes to the File menu. Likewise, Alt-Enter does nothing when My Documents is selected. If you disable or do not configure this setting, the Properties option is displayed as usual.
USER	Administrative Templates\Desktop	Do not add shares of recently opened documents to My Network Places	At least Microsoft Windows 2000	Remote shared folders are not added to My Network Places whenever you open a document in the shared folder. If you disable this setting or do not configure it, when you open a document in a remote shared folder, the system adds a connection to the shared folder to My Network Places. If you enable this setting, shared folders are not added to My Network Places automatically when you open a document in the shared folder.
USER	Administrative Templates\Desktop	Remove Recycle Bin icon from desktop	At least Microsoft Windows XP Professional or Windows Server 2003 family	Removes most occurrences of the Recycle Bin icon. This setting removes the Recycle Bin icon from the desktop, from Windows Explorer, from programs that use the Windows Explorer windows, and from the standard Open dialog box. This setting does not prevent the user from using other methods to gain access to the contents of the Recycle Bin folder. Note: To make changes to this setting effective, you must log off and then log back on.
USER	Administrative Templates\Desktop	Remove Properties from the Recycle Bin context menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	Removes the Properties option from the Recycle Bin context menu. If you enable this setting, the Properties option will not be present when the user right-clicks on Recycle Bin or opens Recycle Bin and then clicks File. Likewise, Alt-Enter does nothing when Recycle Bin is selected. If you disable or do not configure this setting, the Properties option is displayed as usual.
USER	Administrative Templates\Desktop	Don't save settings at exit	At least Microsoft Windows 2000	Prevents users from saving certain changes to the desktop. If you enable this setting, users can change the desktop, but some changes, such as the position of open windows or the size and position of the taskbar, are not saved when users log off. However, shortcuts placed on

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				the desktop are always saved.
USER	Administrative Templates\Desktop	Prevent adding, dragging, dropping and closing the Taskbar's toolbars	At least Microsoft Windows 2000	Prevents users from manipulating desktop toolbars. If you enable this setting, users cannot add or remove toolbars from the desktop. Also, users cannot drag toolbars on to or off of docked toolbars. Note: If users have added or removed toolbars, this setting prevents them from restoring the default configuration. Tip: To view the toolbars that can be added to the desktop, right-click a docked toolbar (such as the taskbar beside the Start button), and point to Toolbars. Also, see the Prohibit adjusting desktop toolbars setting.
USER	Administrative Templates\Desktop	Prohibit adjusting desktop toolbars	At least Microsoft Windows 2000	Prevents users from adjusting the length of desktop toolbars. Also, users cannot reposition items or toolbars on docked toolbars. This setting does not prevent users from adding or removing toolbars on the desktop. Note: If users have adjusted their toolbars, this setting prevents them from restoring the default configuration. Also, see the Prevent adding, dragging, dropping and closing the Taskbar's toolbars setting.
USER	Administrative Templates\Desktop	Wallpaper		
USER	Administrative Templates\Desktop\Active Desktop	Enable Active Desktop	At least Microsoft Windows 2000	Enables Active Desktop and prevents users from disabling it. This setting prevents users from trying to enable or disable Active Desktop while a policy controls it. If you disable this setting or do not configure it, Active Desktop is disabled by default, but users can enable it. Note: If both the Enable Active Desktop setting and the Disable Active Desktop setting are enabled, the Disable Active Desktop setting is ignored. If the Turn on Classic Shell setting (in User Configuration\Administrative Templates\Windows Components\Windows Explorer) is enabled, Active Desktop is disabled, and both of these policies are ignored.
USER	Administrative Templates\Desktop\Active Desktop	Disable Active Desktop	At least Microsoft Windows 2000	Disables Active Desktop and prevents users from enabling it. This setting prevents users from trying to enable or disable Active Desktop while a policy controls it. If you disable this setting or do not configure it, Active Desktop is disabled by default, but users can enable it. Note: If both the Enable Active Desktop setting and the Disable Active Desktop setting are enabled, the Disable Active Desktop setting is ignored. If the Turn on Classic Shell setting (in User Configuration\Administrative Templates\Windows Components\Windows Explorer) is enabled, Active Desktop is disabled, and both these policies are ignored.
USER	Administrative Templates\Desktop\Active Desktop	Prohibit changes	At least Microsoft Windows 2000	Prevents the user from enabling or disabling Active Desktop or changing the Active Desktop configuration. This is a comprehensive setting that

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				locks down the configuration you establish by using other policies in this folder. This setting removes the Web tab from Display in Control Panel. As a result, users cannot enable or disable Active Desktop. If Active Desktop is already enabled, users cannot add, remove, or edit Web content or disable, lock, or synchronize Active Desktop components.
USER	Administrative Templates\Desktop\Active Desktop	Add/Delete items	At least Microsoft Windows 2000	Adds and deletes specified Web content items. You can use the Add box in this setting to add particular Web-based items or shortcuts to users' desktops. Users can close or delete the items (if settings allow), but the items are added again each time the setting is refreshed. You can also use this setting to delete particular Web-based items from users' desktops. Users can add the item again (if settings allow), but the item is deleted each time the setting is refreshed. Note: Removing an item from the Add list for this setting is not the same as deleting it. Items that are removed from the Add list are not removed from the desktop. They are simply not added again. Note: For this setting to take affect, you must log off and log on to the system.
USER	Administrative Templates\Desktop\Active Desktop	Prohibit adding items	At least Microsoft Windows 2000	Prevents users from adding Web content to their Active Desktop. This setting removes the New button from Web tab in Display in Control Panel. As a result, users cannot add Web pages or pictures from the Internet or an intranet to the desktop. This setting does not remove existing Web content from their Active Desktop, or prevent users from removing existing Web content. Also, see the Disable all items setting.
USER	Administrative Templates\Desktop\Active Desktop	Prohibit closing items	At least Microsoft Windows 2000	Prevents users from removing Web content from their Active Desktop. In Active Desktop, you can add items to the desktop but close them so they are not displayed. If you enable this setting, items added to the desktop cannot be closed; they always appear on the desktop. This setting removes the check boxes from items on the Web tab in Display in Control Panel. Note: This setting does not prevent users from deleting items from their Active Desktop.
USER	Administrative Templates\Desktop\Active Desktop	Prohibit deleting items	At least Microsoft Windows 2000	Prevents users from deleting Web content from their Active Desktop. This setting removes the Delete button from the Web tab in Display in Control Panel. As a result, users can temporarily remove, but not delete, Web content from their Active Desktop. This setting does not prevent users from adding Web content to their Active Desktop. Also, see the Prohibit closing items and Disable all items settings.
USER	Administrative Templates\Desktop\Active Desktop	Prohibit editing items	At least Microsoft Windows 2000	Prevents users from changing the properties of Web content items on their Active Desktop. This setting disables the Properties button on the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Web tab in Display in Control Panel. Also, it removes the Properties item from the menu for each item on the Active Desktop. As a result, users cannot change the properties of an item, such as its synchronization schedule, password, or display characteristics.
USER	Administrative Templates\Desktop\Active Desktop	Disable all items	At least Microsoft Windows 2000	Removes Active Desktop content and prevents users from adding Active Desktop content. This setting removes all Active Desktop items from the desktop. It also removes the Web tab from Display in Control Panel. As a result, users cannot add Web pages or pictures from the Internet or an intranet to the desktop. Note: This setting does not disable Active Desktop. Users can still use image formats, such as JPEG and GIF, for their desktop wallpaper.
USER	Administrative Templates\Desktop\Active Desktop	Allow only bitmapped wallpaper	At least Microsoft Windows 2000	Permits only bitmap images for wallpaper. This setting limits the desktop background (wallpaper) to bitmap (.bmp) files. If users select files with other image formats, such as JPEG, GIF, PNG, or HTML, through the Browse button on the Desktop tab, the wallpaper does not load. Files that are autoconverted to a .bmp format, such as JPEG, GIF, and PNG, can be set as Wallpaper by right-clicking the image and selecting Set as Wallpaper. Also, see the Active Desktop Wallpaper and the Prevent changing wallpaper (in User Configuration\Administrative Templates\Control Panel\Display) settings.
USER	Administrative Templates\Desktop\Active Desktop	Active Desktop Wallpaper	At least Microsoft Windows 2000	Specifies the desktop background (wallpaper) displayed on all users' desktops. This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp), JPEG (*.jpg), or HTML (*.htm, *.html) file. To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternative wallpaper. You can also use this setting to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification. If you disable this setting or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice. Also, see the Allow only bitmapped wallpaper in the same location, and the Prevent changing wallpaper setting in User Configuration\Administrative Templates\Control Panel. Note: You need to enable the Active Desktop to use this setting. Note: This setting does not apply to Terminal Server sessions.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Desktop\Active Directory	Enable filter in Find dialog box	At least Microsoft Windows 2000	Displays the filter bar above the results of an Active Directory search. The filter bar consists of buttons for applying additional filters to search results. If you enable this setting, the filter bar appears when the Active Directory Find dialog box opens, but users can hide it. If you disable this setting or do not configure it, the filter bar does not appear, but users can display it by selecting Filter on the View menu. To see the filter bar, open My Network Places, click Entire Network, and then click Directory. Right-click the name of a Windows domain, and click Find. Type the name of an object in the directory, such as Administrator. If the filter bar does not appear above the resulting display, on the View menu, click Filter.
USER	Administrative Templates\Desktop\Active Directory	Hide Active Directory folder	Only works on Microsoft Windows 2000	Hides the Active Directory folder in My Network Places. The Active Directory folder displays Active Directory objects in a browse window. If you enable this setting, the Active Directory folder does not appear in the My Network Places folder. If you disable this setting or do not configure it, the Active Directory folder appears in the My Network Places folder. This setting is designed to let users search Active Directory but not tempt them to casually browse Active Directory.
USER	Administrative Templates\Desktop\Active Directory	Maximum size of Active Directory searches	At least Microsoft Windows 2000	Specifies the maximum number of objects the system displays in response to a command to browse or search Active Directory. This setting affects all browse displays associated with Active Directory, such as those in Local Users and Groups, Active Directory Users and Computers, and dialog boxes used to set permissions for user or group objects in Active Directory. If you enable this setting, you can use the Number of objects returned box to limit returns from an Active Directory search. If you disable this setting or do not configure it, the system displays up to 10,000 objects. This consumes approximately 2 MB of memory or disk space. This setting is designed to protect the network and the domain controller from the effect of expansive searches.
USER	Administrative Templates\Display settings	Text Size		
USER	Administrative Templates\Display settings	General Colors		
USER	Administrative Templates\Display settings	Link colors		
USER	Administrative Templates\IE	INETCORP.ADM		

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Maintenance Only			
USER	Administrative Templates\Network\Network Connections	Prohibit adding and removing components for a LAN or remote access connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether administrators can add and remove network components for a LAN or remote access connection. This setting has no effect on nonadministrators. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Install and Uninstall buttons for components of connections are disabled, and administrators are not permitted to access network components in the Windows Components Wizard. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Install and Uninstall buttons for components of connections in the Network Connections folder are enabled. Also, administrators can gain access to network components in the Windows Components Wizard. The Install button opens the dialog boxes used to add network components. Clicking the Uninstall button removes the selected component in the components list (above the button). The Install and Uninstall buttons appear in the properties dialog box for connections. These buttons are on the General tab for LAN connections and on the Networking tab for remote access connections. Note: When the Prohibit access to properties of a LAN connection, Ability to change properties of an all user remote access connection, or Prohibit changing properties of a private remote access connection settings are set to deny access to the connection properties dialog box, the Install and Uninstall buttons for connections are blocked. Note: Nonadministrators are already prohibited from adding and removing connection components, regardless of this setting.
USER	Administrative Templates\Network\Network Connections	Prohibit access to the Advanced Settings item on the Advanced menu	At least Microsoft Windows 2000 Service Pack 1	Determines whether the Advanced Settings item on the Advanced menu in Network Connections is enabled for administrators. The Advanced Settings item lets users view and change bindings and view and change the order in which the computer accesses connections, network providers, and print providers. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Advanced Settings item is disabled for administrators. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Advanced Settings item is enabled for administrators. Note: Nonadministrators are already prohibited from accessing the Advanced Settings dialog box, regardless of this setting.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Network\Network Connections	Prohibit TCP/IP advanced configuration	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can configure advanced TCP/IP settings. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Advanced button on the Internet Protocol (TCP/IP) Properties dialog box is disabled for all users (including administrators). As a result, users cannot open the Advanced TCP/IP Settings Properties page and modify IP settings, such as DNS and WINS server information. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting, the Advanced button is enabled, and all users can open the Advanced TCP/IP Setting dialog box. Note: This setting is superseded by settings that prohibit access to properties of connections or connection components. When these policies are set to deny access to the connection properties dialog box or Properties button for connection components, users cannot gain access to the Advanced button for TCP/IP configuration. Note: Nonadministrators (excluding Network Configuration Operators) do not have permission to access TCP/IP advanced configuration for a LAN connection, regardless of this setting. Tip: To open the Advanced TCP/IP Setting dialog box, in the Network Connections folder, right-click a connection icon, and click Properties. For remote access connections, click the Networking tab. In the Components checked are used by this connection box, click Internet Protocol (TCP/IP), click the Properties button, and then click the Advanced button. Note: Changing this setting from Enabled to Not Configured does not enable the Advanced button until the user logs off.
USER	Administrative Templates\Network\Network Connections	Prohibit Enabling/Disabling components of a LAN connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether administrators can enable and disable the components used by LAN connections. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the check boxes for enabling and disabling components are disabled. As a result, administrators cannot enable or disable the components that a connection uses. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Properties dialog box for a connection includes a check box beside the name of each component that the connection uses. Selecting the check box enables the component, and clearing the check box disables the component. Note: When the Prohibit access to properties of a LAN connection setting is enabled, users are blocked from accessing the check boxes for

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				enabling and disabling the components of a LAN connection. Note: Nonadministrators are already prohibited from enabling or disabling components for a LAN connection, regardless of this setting.
USER	Administrative Templates\Network\Network Connections	Ability to delete all user remote access connections	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can delete all user remote access connections. To create an all-user remote access connection, on the Connection Availability page in the New Connection Wizard, click the For all users option. If you enable this setting, all users can delete shared remote access connections. In addition, if your file system is NTFS, users need to have Write access to Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk to delete a shared remote access connection. If you disable this setting (and enable the Enable Network Connections settings for Administrators setting), users (including administrators) cannot delete all-user remote access connections. (By default, users can still delete their private connections, but you can change the default by using the Prohibit deletion of remote access connections setting.) Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you do not configure this setting, only Administrators and Network Configuration Operators can delete all user remote access connections. Important: When enabled, the Prohibit deletion of remote access connections setting takes precedence over this setting. Users (including administrators) cannot delete any remote access connections, and this setting is ignored. Note: LAN connections are created and deleted automatically by the system when a LAN adapter is installed or removed. You cannot use the Network Connections folder to create or delete a LAN connection. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.
USER	Administrative Templates\Network\Network Connections	Prohibit deletion of remote access connections	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can delete remote access connections. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), users (including administrators) cannot delete any remote access connections. This setting also disables the Delete option on the context menu for a remote access connection and on the File menu in the Network Connections folder. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, all users can delete their private remote access connections. Private connections are those that are available only to one user. (By default,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				only Administrators and Network Configuration Operators can delete connections available to all users, but you can change the default by using the Ability to delete all user remote access connections setting.) Important: When enabled, this setting takes precedence over the Ability to delete all user remote access connections setting. Users cannot delete any remote access connections, and the Ability to delete all user remote access connections setting is ignored. Note: LAN connections are created and deleted automatically when a LAN adapter is installed or removed. You cannot use the Network Connections folder to create or delete a LAN connection. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.
USER	Administrative Templates\Network\Network Connections	Prohibit access to the Remote Access Preferences item on the Advanced menu	At least Microsoft Windows 2000 Service Pack 1	Determines whether the Remote Acccess Preferences item on the Advanced menu in Network Connections folder is enabled. The Remote Access Preferences item lets users create and change connections before logon and configure automatic dialing and callback features. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Remote Access Preferences item is disabled for all users (including administrators). Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Remote Access Preferences item is enabled for all users.
USER	Administrative Templates\Network\Network Connections	Enable Windows 2000 Network Connections settings for Administrators	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether settings that existed in Windows 2000 Server family will apply to Administrators. The set of Network Connections group settings that existed in Windows 2000 Professional also exists in Windows XP Professional. In Windows 2000 Professional, all of these settings had the ability to prohibit the use of certain features from Administrators. By default, Network Connections group settings in Windows XP Professional do not have the ability to prohibit the use of features from Administrators. If you enable this setting, the Windows XP settings that existed in Windows 2000 Professional will have the ability to prohibit Administrators from using certain features. These settings are Ability to rename LAN connections or remote access connections available to all users, Prohibit access to properties of components of a LAN connection, Prohibit access to properties of components of a remote access connection, Ability to access TCP/IP advanced configuration, Prohibit access to the Advanced Settings Item on the Advanced Menu, Prohibit adding and removing components for a LAN or remote access connection, Prohibit access to properties of a LAN

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				connection, Prohibit Enabling/Disabling components of a LAN connection, Ability to change properties of an all user remote access connection, Prohibit changing properties of a private remote access connection, Prohibit deletion of remote access connections, Ability to delete all user remote access connections, Prohibit connecting and disconnecting a remote access connection, Ability to Enable/Disable a LAN connection, Prohibit access to the New Connection Wizard, Prohibit renaming private remote access connections, Prohibit access to the Remote Access Preferences item on the Advanced menu, Prohibit viewing of status for an active connection. When this setting is enabled, settings that exist in both Windows 2000 Professional and Windows XP Professional behave the same for administrators. If you disable this setting or do not configure it, Windows XP settings that existed in Windows 2000 will not apply to administrators. Note: This setting is intended to be used in a situation in which the Group Policy object that these settings are being applied to contains both Windows 2000 Professional and Windows XP Professional computers, and identical Network Connections policy behavior is required between all Windows 2000 Professional and Windows XP Professional computers.
USER	Administrative Templates\Network\Network Connections	Prohibit access to properties of components of a LAN connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether Administrators and Network Configuration Operators can change the properties of components used by a LAN connection. This setting determines whether the Properties button for components of a LAN connection is enabled. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Properties button is disabled for Administrators. Network Configuration Operators are prohibited from accessing connection components, regardless of the Enable Network Connections settings for Administrators setting. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting does not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Properties button is enabled for administrators and Network Configuration Operators. The Local Area Connection Properties dialog box includes a list of the network components that the connection uses. To view or change the properties of a component, click the name of the component, and then click the Properties button beneath the component list. Note: Not all network components have configurable properties. For components that are not configurable, the Properties button is always disabled. Note: When the Prohibit access to properties of a LAN connection setting is enabled,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				users are blocked from accessing the Properties button for LAN connection components. Note: Network Configuration Operators only have permission to change TCP/IP properties. Properties for all other components are unavailable to these users. Note: Nonadministrators are already prohibited from accessing properties of components for a LAN connection, regardless of this setting.
USER	Administrative Templates\Network\Network Connections	Ability to Enable/Disable a LAN connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can enable/disable LAN connections. If you enable this setting, the Enable and Disable options for LAN connections are available to users (including nonadministrators). Users can enable/disable a LAN connection by double-clicking the icon representing the connection, by right-clicking it, or by using the File menu. If you disable this setting (and enable the Enable Network Connections settings for Administrators setting), double-clicking the icon has no effect, and the Enable and Disable menu items are disabled for all users (including administrators). Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you do not configure this setting, only Administrators and Network Configuration Operators can enable/disable LAN connections. Note: Administrators can still enable/disable LAN connections from Device Manager when this setting is disabled.
USER	Administrative Templates\Network\Network Connections	Prohibit access to properties of a LAN connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can change the properties of a LAN connection. This setting determines whether the Properties menu item is enabled, and thus, whether the Local Area Connection Properties dialog box is available to users. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Properties menu items are disabled for all users, and users cannot open the Local Area Connection Properties dialog box. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, a Properties menu item appears when users right-click the icon representing a LAN connection. Also, when users select the connection, Properties is enabled on the File menu. Note: This setting takes precedence over settings that manipulate the availability of features inside the Local Area Connection Properties dialog box. If this setting is enabled, nothing within the properties dialog box for a LAN connection is available to users. Note: Nonadministrators have the right to view the properties dialog box for a connection but not to make changes,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				regardless of this setting.
USER	Administrative Templates\Network\Network Connections	Prohibit access to the New Connection Wizard	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can use the New Connection Wizard, which creates new network connections. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Make New Connection icon does not appear in the Start Menu on in the Network Connections folder. As a result, users (including administrators) cannot start the New Connection Wizard. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Make New Connection icon appears in the Start menu and in the Network Connections folder for all users. Clicking the Make New Connection icon starts the New Connection Wizard. Note: Changing this setting from Enabled to Not Configured does not restore the Make New Connection icon until the user logs off or on. When other changes to this setting are applied, the icon does not appear or disappear in the Network Connections folder until the folder is refreshed. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.
USER	Administrative Templates\Network\Network Connections	Ability to change properties of an all user remote access connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether a user can view and change the properties of remote access connections that are available to all users of the computer. To create an all-user remote access connection, on the Connection Availability page in the New Connection Wizard, click the For all users option. This setting determines whether the Properties menu item is enabled, and thus, whether the Remote Access Connection Properties dialog box is available to users. If you enable this setting, a Properties menu item appears when any user right-clicks the icon for a remote access connection. Also, when any user selects the connection, Properties appears on the File menu. If you disable this setting (and enable the Enable Network Connections settings for Administrators setting), the Properties menu items are disabled, and users (including administrators) cannot open the remote access connection properties dialog box. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you do not configure this setting, only Administrators and Network Configuration Operators can change properties of all-user remote access connections. Note: This setting takes precedence over settings that manipulate the availability of features inside the Remote Access Connection Properties

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				dialog box. If this setting is disabled, nothing within the properties dialog box for a remote access connection will be available to users. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.
USER	Administrative Templates\Network\Network Connections	Prohibit access to properties of components of a remote access connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can view and change the properties of components used by a private or all-user remote access connection. This setting determines whether the Properties button for components used by a private or all-user remote access connection is enabled. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Properties button is disabled for all users (including administrators). Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting does not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Properties button is enabled for all users. The Networking tab of the Remote Access Connection Properties dialog box includes a list of the network components that the connection uses. To view or change the properties of a component, click the name of the component, and then click the Properties button beneath the component list. Note: Not all network components have configurable properties. For components that are not configurable, the Properties button is always disabled. Note: When the Ability to change properties of an all user remote access connection or Prohibit changing properties of a private remote access connection settings are set to deny access to the Remote Access Connection Properties dialog box, the Properties button for remote access connection components is blocked. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.
USER	Administrative Templates\Network\Network Connections	Prohibit connecting and disconnecting a remote access connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can connect and disconnect remote access connections. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), double-clicking the icon has no effect, and the Connect and Disconnect menu items are disabled for all users (including administrators). Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Connect and Disconnect options for remote access connections are available to all users. Users can connect or disconnect a remote access connection by double-clicking the icon representing the connection, by right-clicking it,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				or by using the File menu.
USER	Administrative Templates\Network\Network Connections	Prohibit changing properties of a private remote access connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can view and change the properties of their private remote access connections. Private connections are those that are available only to one user. To create a private connection, on the Connection Availability page in the New Connection Wizard, click the Only for myself option. This setting determines whether the Properties menu item is enabled, and thus, whether the Remote Access Connection Properties dialog box for a private connection is available to users. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Properties menu items are disabled, and no users (including administrators) can open the Remote Access Connection Properties dialog box for a private connection. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, a Properties menu item appears when any user right-clicks the icon representing a private remote access connection. Also, when any user selects the connection, Properties appears on the File menu. Note: This setting takes precedence over settings that manipulate the availability of features in the Remote Access Connection Properties dialog box. If this setting is enabled, nothing within the properties dialog box for a remote access connection will be available to users. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.
USER	Administrative Templates\Network\Network Connections	Ability to rename all user remote access connections	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether nonadministrators can rename all-user remote access connections. To create an all-user connection, on the Connection Availability page in the New Connection Wizard, click the For all users option. If you enable this setting, the Rename option is enabled for all-user remote access connections. Any user can rename all-user connections by clicking an icon representing the connection or by using the File menu. If you disable this setting, the Rename option is disabled for nonadministrators only. If you do not configure the setting, only Administrators and Network Configuration Operators can rename all-user remote access connections. Note: This setting does not apply to Administrators Note: When the Ability to rename LAN connections or remote access connections available to all users setting is configured (set to either Enabled or Disabled), this setting does not apply. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Network\Network Connections	Ability to rename LAN connections or remote access connections available to all users	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can rename LAN or all user remote access connections. If you enable this setting, the Rename option is enabled for all users. Users can rename connections by clicking the icon representing a connection or by using the File menu. If you disable this setting (and enable the Enable Network Connections settings for Administrators setting), the Rename option for LAN and all user remote access connections is disabled for all users (including Administrators and Network Configuration Operators). Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If this setting is not configured, only Administrators and Network Configuration Operators have the right to rename LAN or all user remote access connections. Note: When configured, this setting always takes precedence over the Ability to rename LAN connections and Ability to rename all user remote access connections settings. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to rename remote access connections.
USER	Administrative Templates\Network\Network Connections	Ability to rename LAN connections	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether nonadministrators can rename a LAN connection. If you enable this setting, the Rename option is enabled for LAN connections. Nonadministrators can rename LAN connections by clicking an icon representing the connection or by using the File menu. If you disable this setting, the Rename option is disabled for nonadministrators only. If you do not configure this setting, only Administrators and Network Configuration Operators can rename LAN connections Note: This setting does not apply to Administrators. Note: When the Ability to rename LAN connections or remote access connections available to all users setting is configured (set to either enabled or disabled), this setting does not apply.
USER	Administrative Templates\Network\Network Connections	Prohibit renaming private remote access connections	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can rename their private remote access connections. Private connections are those that are available only to one user. To create a private connection, on the Connection Availability page in the New Connection Wizard, click the Only for myself option. If you enable this setting (and enable the Enable Network Connections settings for Administrators setting), the Rename option is disabled for all users (including administrators). Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Rename option is enabled for all users' private remote access connections. Users can

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				rename their private connection by clicking an icon representing the connection or by using the File menu. Note: This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.
USER	Administrative Templates\Network\Network Connections	Prohibit viewing of status for an active connection	At least Microsoft Windows 2000 Service Pack 1	Determines whether users can view the status for an active connection. Connection status is available from the connection status taskbar icon or from the Status dialog box. The Status dialog box displays information about the connection and its activity. It also provides buttons to disconnect and to configure the properties of the connection. If you enable this setting, the connection status taskbar icon and Status dialog box are not available to users (including administrators). The Status option is disabled in the context menu for the connection and on the File menu in the Network Connections folder. Users cannot choose to show the connection icon in the taskbar from the Connection Properties dialog box. Important: If the Enable Network Connections settings for Administrators is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the connection status taskbar icon and Status dialog box are available to all users.
USER	Administrative Templates\Network\Offline Files	Do not automatically make redirected folders available offline	At least Microsoft Windows XP Professional or Windows Server 2003 family	All redirected shell folders, such as My Documents, Desktop, Start Menu, and Application Data, are available offline by default. This setting allows you to change this behavior so that redirected shell folders are not automatically available for offline use. However, users can still choose to make files and folders available offline themselves. If you enable this setting, the users must manually select the files they wish to be made available offline. If you disable this setting or do not configure it, redirected shell folders are automatically made available offline. All subfolders within the redirected folders are also made available offline. Note: This setting does not prevent files from being automatically cached if the network share is configured for Automatic Caching, nor does it affect the availability of the Make Available Offline menu option in the user interface. Note: Do not enable this setting unless you are certain that users will not need access to all of their redirected files in the event that the network or server holding the redirected files becomes unavailable.
USER	Administrative Templates\Network\Offline Files	Administratively assigned offline files	At least Microsoft Windows 2000	Lists network files and folders that are always available for offline use. This setting makes the specified files and folders available offline to users of the computer. To assign a folder, click Show, and then click

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Add. In the Type the name of the item to be added box, type the fully qualified UNC path to the file or folder. Leave the Enter the value of the item to be added field blank. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the settings will be combined and all specified files will be available for offline use.
USER	Administrative Templates\Network\Offline Files	Non-default server disconnect actions	At least Microsoft Windows 2000	Determines how computers respond when they are disconnected from particular offline file servers. This setting overrides the default response, a user-specified response, and the response specified in the Action on server disconnect setting. To use this setting, click Show, and then click Add. In the Type the name of the item to be added box, type the server's computer name. Then, in the Type the value of the item to be added box, type 0 if users can work offline when they are disconnected from this server, or type 1 if they cannot. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured for a particular server, the setting in Computer Configuration takes precedence over the setting in User Configuration. Both Computer and User configuration take precedence over a user's setting. This setting does not prevent users from setting custom actions through the Offline Files tab. However, users are unable to change any custom actions established via this setting. Tip: To configure this setting without establishing a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click Advanced. This setting corresponds to the settings in the Exception list section.
USER	Administrative Templates\Network\Offline Files	Event logging level	At least Microsoft Windows 2000	Determines which events the Offline Files feature records in the event log. Offline Files records events in the Application log in Event Viewer when it detects errors. By default, Offline Files records an event only when the offline files storage cache is corrupted. However, you can use this setting to specify additional events you want Offline Files to record. To use this setting, in the Enter box, select the number corresponding to the events you want the system to log. The levels are cumulative; that is, each level includes the events in all preceding levels. 0 records an error when the offline storage cache is corrupted. 1 also records an event when the server hosting the offline file is disconnected from the network. 2 also records events when the local computer is connected and disconnected from the network. 3 also records an event when the server hosting the offline file is reconnected to the network. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				precedence over the setting in User Configuration.
USER	Administrative Templates\Network\Offline Files	Action on server disconnect	At least Microsoft Windows 2000	Determines whether network files remain available if the computer is suddenly disconnected from the server hosting the files. This setting also disables the When a network connection is lost option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it. If you enable this setting, you can use the Action box to specify how computers in the group respond. -- Work offline indicates that the computer can use local copies of network files while the server is inaccessible. -- Never go offline indicates that network files are not available while the server is inaccessible. If you disable this setting or select the Work offline option, users can work offline if disconnected. If you do not configure this setting, users can work offline by default, but they can change this option. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To configure this setting without establishing a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, click Advanced, and then select an option in the When a network connection is lost section. Also, see the Non-default server disconnect actions setting.
USER	Administrative Templates\Network\Offline Files	Prevent use of Offline Files folder	At least Microsoft Windows 2000	Disables the Offline Files folder. This setting disables the View Files button on the Offline Files tab. As a result, users cannot use the Offline Files folder to view or open copies of network files stored on their computer. Also, they cannot use the folder to view characteristics of offline files, such as their server status, type, or location. This setting does not prevent users from working offline or from saving local copies of files available offline. Also, it does not prevent them from using other programs, such as Windows Explorer, to view their offline files. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To view the Offline Files Folder, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click View Files.
USER	Administrative Templates\Network\Offline Files	Prohibit user configuration of Offline Files	At least Microsoft Windows 2000	Prevents users from enabling, disabling, or changing the configuration of Offline Files. This setting removes the Offline Files tab from the Folder Options dialog box. It also removes the Settings item from the Offline Files context menu and disables the Settings button on the Offline Files

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Status dialog box. As a result, users cannot view or change the options on the Offline Files tab or Offline Files dialog box. This is a comprehensive setting that locks down the configuration you establish by using other settings in this folder. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: This setting provides a quick method for locking down the default settings for Offline Files. To accept the defaults, just enable this setting. You do not have to disable any other settings in this folder.
USER	Administrative Templates\Network\Offline Files	Remove 'Make Available Offline'	At least Microsoft Windows 2000	Prevents users from making network files and folders available offline. This setting removes the Make Available Offline option from the File menu and from all context menus in Windows Explorer. As a result, users cannot designate files to be saved on their computer for offline use. However, this setting does not prevent the system from saving local copies of files that reside on network shares designated for automatic caching. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
USER	Administrative Templates\Network\Offline Files	Prohibit 'Make Available Offline' for these file and folders	At least Microsoft Windows XP Professional or Windows Server 2003 family	Prohibits specific network files and folders from being made available for offline use. To prohibit the Make Available Offline option for specific files or folders, enable this setting, click Show, and then click Add. In the Type the name of the item to be added box, type the fully qualified UNC path to the file or folder. Leave the Enter the value of the item to be added field blank. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the settings are combined, and all specified files will not be available for offline use. Note: This setting does not prevent files from being automatically cached if the network share is configured for Automatic Caching. It only affects the availability of the Make Available Offline menu option in the user interface. Note: If the Disable Make Available Offline setting is enabled, this setting has no effect.
USER	Administrative Templates\Network\Offline Files	Turn off reminder balloons	At least Microsoft Windows 2000	Hides or displays reminder balloons, and prevents users from changing the setting. Reminder balloons appear above the Offline Files icon in the notification area to notify users when they have lost the connection to a networked file and are working on a local copy of the file. Users can then decide how to proceed. If you enable this setting, the system hides the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				reminder balloons, and prevents users from displaying them. If you disable the setting, the system displays the reminder balloons and prevents users from hiding them. If this setting is not configured, reminder balloons are displayed by default when you enable offline files, but users can change the setting. To prevent users from changing the setting while a setting is in effect, the system disables the Enable reminders option on the Offline Files tab This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To display or hide reminder balloons without establishing a setting, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This setting corresponds to the Enable reminders check box.
USER	Administrative Templates\Network\Offline Files	Reminder balloon frequency	At least Microsoft Windows 2000	Determines how often reminder balloon updates appear. If you enable this setting, you can select how often reminder balloons updates apppear and also prevent users from changing this setting. Reminder balloons appear when the user's connection to a network file is lost or reconnected, and they are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this setting to change the update interval. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To set reminder balloon frequency without establishing a setting, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This setting corresponds to the Display reminder balloons every ... minutes option.
USER	Administrative Templates\Network\Offline Files	Initial reminder balloon lifetime	At least Microsoft Windows 2000	Determines how long the first reminder balloon for a network status change is displayed. Reminder balloons appear when the user's connection to a network file is lost or reconnected, and they are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this setting to change the duration of the first reminder. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Network\Offline Files	Reminder balloon lifetime	At least Microsoft Windows 2000	Determines how long updated reminder balloons are displayed. Reminder balloons appear when the user's connection to a network file is lost or reconnected, and they are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this setting to change the duration of the update reminder. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
USER	Administrative Templates\Network\Offline Files	Synchronize all offline files before logging off	At least Microsoft Windows 2000	Determines whether offline files are fully synchronized when users log off. This setting also disables the Synchronize all offline files before logging off option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it. If you enable this setting, offline files are fully synchronized. Full synchronization ensures that offline files are complete and current. If you disable this setting, the system only performs a quick synchronization. Quick synchronization ensures that files are complete, but does not ensure that they are current. If you do not configure this setting, the system performs a quick synchronization by default, but users can change this option. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To change the synchronization method without changing a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then select the Synchronize all offline files before logging off option.
USER	Administrative Templates\Network\Offline Files	Synchronize all offline files when logging on	At least Microsoft Windows 2000	Determines whether offline files are fully synchronized when users log on. This setting also disables the Synchronize all offline files before logging on option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it. If you enable this setting, offline files are fully synchronized at logon. Full synchronization ensures that offline files are complete and current. Enabling this setting automatically enables logon synchronization in Synchronization Manager. If this setting is disabled and Synchronization Manager is configured for logon synchronization, the system performs only a quick synchronization. Quick synchronization ensures that files are complete but does not ensure that they are current. If you do not configure this setting and Synchronization Manager is configured for logon synchronization, the system performs a quick synchronization by default,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				but users can change this option. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To change the synchronization method without setting a setting, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then select the Synchronize all offline files before logging on option.
USER	Administrative Templates\Network\Offline Files	Synchronize offline files before suspend	At least Microsoft Windows 2000	Determines whether offline files are synchonized before a computer is suspended. If you enable this setting, offline files will be synchronized whenever the computer is suspended. Setting the synchronization action to Quick ensures only that all files in the cache are complete. Setting the synchronization action to Full ensures that all cached files and folders are up to date with the most current version. If you disable or do not configuring this setting, a synchronization will not occur when the computer is suspended. Note: If the computer is suspended by closing the display on a portable computer, a synchronization is not performed. If multiple users are logged on to the computer at the time the computer is suspended, a synchronization is not performed.
USER	Administrative Templates\Shared Folders	Allow DFS roots to be published	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether the user can publish DFS roots in Active Directory. If you enable this setting or do not configure it, users can use the Publish in Active Directory option to publish DFS roots as shared folders in Active Directory. If you disable this setting, the user cannot publish DFS roots in Active Directory, and the Publish in Active Directory option is disabled. Note: The default is to allow shared folders to be published when this setting is not configured.
USER	Administrative Templates\Shared Folders	Allow shared folders to be published	At least Microsoft Windows XP Professional or Windows Server 2003 family	Determines whether the user can publish shared folders in Active Directory. If you enable this setting or do not configure it, users can use the Publish in Active Directory option in the Shared Folders snap-in to publish shared folders in Active Directory. If you disable this setting, the user cannot publish shared folders in Active Directory, and the Publish in Active Directory option is disabled. Note: The default is to allow shared folders to be published when this setting is not configured
USER	Administrative Templates\Shell\Restrictions	Remove Shut Down command from Start menu		
USER	Administrative Templates\Shell\Restrictions	Hide all items on desktop		

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Shell\Restrictions	Hide drives in My Computer		
USER	Administrative Templates\Shell\Restrictions	Hide Network Neighborhood		
USER	Administrative Templates\Shell\Restrictions	No Entire Network in Network Neighborhood		
USER	Administrative Templates\Shell\Restrictions	Don't save settings at exit		
USER	Administrative Templates\Shell\Restrictions	No workgroup contents in Network Neighborhood		
USER	Administrative Templates\Shell\Restrictions	Remove Find command from Start menu		
USER	Administrative Templates\Shell\Restrictions	Remove folders from Settings on Start menu		
USER	Administrative Templates\Shell\Restrictions	Remove Run command from Start menu		
USER	Administrative Templates\Shell\Restrictions	Remove Taskbar from Settings on Start menu		
USER	Administrative Templates\Start Menu and Taskbar	Clear history of recently opened documents on exit	At least Microsoft Windows 2000	Clear history of recently opened documents on exit. If you enable this setting, the system deletes shortcuts to recently used document files when the user logs off. As a result, the Documents menu on the Start menu is always empty when the user logs on. If you disable or do not configure this setting, the system retains document shortcuts, and when a user logs on the Documents menu appears just as it did when the user logged off. Note: The system saves document shortcuts in the user profile in the System-drive\Documents and Settings\User-name\Recent folder. Also, see the Remove Documents menu from Start Menu and Do not keep history of recently opened documents policies in this folder. The system only uses this setting when neither of these related settings are selected. This setting does not clear the list of recent files that Windows programs display at the bottom of the File menu. See the Do not keep history of recently opened documents setting. This policy setting also does not hide document shortcuts displayed in the Open dialog box. See

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				the Hide the dropdown list of recent files setting.
USER	Administrative Templates\Start Menu and Taskbar	Add Logoff to the Start Menu	At least Microsoft Windows 2000	Adds the Log Off <username> item to the Start menu and prevents users from removing it. If you enable this setting, the Log Off <username> item appears in the Start menu. This setting also removes the Display Logoff item from Start Menu Options. As a result, users cannot remove the Log Off <username> item from the Start Menu. If you disable this setting or do not configure it, users can use the Display Logoff item to add and remove the Log Off item. 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. Note: To add or remove the Log Off item on a computer, click Start, click Settings, click Taskbar and Start Menu, click the Start Menu Options tab, and then, in the Start Menu Settings box, click Display Logoff. Also, see Remove Logoff in User Configuration\Administrative Templates\System\Logon/Logoff.
USER	Administrative Templates\Start Menu and Taskbar	Gray unavailable Windows Installer programs Start Menu shortcuts	At least Microsoft Windows 2000	Displays Start menu shortcuts to partially installed programs in gray text. This setting makes it easier for users to distinguish between programs that are fully installed and those that are only partially installed. Partially installed programs include those that a system administrator assigns using Windows Installer and those that users have configured for full installation upon first use. If you disable this setting or do not configure it, all Start menu shortcuts appear as black text. Note: Enabling this setting can make the Start menu slow to open.
USER	Administrative Templates\Start Menu and Taskbar	Turn off personalized menus	At least Microsoft Windows 2000	Disables personalized menus. Windows personalizes long menus by moving recently used items to the top of the menu and hiding items that have not been used recently. Users can display the hidden items by clicking an arrow to extend the menu. If you enable this setting, the system does not personalize menus. All menu items appear and remain in standard order. Also, this setting removes the Use Personalized Menus option so users do not try to change the setting while a setting is in effect. Note: Personalized menus require user tracking. If you enable the Turn off user tracking setting, the system disables user tracking and personalized menus and ignores this setting. Tip: To Turn off personalized menus without specifying a setting, click Start, click Settings, click Taskbar and Start Menu, and then, on the General tab, clear the Use Personalized Menus option.
USER	Administrative Templates\Start Menu and Taskbar	Lock the Taskbar	At least Microsoft Windows XP Professional or	This setting effects the taskbar, which is used to switch between running applications. The taskbar includes the Start button, list of currently running tasks, and the notification area. By default, the taskbar is located

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			Windows Server 2003 family	at the bottom of the screen, but it can be dragged to any side of the screen. When it is locked, it cannot be moved or resized. If you enable this setting, it prevents the user from moving or resizing the taskbar. While the taskbar is locked, auto-hide and other taskbar options are still available in Taskbar properties. If you disable this setting or do not configure it, the user can configure the taskbar position. Note: Enabling this setting also locks the quicklaunch bar and any other toolbars that the user has on their taskbar. The toolbar's position is locked, and the user cannot show and hide various toolbars using the taskbar context menu.
USER	Administrative Templates\Start Menu and Taskbar	Add Run in Separate Memory Space check box to Run dialog box	At least Microsoft Windows 2000	Lets users run a 16-bit program in a dedicated (not shared) Virtual DOS Machine (VDM) process. All DOS and 16-bit programs run on Windows 2000 Professional and Windows XP Professional in the Windows Virtual DOS Machine program. VDM simulates a 16-bit environment, complete with the DLLs required by 16-bit programs. By default, all 16-bit programs run as threads in a single, shared VDM process. As such, they share the memory space allocated to the VDM process and cannot run simultaneously. Enabling this setting adds a check box to the Run dialog box, giving users the option of running a 16-bit program in its own dedicated NTVDM process. The additional check box is enabled only when a user enters a 16-bit program in the Run dialog box.
USER	Administrative Templates\Start Menu and Taskbar	Turn off notification area cleanup	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting effects the notification area, also called the system tray. The notification area is located in the task bar, generally at the bottom of the screen, and itincludes the clock and current notifications. This setting determines whether the items are always expanded or always collapsed. By default, notifications are collapsed. The notification cleanup << icon can be referred to as the notification chevron. If you enable this setting, the system notification area expands to show all of the notifications that use this area. If you disable this setting, the system notification area will always collapse notifications. If you do not configure it, the user can choose if they want notifications collapsed.
USER	Administrative Templates\Start Menu and Taskbar	Remove Balloon Tips on Start Menu items	At least Microsoft Windows XP Professional or Windows Server 2003 family	Hides pop-up text on the Start menu and in the notification area. When you hold the cursor over an item on the Start menu or in the notification area, the system displays pop-up text providing additional information about the object. If you enable this setting, some of this pop-up text is not displayed. The pop-up text affected by this setting includes Click here to begin on the Start button, Where have all my programs gone on the Start menu, and Where have my icons gone in the notification area. If you disable this setting or do not configure it, all pop-up text is

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				displayed on the Start menu and in the notification area.
USER	Administrative Templates\Start Menu and Taskbar	Remove Drag-and-drop context menus on the Start Menu	At least Microsoft Windows 2000	Prevents users from using the drag-and-drop method to reorder or remove items on the Start menu. Also, it removes context menus from the Start menu. If you disable this setting or do not configure it, users can remove or reorder Start menu items by dragging and dropping the item. They can display context menus by right-clicking a Start menu item. This setting does not prevent users from using other methods of customizing the Start menu or performing the tasks available from the context menus. Also, see the Prevent changes to Taskbar and Start Menu Settings and the Remove access to the context menus for taskbar settings.
USER	Administrative Templates\Start Menu and Taskbar	Remove and prevent access to the Shut Down command	At least Microsoft Windows 2000	Prevents users from shutting down or restarting Windows. This setting removes the Shut Down option from the Start menu and disables the Shut Down button on the Windows Security dialog box, which appears when you press CTRL+ALT+DEL. This setting prevents users from using the Windows user interface to shut down the system, although it does not prevent them from running programs that shut down Windows. If you disable this setting or do not configure it, the Shut Down menu option appears, and the Shut Down button is enabled. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
USER	Administrative Templates\Start Menu and Taskbar	Remove common program groups from Start Menu	At least Microsoft Windows 2000	Removes items in the All Users profile from the Programs menu on the Start menu. By default, the Programs menu contains items from the All Users profile and items from the user's profile. If you enable this setting, only items in the user's profile appear in the Programs menu. Tip: To see the Program menu items in the All Users profile, on the system drive, go to Documents and Settings\All Users\Start Menu\Programs.
USER	Administrative Templates\Start Menu and Taskbar	Remove Favorites menu from Start Menu	At least Microsoft Windows 2000	Prevents users from adding the Favorites menu to the Start menu or classic Start menu. If you enable this setting, the Display Favorites item does not appear in the Advanced Start menu options box. If you disable or do not configure this setting, the Display Favorite item is available. Note:The Favorities menu does not appear on the Start menu by default. To display the Favorites menu, right-click Start, click Properties, and then click Customize. If you are using Start menu, click the Advanced tab, and then, under Start menu items, click the Favorites menu. If you are using the classic Start menu, click Display Favorites under Advanced Start menu options. Note:The items that appear in the Favorites menu when you install Windows are preconfigured by the system to appeal to

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				most users. However, users can add and remove items from this menu, and system administrators can create a customized Favorites menu for a user group. Note:This setting only affects the Start menu. The Favorites item still appears in Windows Explorer and in Internet Explorer.
USER	Administrative Templates\Start Menu and Taskbar	Remove Search menu from Start Menu	At least Microsoft Windows 2000	Removes the Search item from the Start menu, and disables some Windows Explorer search elements. This setting removes the Search item from the Start menu and from the context menu that appears when you right-click the Start menu. Also, the system does not respond when users press the Application key (the key with the Windows logo)+ F. 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 context 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. Also, see the Remove Search button from Windows Explorer setting in User Configuration\Administrative Templates\Windows Components\Windows Explorer. Note: This setting also prevents the user from using the F3 key.
USER	Administrative Templates\Start Menu and Taskbar	Remove frequent programs list from the Start Menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	If you enable this setting, the frequently used programs list is removed from the Start menu. If you disable this setting or do not configure it, the frequently used programs list remains on the simple Start menu.
USER	Administrative Templates\Start Menu and Taskbar	Remove Help menu from Start Menu	At least Microsoft Windows 2000	Removes the Help command from the Start menu. This setting only affects the Start menu. It does not remove the Help menu from Windows Explorer and does not prevent users from running Help.
USER	Administrative Templates\Start Menu and Taskbar	Turn off user tracking	At least Microsoft Windows 2000	Disables user tracking. This setting prevents the system from tracking the programs users run, the paths they navigate, and the documents they open. The system uses this information to customize Windows features, such as personalized menus. If you enable this setting, the system does not track these user actions. The system disables customized features that require user tracking information, including personalized menus. Also, see the Turn off personalized menus setting.
USER	Administrative Templates\Start Menu and Taskbar	Remove All Programs list from the Start menu	At least Microsoft Windows XP Professional or	If you enable this setting, the All Programs item is removed from the simple Start menu. If you disable this setting or do not configure it, the All Programs item remains on the simple Start menu.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			Windows Server 2003 family	
USER	Administrative Templates\Start Menu and Taskbar	Remove Network Connections from Start Menu	At least Microsoft Windows 2000	Prevents users from running Network Connections. This setting prevents the Network Connections folder from opening. This setting also removes Network Connections from Settings on the 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. Also, see the Disable programs on Settings menu and Disable Control Panel settings and the settings in the Network Connections folder (Computer Configuration and User Configuration\Administrative Templates\Network\Network Connections).
USER	Administrative Templates\Start Menu and Taskbar	Remove pinned programs list from the Start Menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	If you enable this setting, the Pinned Programs list is removed from the Start menu, and the Internet and Email checkboxes are removed from the simple Start menu customization CPL. If you disable this setting or do not configure it, the Pinned Programs list remains on the simple Start menu.
USER	Administrative Templates\Start Menu and Taskbar	Do not keep history of recently opened documents	At least Microsoft Windows 2000	Prevents the operating system and installed programs from creating and displaying shortcuts to recently opened documents. If you enable this setting, the system and Windows programs do not create shortcuts to documents opened while the setting is in effect. Also, they retain but do not display existing document shortcuts. The system empties the Documents menu on the Start menu, and Windows programs do not display shortcuts at the bottom of the File menu. If you disable this setting, the system defaults are enforced. Disabling this setting has no effect on the system. Note: The system saves document shortcuts in the user profile in the System-drive\Documents and Settings\User-name\Recent folder. Also, see the Remove Documents menu from Start Menu and Clear history of recently opened documents on exit policies in this folder. If you enable this setting but do not enable the Remove Documents menu from Start Menu setting, the Documents menu appears on the Start menu, but it is empty. If you enable this setting, but then later disable it or set it to Not Configured, the document shortcuts saved before the setting was enabled reappear in the Documents menu and program File menus. This setting does not hide document shortcuts displayed in the Open dialog box. See the Hide the dropdown list of recent files setting. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Start Menu and Taskbar	Remove Documents menu from Start Menu	At least Microsoft Windows 2000	Removes the Documents menu from the Start menu. The Documents menu contains links to the nonprogram files that users have most recently opened. It appears so that users can easily reopen their documents. If you enable this setting, the system saves document shortcuts but does not display them in the Documents menu. If you later disable it or set it to Not Configured, the document shortcuts saved before the setting was enabled and while it was in effect appear in the Documents menu. Note: This setting does not prevent Windows programs from displaying shortcuts to recently opened documents. See the Do not keep history of recently opened documents setting. Also, see the Do not keep history of recently opened documents and Clear history of recenTly opened documents on exit policies in this folder. This setting also does not hide document shortcuts displayed in the Open dialog box. See the Hide the dropdown list of recent files setting.
USER	Administrative Templates\Start Menu and Taskbar	Do not use the search-based method when resolving shell shortcuts	At least Microsoft Windows 2000	Prevents the system from conducting a comprehensive search of the target drive to resolve a shortcut. By default, when the system cannot find the target file for a shortcut (.lnk), it searches all paths associated with the shortcut. If the target file is located on an NTFS partition, the system then uses the target's file ID to find a path. If the resulting path is not correct, it conducts a comprehensive search of the target drive in an attempt to find the file. If you enable this setting, the system does not conduct the final drive search. It just displays a message explaining that the file is not found. Note: This setting only applies to target files on NTFS partitions. FAT partitions do not have this ID tracking and search capability. Also, see the Do not track Shell shortcuts during roaming and the Do not use the tracking-based method when resolving shell shortcuts settings.
USER	Administrative Templates\Start Menu and Taskbar	Do not use the tracking-based method when resolving shell shortcuts	At least Microsoft Windows 2000	Prevents the system from using NTFS tracking features to resolve a shortcut. By default, when the system cannot find the target file for a shortcut (.lnk), it searches all paths associated with the shortcut. If the target file is located on an NTFS partition, the system then uses the target's file ID to find a path. If the resulting path is not correct, it conducts a comprehensive search of the target drive in an attempt to find the file. If you enable this setting, the system does not try to locate the file by using its file ID. It skips this step and begins a comprehensive search of the drive specified in the target path. Note: This setting only applies to target files on NTFS partitions. FAT partitions do not have this ID tracking and search capability. Also, see the Do not track Shell shortcuts during roaming and the Do not use the search-based method

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				when resolving shell shortcuts settings.
USER	Administrative Templates\Start Menu and Taskbar	Remove Run menu from Start Menu	At least Microsoft Windows 2000	Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager. If you enable this setting, the following changes occur: (1) The Run command is removed from the Start menu. (2) The New Task (Run) command is removed from Task Manager. (3) The user will be blocked from entering the following into the Internet Explorer Address Bar: --- A UNC path: \\<server>\<share> --- Accessing local drives: e.g., C: --- Accessing local folders: e.g., \temp> Also, users with extended keyboards will no longer be able to display the Run dialog box by pressing the Application key (the key with the Windows logo) + R. If you disable or do not configure this setting, users will be able to access the Run command in the Start menu and in Task Manager and use the Internet Explorer Address Bar. Note:This setting affects the specified interface only. It does not prevent users from using other methods to run programs. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
USER	Administrative Templates\Start Menu and Taskbar	Remove programs on Settings menu	At least Microsoft Windows 2000	Prevents Control Panel, Printers, and Network Connections from running. This setting removes the Control Panel, Printers, and Network and Connection folders from Settings on the Start menu, and from 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 start Display or right-clicking My Computer to start System. Also, see the Disable Control Panel, Disable Display in Control Panel, and Remove Network Connections from Start Menu settings.
USER	Administrative Templates\Start Menu and Taskbar	Prevent changes to Taskbar and Start Menu Settings	At least Microsoft Windows 2000	Removes the Taskbar and Start Menu item from Settings on the Start menu. This setting also prevents the user from opening the Taskbar Properties dialog box. If the user right-clicks the taskbar and then clicks Properties, a message appears explaining that a setting prevents the action.
USER	Administrative Templates\Start Menu and Taskbar	Remove Set Program Access and Defaults from Start menu	At least Microsoft Windows 2000 Service Pack 3 or Microsoft Windows XP Professional	Removes the Set Program Access and Defaults icon from the Start menu. Clicking the Set Program Access and Defaults icon from the Start menu opens Add or Remove Programs and provides adminstrators the ability to specify default programs for certain activities, such as Web browsing or sending e-mail, as well as which programs are accessible from the Start menu, desktop, and other locations. Note: This setting

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
			Service Pack 1	does not prevent the Set Program Access and Defaults button from appearing in Add or Remove Programs. See the Hide the Set Program Access and Defaults page setting.
USER	Administrative Templates\Start Menu and Taskbar	Remove My Documents icon from Start Menu	At least Microsoft Windows 2000	Removes the My Documents icon from the Start menu and its submenus. This setting only removes the icon. It does not prevent the user from using other methods to gain access to the contents of the My Documents folder. Note: To make changes to this setting effective, you must log off and then log on. Also, see the Remove My Documents icon on the desktop setting.
USER	Administrative Templates\Start Menu and Taskbar	Remove My Music icon from Start Menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	Removes the My Music icon from the Start Menu.
USER	Administrative Templates\Start Menu and Taskbar	Remove My Network Places icon from Start Menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	Removes the My Network Places icon from the Start Menu.
USER	Administrative Templates\Start Menu and Taskbar	Remove My Pictures icon from Start Menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	Removes the My Pictures icon from the Start Menu.
USER	Administrative Templates\Start Menu and Taskbar	Remove user's folders from the Start Menu	At least Microsoft Windows 2000	Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden. This setting is designed for use with redirected folders. Redirected folders appear on the main (bottom) section of the Start menu. However, the original, user-specific version of the folder still appears on the top section of the Start menu. Because the appearance of two folders with the same name might confuse users, you can use this setting to hide user-specific folders. Note that this setting hides all user-specific folders, not just those associated with redirected folders. If you enable this setting, no folders appear on the top section of the Start menu. If users add folders to the Start Menu directory in their user profiles, the folders appear in the directory but not on the Start menu. If you disable this setting or do not configured it, Windows 2000 Professional and Windows XP Professional

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				display folders on both sections of the Start menu.
USER	Administrative Templates\Start Menu and Taskbar	Force classic Start Menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting effects the presentation of the Start menu. The classic Start menu in Windows 2000 Professional 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. If you enable this setting, the Start menu displays the classic Start menu in the Windows 2000 style and displays the standard desktop icons. If you disable this setting, the Start menu only displays in the new style, meaning the desktop icons are now on the Start page. If you do not configure this setting, the default is the new style, and the user can change the view.
USER	Administrative Templates\Start Menu and Taskbar	Remove Clock from the system notification area	At least Microsoft Windows XP Professional or Windows Server 2003 family	Prevents the clock in the system notification area from being displayed. If you enable this setting, the clock will not be displayed in the system notification area. If you disable or do not configure this setting, the default behavior of the clock appearing in the notification area will occur.
USER	Administrative Templates\Start Menu and Taskbar	Prevent grouping of taskbar items	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting effects the taskbar buttons used to switch between running programs. Taskbar grouping consolidates similar applications when there is no room on the taskbar. It kicks in when the user's taskbar is full. If you enable this setting, it prevents the taskbar from grouping items that share the same program name. By default, this setting is always enabled. If you disable or do not configure it, items on the taskbar that share the same program are grouped together. The users have the option to disable grouping if they choose.
USER	Administrative Templates\Start Menu and Taskbar	Do not display any custom toolbars in the taskbar	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting affects the taskbar. The taskbar includes the Start button, buttons for currently running tasks, custom toolbars, the notification area, and the system clock. Toolbars include Quick Launch, Address, Links, Desktop, and other custom toolbars created by the user or by an application. If this setting is enabled, the taskbar does not display any custom toolbars, and the user cannot add any custom toolbars to the taskbar. Moreover, the Toolbars menu command and submenu are removed from the context menu. The taskbar displays only the Start button, taskbar buttons, the notification area, and the system clock. If this setting is disabled or is not configured, the taskbar displays all toolbars. Users can add or remove custom toolbars, and the Toolbars

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				command appears in the context menu.
USER	Administrative Templates\Start Menu and Taskbar	Remove access to the context menus for the taskbar	At least Microsoft Windows 2000	Hides the menus that appear when you right-click the taskbar and items on the taskbar, such as the Start button, the clock, and the taskbar buttons. This setting does not prevent users from using other methods to issue the commands that appear on these menus.
USER	Administrative Templates\Start Menu and Taskbar	Hide the notification area	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting affects the notification area (previously called the system tray) on the taskbar. Description: The notification area is located at the far right end of the task bar and includes the icons for current notifications and the system clock. If this setting is enabled, the user's entire notification area, including the notification icons, is hidden. The taskbar displays only the Start button, taskbar buttons, custom toolbars (if any), and the system clock. If this setting is disabled or is not configured, the notification area is shown in the user's taskbar. Note: Enabling this setting overrides the Turn off notification area cleanup setting, because if the notification area is hidden, there is no need to clean up the icons.
USER	Administrative Templates\Start Menu and Taskbar	Remove user name from Start Menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	Remove user name from Start Menu
USER	Administrative Templates\Start Menu and Taskbar	Remove links and access to Windows Update	At least Microsoft Windows 2000	Prevents users from connecting to the Windows Update Web site. This setting blocks user access to the Windows Update Web site at http://windowsupdate.microsoft.com. Also, the setting removes the Windows Update hyperlink from the Start menu and from the Tools menu in Internet Explorer. Windows Update, the online extension of Windows, offers software updates to keep a user's system up-to-date. The Windows Update Product Catalog determines any system files, security fixes, and Microsoft updates that users need and shows the newest versions available for download. Also, see the Hide the Add programs from Microsoft option setting.
USER	Administrative Templates\Start Menu and Taskbar	Remove the Undock PC button from the Start Menu	At least Microsoft Windows XP Professional or Windows Server 2003 family	If you enable this setting, the Undock PC button is removed from the simple Start Menu, and your PC cannot be undocked. If you disable this setting or do not configure it, the Undock PC button remains on the simple Start menu, and your PC can be undocked.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Start Menu and Taskbar	Remove Logoff on the Start Menu	At least Microsoft Windows 2000	Removes the Log Off <username> item from the Start menu and prevents users from restoring it. If you enable this setting, the Log Off <username> item does not appear in the Start menu. This setting also removes the Display Logoff item from Start Menu Options. As a result, users cannot restore the Log Off <username> item to the Start Menu. If you disable this setting or do not configure it, users can use the Display Logoff item to add and remove the Log Off item. 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, and it does not prevent users from using other methods to log off. Tip: To add or remove the Log Off item on a computer, click Start, click Settings, click Taskbar and Start Menu, click the Start Menu Options tab and, in the Start Menu Settings box, click Display Logoff. See also: Remove Logoff in User Configuration\Administrative Templates\System\Logon/Logoff.
USER	Administrative Templates\System	Download missing COM components	At least Microsoft Windows 2000	Directs the system to search Active Directory for missing Component Object Model (COM) components that a program requires. Many Windows programs, such as the MMC snap-ins, use the interfaces provided by the COM. These programs cannot perform all of their functions unless Windows has internally registered the required components. If you enable this setting and a component registration is missing, the system searches for it in Active Directory and if it is found, downloads it. The resulting searches might make some programs start or run slowly. If you disable this setting or do not configure it, the program continues without the registration. As a result, the program might not perform all of its functions, or it might stop. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
USER	Administrative Templates\System	Turn off Autoplay	At least Microsoft Windows 2000	Turns off the Autoplay feature. Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately. By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives. If you enable this setting, you can also disable Autoplay on CD-ROM drives or disable Autoplay on all drives. This setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default. Note: This setting appears in both the Computer Configuration and User Configuration folders. If the settings

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration. Note: This setting does not prevent Autoplay for music CDs.
USER	Administrative Templates\System	Prevent access to the command prompt	At least Microsoft Windows 2000	Prevents users from running the interactive command prompt, Cmd.exe. This setting also determines whether batch files (.cmd and .bat) can run on the computer. If you enable this setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action. Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Terminal Services.
USER	Administrative Templates\System	Prevent access to registry editing tools	At least Microsoft Windows 2000	Disables the Windows registry editor Regedit.exe. If this setting is enabled and the user tries to start a registry editor, a message appears explaining that a setting prevents the action. To prevent users from using other administrative tools, use the Run only allowed Windows applications setting.
USER	Administrative Templates\System	Don't run specified Windows applications	At least Microsoft Windows 2000	Prevents Windows from running the programs you specify in this setting. If you enable this setting, users cannot run programs that you add to the list of disallowed applications. This setting only prevents users from running programs that are started by the Windows Explorer process. It does not prevent users from running programs, such as Task Manager, that are started by the system process or by other processes. Also, if you permit users to gain access to the command prompt, Cmd.exe, this setting does not prevent them from starting programs in the command window that they are not permitted to start by using Windows Explorer. Note: To create a list of disallowed applications, click Show, click Add, and then enter the application executable name (e.g., Winword.exe, Poledit.exe, Powerpnt.exe).
USER	Administrative Templates\System	Configure driver search locations	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting configures the location that Windows searches for drivers when a new piece of hardware is found. By default, Windows searches the following places for drivers: local installation, floppy drives, CD-ROM drives, Windows Update. Using this setting, you may remove the floppy and CD-ROM drives from the search algorithm. If you enable this setting, you can remove the locations by selecting the associated check box beside the location name. If you disable or do not configure this setting, Windows searches the installation location, floppy drives, and CD-ROM drives. Note: To prevent searching Windows Update for drivers also see Turn off Windows Update device driver searching in Administrative Templates/System/Internet Communication

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Management/Internet Communication settings.
USER	Administrative Templates\System	Turn off Windows Update device driver search prompt	At least Microsoft Windows XP Professional with SP2	Specifies whether the administrator will be prompted about going to Windows Update to search for device drivers using the Internet. Note: This setting only has effect if Turn off Windows Update device driver searching in Administrative Templates/System/Internet Communication Management/Internet Communication settings is disabled or not configured. If this setting is enabled, administrators will not be prompted to search Windows Update. If this setting is disabled or not configured and Turn off Windows Update device driver searching is disabled or not configured, the administrator will be prompted for consent before going to Windows Update to search for device drivers.
USER	Administrative Templates\System	Code signing for device drivers	At least Microsoft Windows 2000	Determines how the system responds when a user tries to install device driver files that are not digitally signed. This setting establishes the least secure response permitted on the systems of users in the group. Users can use System in Control Panel to select a more secure setting, but when this setting is enabled, the system does not implement any setting less secure than the one the setting established. When you enable this setting, use the drop-down box to specify the desired response. -- Ignore directs the system to proceed with the installation even if it includes unsigned files. -- Warn notifies the user that files are not digitally signed and lets the user decide whether to stop or to proceed with the installation and whether to permit unsigned files to be installed. Warn is the default. -- Block directs the system to refuse to install unsigned files. As a result, the installation stops, and none of the files in the driver package are installed. To change driver file security without specifying a setting, use System in Control Panel. Right-click My Computer, click Properties, click the Hardware tab, and then click the Driver Signing button.
USER	Administrative Templates\System	Windows Automatic Updates	Only works on Microsoft Windows XP Professional	This setting controls automatic updates to a user's computer. Whenever a user connects to the Internet, Windows searches for updates available for the software and hardware on their computer and automatically downloads them. This happens in the background, and the user is prompted when downloaded components are ready to be installed, or prior to downloading, depending on their configuration. If you enable this setting, it prohibits Windows from searching for updates. If you disable or do not configure it, Windows searches for updates and automatically downloads them. Note: Windows Update is an online catalog customized for your computer that consists of items such as drivers,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				critical updates, Help files, and Internet products that you can download to keep your computer up to date. Also, see the Remove links and access to Windows Update setting. If the Remove links and access to Windows Update setting is enabled, the links to Windows Update on the Start menu are also removed. Note: If you have installed Windows XP Service Pack 1 or the update to Automatic Updates that was released after Windows XP was originally shipped, then you should use the new Automatic Updates settings located at: 'Computer Configuration / Administrative Templates / Windows Update'
USER	Administrative Templates\System	Don't display the Getting Started welcome screen at logon	Only works on Microsoft Windows 2000	Supresses the welcome screen. This setting hides the welcome screen that is displayed on Windows 2000 Professional and Windows XP Professional each time the user logs on. Users can still display the welcome screen by selecting it on the Start menu or by typing Welcome in the Run dialog box. This setting applies only to Windows 2000 Professional and Windows XP Professional. It does not affect the Configure Your Server on a Windows 2000 Server screen on Windows 2000 Server. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: To display the welcome screen, click Start, point to Programs, point to Accessories, point to System Tools, and then click Getting Started. To suppress the welcome screen without specifying a setting, clear the Show this screen at startup check box on the welcome screen.
USER	Administrative Templates\System	Run only allowed Windows applications	At least Microsoft Windows 2000	Limits the Windows programs that users have permission to run on the computer. If you enable this setting, users can only run programs that you add to the List of Allowed Applications. This setting only prevents users from running programs that are started by the Windows Explorer process. It does not prevent users from running programs such as Task Manager, which are started by the system process or by other processes. Also, if users have access to the command prompt, Cmd.exe, this setting does not prevent them from starting programs in the command window that they are not permitted to start by using Windows Explorer. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting. Note: To create a list of allowed applications, click Show, click Add, and then enter the application executable name (e.g., Winword.exe, Poledit.exe, Powerpnt.exe).

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\System	Restrict these programs from being launched from Help	At least Microsoft Windows XP Professional or Windows Server 2003 family	Allows you to restrict programs from being run from online Help. If you enable this setting, you can prevent programs that you specify from being allowed to be run from Help. When you enable this setting, enter the list of the programs you want to restrict. Enter the file name of the executable for each application, separated by commas. If you disable or do not configure this setting, users will be able to run applications from online Help. Note: You can also restrict users from running applications by using the Software Restriction settings available in Computer Configuration\Security Settings. Note: This setting is available under Computer Configuration and User Comfiguration. If both are set, the list of programs specified in each of these will be restricted.
USER	Administrative Templates\System	Custom user interface	At least Microsoft Windows 2000	Specifies an alternate user interface for Windows 2000. The Explorer program (%systemdrive%\program files\internet explorer\iExplorer.exe) creates the familiar Windows interface, but you can use this setting to specify an alternate interface. If you enable this setting, the system starts the interface you specify instead of Explorer.exe. To use this setting, copy your interface program to a network share or to your system drive. Then, enable this setting, and type the name of the interface program, including the file name extension, in the Shell name text box. If the interface program file is not located in a folder specified in the Path environment variable for your system, enter the fully qualified path to the file. If you disable this setting or do not configure it, the setting is ignored and the system displays the Explorer interface. Tip: To find the folders indicated by the Path environment variable, click System Properties in Control Panel, click the Advanced tab, click the Environment Variables button, and then, in the System variables box, click Path.
USER	Administrative Templates\System	Century interpretation for Year 2000	At least Microsoft Windows 2000	Determines how programs interpret two-digit years. This setting specifies the largest two-digit year interpreted as being preceded by 20. All numbers less than or equal to the specified value are interpreted as being preceded by 20. All numbers greater than the specified value are interpreted as being preceded by 19. For example, the default value, 2029, specifies that all two-digit years less than or equal to 29 (00 to 29) are interpreted as being preceded by 20, that is 2000 to 2029. Conversely, all two-digit years greater than 29 (30 to 99) are interpreted as being preceded by 19, that is, 1930 to 1999. This setting only affects the programs that use this Windows feature to interpret two-digit years. If a program does not interpret two-digit years correctly, consult the documentation or manufacturer of the program.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\System\Ctrl+Alt+Del Options	Remove Change Password	At least Microsoft Windows 2000	Prevents users from changing their Windows password on demand. This setting disables the Change Password button on the Windows Security dialog box (which appears when you press Ctrl+Alt+Del). However, users are still able to change their password when prompted by the system. The system prompts users for a new password when an administrator requires a new password or their password is expiring.
USER	Administrative Templates\System\Ctrl+Alt+Del Options	Remove Lock Computer	At least Microsoft Windows 2000	Prevents users from locking the system. While locked, the desktop is hidden and the system cannot be used. Only the user who locked the system or the system administrator can unlock it. Tip:To lock a computer without configuring a setting, press Ctrl+Alt+Delete, and then click Lock Computer.
USER	Administrative Templates\System\Ctrl+Alt+Del Options	Remove Task Manager	At least Microsoft Windows 2000	Prevents users from starting Task Manager (Taskmgr.exe). If this setting is enabled and users try to start Task Manager, a message appears explaining that a policy prevents the action. Task Manager lets users start and stop programs; monitor the performance of their computers; view and monitor all programs running on their computers, including system services; find the executable names of programs; and change the priority of the process in which programs run.
USER	Administrative Templates\System\Ctrl+Alt+Del Options	Remove Logoff	At least Microsoft Windows 2000	Prevents the user from logging off. This setting does not let the user log off the system by using any method, including programs run from the command line, such as scripts. It also disables or removes all menu items and buttons that log the user off the system. Also, see the Remove Logoff on the Start Menu setting.
USER	Administrative Templates\System\Group Policy	Disallow Interactive Users from generating Resultant Set of Policy data	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting controls the ability of users to view their Resultant Set of Policy (RSoP) data. By default, interactively logged on users can view their own Resultant Set of Policy (RSoP) data. If this setting is enabled, interactive users cannot generate RSoP data. If this setting is not configured or disabled, interactive Users can generate RSoP. Note: This setting does not affect administrators. If this setting is enabled or disabled, by default, administrators can view RSoP data. Note: To view RSoP data on a client computer, use the RSoP snap-in for the Microsoft Management Console. You can launch the RSoP snap-in from the command line by typing RSOP.msc Note: This setting exists as both a User Configuration and Computer Configuration setting. Also, see the Turn off Resultant set of Policy Logging setting in Computer Configuration\Administrative Templates\System\GroupPolicy.
USER	Administrative	Turn off automatic	At least Microsoft	Prevents the system from updating the Administrative Templates source

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Templates\System\Group Policy	update of ADM files	Windows 2000	files automatically when you open the Group Policy Object Editor. Administrators may want to use this if they are concerned about the amount of space used on the system volume of a DC. By default, when you start the Group Policy Object Editor, a timestamp comparison is performed on the source files in the local %SYSTEMROOT%\inf directory and the source files stored in the GPO. If the local files are newer, they are copied into the GPO. Changing the status of this setting to Enabled will keep any source files from copying to the GPO. Changing the status of this setting to Disabled will enforce the default behavior. Files will always be copied to the GPO if they have a later timestamp. NOTE: If the Computer Configuration policy setting, Always use local ADM files for the Group Policy Object Editor is enabled, the state of this setting is ignored and always treated as Enabled.
USER	Administrative Templates\System\Group Policy	Enforce Show Policies Only	At least Microsoft Windows 2000	Prevents administrators from viewing or using Group Policy preferences. A Group Policy administration (.adm) file can contain both true settings and preferences. True settings, which are fully supported by Group Policy, must use registry entries in the Software\Policies or Software\Microsoft\Windows\CurrentVersion\Policies registry subkeys. Preferences, which are not fully supported, use registry entries in other subkeys. If you enable this setting, the Show Policies Only command is turned on, and administrators cannot turn it off. As a result, Group Policy Object Editor displays only true settings; preferences do not appear. If you disable this setting or do not configure it, the Show Policies Only command is turned on by default, but administrators can view preferences by turning off the Show Policies Only command. Note: To find the Show Policies Only command, in Group Policy Object Editor, click the Administrative Templates folder (either one), right-click the same folder, and then point to View. In Group Policy Object Editor, preferences have a red icon to distinguish them from true settings, which have a blue icon.
USER	Administrative Templates\System\Group Policy	Group Policy domain controller selection	At least Microsoft Windows 2000	Determines which domain controller the Group Policy Object Editor snap-in uses. -- Use the Primary Domain Controller indicates that the Group Policy Object Editor snap-in reads and writes changes to the domain controller designated as the PDC Operations Master for the domain. -- Inherit from Active Directory Snap-ins indicates that the Group Policy Object Editor snap-in reads and writes changes to the domain controller that Active Directory Users and Computers or Active Directory Sites and Services snap-ins use. -- Use any available domain controller indicates that the Group Policy Object Editor snap-in can read

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				and write changes to any available domain controller. If you disable this setting or do not configure it, the Group Policy Object Editor snap-in uses the domain controller designated as the PDC Operations Master for the domain. Note: To change the PDC Operations Master for a domain, in Active Directory Users and Computers, right-click a domain, and then click Operations Masters.
USER	Administrative Templates\System\Group Policy	Group Policy slow link detection	At least Microsoft Windows 2000	Defines a slow connection for purposes of applying and updating Group Policy. If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this setting, the system considers the connection to be slow. The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, the policy processing settings in this folder lets you override the programs' specified responses to slow links. To use this setting, in the Connection speed box, type a decimal number between 0 and 4,294,967,200 (0xFFFFFFA0), indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast. If you disable this setting or do not configure it, the system uses the default value of 500 kilobits per second. This setting appears in the Computer Configuration and User Configuration folders. The setting in Computer Configuration defines a slow link for policies in the Computer Configuration folder. The setting in User Configuration defines a slow link for settings in the User Configuration folder. Also, see the Do not detect slow network connections and related policies in Computer Configuration\Administrative Templates\System\User Profile. Note: If the profile server has IP connectivity, the connection speed setting is used. If the profile server does not have IP connectivity, the SMB timing is used.
USER	Administrative Templates\System\Group Policy	Group Policy refresh interval for users	At least Microsoft Windows 2000	Specifies how often Group Policy for users is updated while the computer is in use (in the background). This setting specifies a background update rate only for the Group Policies in the User Configuration folder. In addition to background updates, Group Policy for users is always updated when users log on. By default, user Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes. You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update user Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations. If you disable

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				this setting, user Group Policy is updated every 90 minutes (the default). To specify that Group Policy for users should never be updated while the computer is in use, select the Turn off background refresh of Group Policy setting. This setting also lets you specify how much the actual update interval varies. To prevent clients with the same update interval from requesting updates simultaneously, the system varies the update interval for each client by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that client requests overlap. However, updates might be delayed significantly. Important: If the Turn off background refresh of Group Policy setting is enabled, this setting is ignored. Note: This setting establishes the update rate for user Group Policies. To set an update rate for computer Group Policies, use the Group Policy refresh interval for computers setting (located in Computer Configuration\Administrative Templates\System\Group Policy). Tip: Consider notifying users that their policy is updated periodically so that they recognize the signs of a policy update. When Group Policy is updated, the Windows desktop is refreshed; it flickers briefly and closes open menus. Also, restrictions imposed by Group Policies, such as those that limit the programs a user can run, might interfere with tasks in progress.
USER	Administrative Templates\System\Group Policy	Default name for new Group Policy objects	At least Microsoft Windows 2000	Sets the default display name for new Group Policy objects. This setting allows you to specify the default name for new Group Policy objects created from policy compliant Group Policy Management tools including the Group Policy tab in Active Directory tools and the GPO browser. The display name may contain environment variables and can be a maximum of 255 characters long. If this setting is Disabled or Not Configured, the default display name of New Group Policy object is used.
USER	Administrative Templates\System\Group Policy	Create new Group Policy object links disabled by default	At least Microsoft Windows 2000	Creates new Group Policy object links in the disabled state. This setting creates all new Group Policy object links in the disabled state by default. After you configure and test the new object links by using a policy compliant Group Policy management tool such as Active Directory Users and Computers or Active Directory Sites and Services, you can enable the object links for use on the system. If you disable this setting or do not configure it, new Group Policy object links are created in the enabled state. If you do not want them to be effective until they are configured and tested, you must disable the object link.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\System\Internet Communication Management	Restrict Internet communication	At least Microsoft Windows XP Professional with SP2	Specifies whether Windows can access the Internet to accomplish tasks that require Internet resources. If this setting is enabled, the policies that are listed in the Internet Communication Management section of Group Policy are all enabled. If this setting is disabled, or not configured, all of the policies listed in this section will be disabled.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off printing over HTTP	At least Microsoft Windows XP Professional with SP2	Specifies whether to allow printing over HTTP from this client. Printing over HTTP allows a client to print to printers on the intranet as well as the Internet. Note: This setting affects the client side of Internet printing only. It does not prevent this machine from acting as an Internet Printing server and making it's shared printers available via HTTP. If you enable this setting, it prevents this client from printing to internet printers over HTTP. If you disable or do not configure this setting, users will be able to choose to print to internet printers over HTTP. Also see the Web-based Printing setting in Computer Configuration/Administrative Templates/Printers.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off downloading of print drivers over HTTP	At least Microsoft Windows XP Professional with SP2	Specifies whether to allow this client to download print driver packages over HTTP. To setup HTTP printing, non-inbox drivers need to be downloaded over HTTP. Note: This setting does not prevent the client from printing to printers on the Intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally. If you enable this setting, print drivers will not be downloaded over HTTP. If you disable this setting or do not configure it, users will be able to download print drivers over HTTP.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Windows Movie Maker automatic codec downloads	At least Microsoft Windows XP Professional with SP2	Specifies whether Windows Movie Maker automatically downloads codecs. Windows Movie Maker can be configured so that codecs are downloaded automatically if the required codecs are not installed on the computer. If you enable this setting, Windows Movie Maker will not attempt to download missing codecs for imported audio and video files. If you disable or do not configure this setting, Windows Movie Maker might attempt to download missing codecs for imported audio and video files.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Windows Movie Maker online Web links	At least Microsoft Windows XP Professional with SP2	Specifies whether links to Web sites are available in Windows Movie Maker. These links include the Windows Movie Maker on the Web and Privacy Statement commands that appear on the Help menu, as well as the Learn more about video filters hyperlink in the Options dialog box and the sign up now hyperlink in the The Web saving option in the Save Movie Wizard. The Windows Movie Maker on the Web command lets

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				users go directly to the Windows Movie Maker Web site to get more information, and the Privacy Statement command lets users view information about privacy issues in respect to Windows Movie Maker. The Learn more about video filters hyperlink lets users learn more about video filters and their role in saving movies process in Windows Movie Maker. The sign up now hyperlink lets users sign up with a video hosting provider on the Web. If you enable this setting, the previously mentioned links to Web sites from Windows Movie Maker are disabled and cannot be selected. If you disable or do not configure this setting, the previously mentioned links to Web sites from Windows Movie Maker are enabled and can be selected.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Windows Movie Maker saving to online video hosting provider	At least Microsoft Windows XP Professional with SP2	Specifies whether users can send a final movie to a video hosting provider on the Web by choosing The Web saving option in the Save Movie Wizard of Windows Movie Maker. When users create a movie in Windows Movie Maker, they can choose to share it in a variety of ways through the Save Movie Wizard. The Web saving option lets users send their movies to a video hosting provider. If you enable this setting, users cannot choose The Web saving option in the Save Movie Wizard of Windows Movie Maker and cannot send a movie to a video hosting provider on the Web. If you disable or do not configure this setting, users can choose The Web saving option in the Save Movie Wizard of Windows Movie Maker and can send a movie to a video hosting provider on the Web.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Internet File Association service	At least Microsoft Windows XP Professional or Windows Server 2003 family	Specifies whether to use the Microsoft Web service for finding an application to open a file with an unhandled file association. When a user opens a file that has an extension that is not associated with any applications on the machine, they are given the choice to choose a local application or use the Web service to find an application. If you enable this setting, the link and the dialog for using the Web service to open an unhandled file association are removed. If you disable or do not configure this setting, the user will be allowed to use the Web service.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off Internet download for Web publishing and online ordering wizards	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family	Specifies whether Windows should download a list of providers for the Web publishing and online prdering wizards. These wizards allow users to select from a list of companies that provide services such as online storage and photographic printing. By default, Windows displays providers downloaded from a Windows Web site in addition to providers specified in the registry. If you enable this setting, Windows will not download providers and only the service providers that are cached in the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				local registry will be displayed. If you disable or do not configure this setting, a list of providers will be downloaded when the user uses the Web publishing or online ordering wizards. See the documentation for the Web publishing and online ordering wizards for more information, including details on specifying service providers in the registry.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off the Order Prints picture task	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family	Specifies whether the Order Prints Online task is available from Picture Tasks in Windows folders. The Order Prints Online Wizard is used to download a list of providers and allow users to order prints online. If you enable this setting, the task Order Prints Online is removed from Picture Tasks in Windows Explorer folders. If you disable or do not configure this setting, the task is displayed.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off the Publish to Web task for files and folders	At least Microsoft Windows XP Professional with SP2	Specifies whether the tasks Publish this file to the Web, Publish this folder to the Web, and Publish the selected items to the Web, are available from File and Folder Tasks in Windows folders. The Web Publishing Wizard is used to download a list of providers and allow users to publish content to the Web. If you enable this setting, these tasks are removed from the File and Folder tasks in Windows folders. If you disable or do not configure this setting, the tasks will be shown.
USER	Administrative Templates\System\Internet Communication Management\Internet Communication settings	Turn off the Windows Messenger Customer Experience Improvement Program	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family	Specifies whether Windows Messenger collects anonymous information about how Windows Messenger software and service is used. With the Customer Experience Improvement program, users can allow Microsoft to collect anonymous information about how the product is used. This information is used to improve the product in future releases. If you enable this setting, Windows Messenger will not collect usage information and the user settings to enable the collection of usage information will not be shown. If you disable this setting, Windows Messenger will collect anonymous usage information and the setting will not be shown. If you do not configure this setting, users will have the choice to opt-in and allow information to be collected.
USER	Administrative Templates\System\Logon	Do not process the legacy run list	At least Microsoft Windows 2000	Ignores the customized run list. You can create a customized list of additional programs and documents that the system starts automatically when it runs on Windows XP Professional, Windows 2000 Professional, Windows NT Workstation 4.0 and earlier. These programs are added to the standard run list of programs and services that the system starts. If you enable this setting, the system ignores the run list for Windows NT Workstation 4.0, Windows 2000 Professional, and Windows XP Professional. If you disable or do not configure this setting, Windows 2000 adds any customized run list configured for Windows NT 4.0 and

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				earlier to its run list. This setting appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Note: To create a customized run list by using a policy, use the Run these applications at startup setting. The customized run lists for Windows NT 4.0 and earlier are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run and HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run. They can be configured by using the Run setting in System Policy Editor for Windows NT 4.0 and earlier. Also, see the Do not process the run once list setting.
USER	Administrative Templates\System\Logon	Do not process the run once list	At least Microsoft Windows 2000	Ignores customized run-once lists. You can create a customized list of additional programs and documents that are started automatically the next time the system starts (but not thereafter). These programs are added to the standard list of programs and services that the system starts. If you enable this setting, the system ignores the run-once list. If you disable this setting or do not configure it, the system runs the programs in the run-once list. This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Note: Customized run-once lists are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce. Also, see the Do not process the legacy run list setting.
USER	Administrative Templates\System\Logon	Run these programs at user logon	At least Microsoft Windows 2000	Specifies additional programs or documents that Windows starts automatically when a user logs on to the system. To use this setting, click Show, click Add, and then, in the text box, type the name of the executable program (.exe) file or document file. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the system starts the programs specified in the Computer Configuration setting just before it starts the programs specified in the User Configuration setting. Also, see the Do not process the legacy run list and the Do not process the run once list settings.
USER	Administrative Templates\System\Power	Prompt for password on resume from hibernate /	At least Microsoft Windows XP	This settings allows you to configure client computers to always lock when resuming from a hibernate or suspend. If you enable this setting,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Management	suspend	Professional or Windows Server 2003 family	the client computer is locked when it is resumed from a suspend or hibernate state. If you disable or do not configure this setting, users can decide if their computer is automatically locked or not after performing a resume operation.
USER	Administrative Templates\System\Restrictions	Disable Registry editing tools		
USER	Administrative Templates\System\Restrictions	Run only allowed Windows applications		
USER	Administrative Templates\System\Scripts	Run legacy logon scripts hidden	At least Microsoft Windows 2000	Hides the instructions in logon scripts written for Windows NT 4.0 and earlier. Logon scripts are batch files of instructions that run when the user logs on. By default, Windows 2000 displays the instructions in logon scripts written for Windows NT 4.0 and earlier in a command window as they run, although it does not display logon scripts written for Windows 2000. If you enable this setting, Windows 2000 does not display logon scripts written for Windows NT 4.0 and earlier. Also, see the Run Logon Scripts Visible setting.
USER	Administrative Templates\System\Scripts	Run logoff scripts visible	At least Microsoft Windows 2000	Displays the instructions in logoff scripts as they run. Logoff scripts are batch files of instructions that run when the user logs off. By default, the system does not display the instructions in the logoff script. If you enable this setting, the system displays each instruction in the logoff script as it runs. The instructions appear in a command window. This setting is designed for advanced users. If you disable this setting or do not configure it, the instructions are suppressed.
USER	Administrative Templates\System\Scripts	Run logon scripts synchronously	At least Microsoft Windows 2000	Directs the system to wait for the logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop. If you enable this setting, Windows Explorer does not start until the logon scripts have finished running. This setting ensures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop. If you disable this setting or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously. This setting appears in the Computer Configuration and User Configuration folders. The setting set in Computer Configuration takes precedence over the setting set in User Configuration.
USER	Administrative Templates\System\Scripts	Run logon scripts visible	At least Microsoft Windows 2000	Displays the instructions in logon scripts as they run. Logon scripts are batch files of instructions that run when the user logs on. By default, the system does not display the instructions in the logon script. If you

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				enable this setting, the system displays each instruction in the logon script as it runs. The instructions appear in a command window. This setting is designed for advanced users. If you disable this setting or do not configure it, the instructions are suppressed.
USER	Administrative Templates\System\User Profiles	Connect home directory to root of the share	At least Microsoft Windows 2000	Restores the definitions of the %HOMESHARE% and %HOMEPATH% environment variables to those used in Windows NT 4.0 and earlier. If you enable this setting, the system uses the Windows NT 4.0 definitions. If you disable this setting or do not configure it, the system uses the new definitions designed for the Windows 2000 operating system. Along with %HOMEDRIVE%, these variables define the home directory of a user profile. The home directory is a persistent mapping of a drive letter on the local computer to a local or remote directory. By default, in Windows 2000 Server Family, %HOMESHARE% stores the fully qualified path to the home directory (such as \\server\share\dir1\dir2\homedir). Users can access the home directory and any of its subdirectories from the home drive letter, but they cannot see or access its parent directories. %HOMEPATH% stores a final backslash and is included for compatibility with earlier systems. On Windows NT 4.0 and earlier, %HOMESHARE% stores only the network share (such as \\server\share). %HOMEPATH% stores the remainder of the fully qualified path to the home directory (such as \dir1\dir2\homedir). As a result, users can access any directory on the home share by using the home directory drive letter. Tip: To specify a home directory in Windows 2000 Server Family, in Active Directory Users and Computers or Local Users and Groups, right-click the name of a user account, click Properties, click the Profile tab, and in the Home folder section, select the Connect option and select a drive letter and home directory. Example: Drive Z is mapped to \\server\share\dir1\dir2\homedir. If this setting is disabled or not configured (Windows 2000 Server Family behavior): -- %HOMEDRIVE% = Z: (mapped to \\server\share\dir1\dir2\homedir) -- %HOMESHARE% = \\server\share\dir1\dir2\homedir -- %HOMEPATH% = \ If the setting is enabled (Windows NT 4.0 behavior): -- %HOMEDRIVE% = Z: (mapped to \\server\share) -- %HOMESHARE% = \\server\share -- %HOMEPATH% = \dir1\dir2\homedir
USER	Administrative Templates\System\User Profiles	Exclude directories in roaming profile	At least Microsoft Windows 2000	Lets you add to the list of folders excluded from the user's roaming profile. This setting lets you exclude folders that are normally included in the user's profile. As a result, these folders do not need to be stored by the network server on which the profile resides and do not follow users to

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				other computers. By default, the History, Local Settings, Temp, and Temporary Internet Files folders are excluded from the user's roaming profile. If you enable this setting, you can exclude additional folders. If you disable this setting or do not configure it, only the default folders are excluded. Note: You cannot use this setting to include the default folders in a roaming user profile.
USER	Administrative Templates\System\User Profiles	Limit profile size	At least Microsoft Windows 2000	Sets the maximum size of each user profile and determines the system's response when a user profile reaches the maximum size. If you disable this setting or do not configure it, the system does not limit the size of user profiles. If you enable this setting, you can do the following: -- Set a maximum permitted user profile size; -- Determine whether the registry files are included in the calculation of the profile size; -- Determine whether users are notified when the profile exceeds the permitted maximum size; -- Specify a customized message notifying users of the oversized profile; -- Determine how often the customized message is displayed. Note: This setting affects both local and roaming profiles.
USER	Administrative Templates\Temporary Internet Files (User)	Temporary Internet Files (User)		
USER	Administrative Templates\Temporary Internet Files (User)	Temporary Internet Files (User)		
USER	Administrative Templates\Unsupported Administrative Templates	Windows.adm		The settings in windows.adm are intended for use with Windows 95, Windows 98 and Windows NT 4.0 clients. Their use in Group Policy is not supported.
USER	Administrative Templates\Unsupported Administrative Templates	Common.adm		The settings in common.adm are intended for use with Windows 95, Windows 98 and Windows NT 4.0 clients. Their use in Group Policy is not supported.
USER	Administrative Templates\Unsupported Administrative Templates	Winnt.adm		The settings in winnt.adm are intended for use with Windows 95, Windows 98 and Windows NT 4.0 clients. Their use in Group Policy is not supported.
USER	Administrative Templates\URL Encoding	URL Encoding		
USER	Administrative Templates\Windows 95 Control Panel\Network	Restrict Network Control Panel		

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows 95 Control Panel\Passwords	Restrict Passwords Control Panel		
USER	Administrative Templates\Windows 95 Control Panel\Printers	Restrict printer settings		
USER	Administrative Templates\Windows 95 Control Panel\System	Restrict System Control Panel		
USER	Administrative Templates\Windows 95 Network\Sharing	Disable file sharing		
USER	Administrative Templates\Windows 95 Network\Sharing	Disable print sharing		
USER	Administrative Templates\Windows 95 Shell\Custom folders	Custom desktop icons		
USER	Administrative Templates\Windows 95 Shell\Custom folders	Custom Network Neighborhood		
USER	Administrative Templates\Windows 95 Shell\Custom folders	Custom Programs folder		
USER	Administrative Templates\Windows 95 Shell\Custom folders	Custom Start menu		
USER	Administrative Templates\Windows 95 Shell\Custom folders	Custom Startup folder		
USER	Administrative Templates\Windows 95 Shell\Custom folders	Hide Start menu subfolders		
USER	Administrative Templates\Windows 95 System\Restrictions	Disable MS-DOS prompt		
USER	Administrative Templates\Windows 95 System\Restrictions	Disable single-mode MS-DOS apps		
USER	Administrative Templates\Windows Components\Application Compatibility	Prevent access to 16-bit applications	At least Microsoft Windows XP Professional with SP1 or Windows Server 2003 family	Specifies whether to prevent the MS-DOS subsystem (ntvdm.exe) from running for all users. This setting affects the launching of 16-bit applications in the operating system. By default, the MS-DOS subsystem runs for all users. You can use this setting to turn off the MS-DOS subsystem, which will reduce resource usage and prevent users from running 16-bit applications. To run any 16-bit application or any

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				application with 16-bit components, ntvdm.exe must be allowed to run. The MS-DOS subsystem starts when the first 16-bit application is launched. While the process is running, any subsequent 16-bit applications launch faster, but overall resource usage on the system is increased. If the status is set to Enabled, ntvdm.exe is prevented from running, which then prevents any 16-bit applications from running. In addition, any 32-bit applications with 16-bit installers or other 16-bit components cannot run. If the status is set to Disabled, the default setting applies and the MS-DOS subsystem runs for all users. If the status is set to Not Configured, the default applies and ntvdm.exe runs for all users. However, if an administrator sets the registry DWORD value HKLM\System\CurrentControlSet\Control\WOW\DisallowedPolicyDefault to 1, the default changes to prevent all 16-bit applications from running. Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable caching of Auto-Proxy scripts	at least Internet Explorer v5.01	Prevents automatic proxy scripts, which interact with a server to automatically configure users' proxy settings, from being stored in the users' cache. If you enable this policy, automatic proxy scripts will not be stored temporarily on the users' computer. If you disable this policy or do not configure it, automatic proxy scripts can be stored in the users' cache.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable external branding of Internet Explorer	at least Internet Explorer v5.01	Prevents branding of Internet programs, such as customization of Internet Explorer and Outlook Express logos and title bars, by another party. If you enable this policy, it prevents customization of the browser by another party, such as an Internet service provider or Internet content provider. If you disable this policy or do not configure it, users could install customizations from another party-for example, when signing up for Internet services. This policy is intended for administrators who want to maintain a consistent browser across an organization.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing Advanced page settings	at least Internet Explorer v5.01	Prevents users from changing settings on the Advanced tab in the Internet Options dialog box. If you enable this policy, users are prevented from changing advanced Internet settings, such as security, multimedia, and printing. Users cannot select or clear the check boxes on the Advanced tab. If you disable this policy or do not configure it, users can select or clear settings on the Advanced tab. If you set the Disable the Advanced page policy (located in \User

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the Advanced page policy removes the Advanced tab from the interface.
USER	Administrative Templates\Windows Components\Internet Explorer	Use Automatic Detection for dial-up connections	at least Internet Explorer v5.01	Specifies that Automatic Detection will be used to configure dial-up settings for users. Automatic Detection uses a DHCP (Dynamic Host Configuration Protocol) or DNS server to customize the browser the first time it is started. If you enable this policy, users' dial-up settings will be configured by Automatic Detection. If you disable this policy or do not configure it, dial-up settings will not be configured by Automatic Detection, unless specified by the user.
USER	Administrative Templates\Windows Components\Internet Explorer	Display error message on proxy script download failure	at least Internet Explorer v5.01	Specifies that error messages will be displayed to users if problems occur with proxy scripts. If you enable this policy, error messages will be displayed when the browser does not download or run a script to set proxy settings. If you disable this policy or do not configure it, error messages will not be displayed when problems occur with proxy scripts.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable importing and exporting of favorites	at least Internet Explorer v5.01	Prevents users from exporting or importing favorite links by using the Import/Export Wizard. If you enable this policy, the Import/Export Wizard cannot import or export favorite links or cookies, which are small text files that contain settings for Web sites. If you disable this policy or do not configure it, users can import and export favorites in Internet Explorer by clicking the File menu, clicking Import and Export, and then running the Import/Export Wizard. Note: If you enable this policy, users can still view screens in the wizard, but when users click Finish, a prompt will appear that states that this feature has been disabled.
USER	Administrative Templates\Windows Components\Internet Explorer	Identity Manager: Prevent users from using Identities	at least Internet Explorer v5.01	Prevents users from configuring unique identities by using Identity Manager. Identity Manager enables users to create multiple accounts, such as e-mail accounts, on the same computer. Each user has a unique identity, with a different password and different program preferences. If you enable this policy, users will not be able to create new identities, manage existing identities, or switch identities. The Switch Identity option will be removed from the File menu in Address Book. If you disable this policy or do not configure it, users can set up and change identities.
USER	Administrative Templates\Windows Components\Internet Explorer	Configure Media Explorer Bar	at least Internet Explorer v6.0	Allows Administrators to enable and disable the Media Explorer Bar and set the auto-play default. The Media Explorer Bar plays music and video content from the Internet. If you disable the Media explorer bar, users cannot display the Media Explorer Bar. The auto-play feature is also

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				disabled. When users click on a link within Internet Explorer, the content will be played by the default media client on their system. If you enable the Media Explorer Bar or do not configure it, users can show and hide the Media Explorer Bar. Administrators also have the ability to turn the auto-play feature on or off. This setting only applies if the Media Explorer Bar is enabled. If checked, the Media Explorer Bar will automatically display and play the media content when the user clicks on a media link. If unchecked, the content will be played by the default media client on their system.
USER	Administrative Templates\Windows Components\Internet Explorer	Configure Outlook Express	at least Internet Explorer v6.0	Allows Administrators to enable and disable the ablility for Outlook Express users to save or open attachments that can potentially contain a virus. If you check the block attachments setting, users will be unable to open or save attachments that could potentially contain a virus. Users will not be able to disable the blocking of attachements in options. If the block attachments setting is not checked, the user can specify to enable or disable the blocking of attachements in options.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing accessibility settings	at least Internet Explorer v5.01	Prevents users from changing accessibility settings. If you enable this policy, the Accessibility button on the General tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can change accessibility settings, such as overriding fonts and colors on Web pages. If you set the Disable the General page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the General page policy removes the General tab from the interface.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing Automatic Configuration settings	at least Internet Explorer v5.01	Prevents users from changing automatic configuration settings. Automatic configuration is a process that administrators can use to update browser settings periodically. If you enable this policy, the automatic configuration settings appear dimmed. The settings are located in the Automatic Configuration area of the Local Area Network (LAN) Settings dialog box. To see the Local Area Network (LAN) Settings dialog box, users open the Internet Options dialog box, click the Connections tab, and then click the LAN Settings button. If you disable this policy or do not configure it, the user can change automatic configuration settings. This policy is intended to enable administrators to ensure that users' settings are updated uniformly through automatic configuration. The Disable the Connections page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Explorer\Internet Control Panel), which removes the Connections tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing Temporary Internet files settings	at least Internet Explorer v5.01	Prevents users from changing the browser cache settings, such as the location and amount of disk space to use for the Temporary Internet Files folder. If you enable this policy, the browser cache settings appear dimmed. These settings are found in the dialog box that appears when users click the General tab and then click the Settings button in the Internet Options dialog box. If you disable this policy or do not configure it, users can change their cache settings. If you set the Disable the General page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the General page policy removes the General tab from the interface.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing Calendar and Contact settings	at least Internet Explorer v5.01	Prevents users from changing the default programs for managing schedules and contacts. If you enable this policy, the Calendar and Contact check boxes appear dimmed in the Internet Programs area. To display these options, users open the Internet Options dialog box, and then click the Programs tab. If you disable this policy or do not configure it, users can determine which programs to use for managing schedules and contacts, if programs that perform these tasks are installed. This Disable the Programs Page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing certificate settings	at least Internet Explorer v5.01	Prevents users from changing certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers. If you enable this policy, the settings in the Certificates area on the Content tab in the Internet Options dialog box appear dimmed. If you disable this policy or do not configure it, users can import new certificates, remove approved publishers, and change settings for certificates that have already been accepted. The Disable the Content page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored. Caution: If you enable this policy, users can still run the Certificate Manager Import Wizard by double-clicking a software publishing

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				certificate (.spc) file. This wizard enables users to import and configure settings for certificates from software publishers that haven't already been configured for Internet Explorer.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing default browser check	at least Internet Explorer v5.01	Prevents Microsoft Internet Explorer from checking to see whether it is the default browser. If you enable this policy, the Internet Explorer Should Check to See Whether It Is the Default Browser check box on the Programs tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can determine whether Internet Explorer will check to see if it is the default browser. When Internet Explorer performs this check, it prompts the user to specify which browser to use as the default. This policy is intended for organizations that do not want users to determine which browser should be their default. The Disable the Programs page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing color settings	at least Internet Explorer v5.01	Prevents users from changing the default Web page colors. If you enable this policy, the color settings for Web pages appear dimmed. The settings are located in the Colors area in the dialog box that appears when the user clicks the General tab and then clicks the Colors button in the Internet Options dialog box. If you disable this policy or do not configure it, users can change the default background and text color of Web pages. If you set the Disable the General page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the General page policy removes the General tab from the interface. Note: The default Web page colors are ignored on Web pages in which the author has specified the background and text colors.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing connection settings	at least Internet Explorer v5.01	Prevents users from changing dial-up settings. If you enable this policy, the Settings button on the Connections tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can change their settings for dial-up connections. If you set the Disable the Connections page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the Connections page policy removes the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Connections tab from the interface.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable Internet Connection wizard	at least Internet Explorer v5.01	Prevents users from running the Internet Connection Wizard. If you enable this policy, the Setup button on the Connections tab in the Internet Options dialog box appears dimmed. Users will also be prevented from running the wizard by clicking the Connect to the Internet icon on the desktop or by clicking Start, pointing to Programs, pointing to Accessories, pointing to Communications, and then clicking Internet Connection Wizard. If you disable this policy or do not configure it, users can change their connection settings by running the Internet Connection Wizard. Note: This policy overlaps with the Disable the Connections page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from the interface. Removing the Connections tab from the interface, however, does not prevent users from running the Internet Connection Wizard from the desktop or the Start menu.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing font settings	at least Internet Explorer v5.01	Prevents users from changing font settings. If you enable this policy, the Font button on the General tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can change the default fonts for viewing Web pages. If you set the Disable the General page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the General page policy removes the General tab from the interface. Note: The default font settings colors are ignored in cases in which the Web page author has specified the font attributes.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable AutoComplete for forms	at least Internet Explorer v5.01	Prevents Microsoft Internet Explorer from automatically completing forms, such as filling in a name or a password that the user has entered previously on a Web page. If you enable this policy, the Forms check box appears dimmed. To display the Forms check box, users open the Internet Options dialog box, click the Content tab, and then click the AutoComplete button. If you disable this policy or do not configure it, users can enable the automatic completion of forms. The Disable the Content page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored. Caution: If you enable this policy after users have used their

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				browser with form automatic completion enabled, it will not clear the automatic completion history for forms that users have already filled out.
USER	Administrative Templates\Windows Components\Internet Explorer	Do not allow AutoComplete to save passwords	at least Internet Explorer v5.01	Disables automatic completion of user names and passwords in forms on Web pages, and prevents users from being prompted to save passwords. If you enable this policy, the User Names and Passwords on Forms and Prompt Me to Save Passwords check boxes appear dimmed. To display these check boxes, users open the Internet Options dialog box, click the Content tab, and then click the AutoComplete button. If you disable this policy or don't configure it, users can determine whether Internet Explorer automatically completes user names and passwords on forms and prompts them to save passwords. The Disable the Content page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing history settings	at least Internet Explorer v5.01	Prevents users from changing the history settings for the browser. If you enable this policy, the settings in the History area on the General tab in the Internet Options dialog box appear dimmed. If you disable this policy or do not configure it, users can change the number of days to store Web page information and clear Web page history. If you set the Disable the General page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the General page policy removes the General tab from the interface.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing home page settings	at least Internet Explorer v5.01	Prevents users from changing the home page of the browser. The home page is the first page that appears when users start the browser. If you enable this policy, the settings in the Home Page area on the General tab in the Internet Options dialog box appear dimmed. If you disable this policy or do not configure it, users can change their home page. If you set the Disable the General page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the General page policy removes the General tab from the interface. This policy is intended for administrators who want to maintain a consistent home page across their organization.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing language settings	at least Internet Explorer v5.01	Prevents users from changing language settings. If you enable this policy, the Languages button on the General tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can change the language settings for viewing Web sites for languages in which the character set has been installed. If you set the Disable the General page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the General page policy removes the General tab from the interface.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing link color settings	at least Internet Explorer v5.01	Prevents users from changing the colors of links on Web pages. If you enable this policy, the color settings for links appear dimmed. The settings are located in the Links area of the dialog box that appears when users click the General tab and then click the Colors button in the Internet Options dialog box. If you disable this policy or do not configure it, users can change the default color of links on Web pages. If you set the Disable the General page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the General page policy removes the General tab from the interface. Note: The default link colors are ignored on Web pages on which the author has specified link colors.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing Messaging settings	at least Internet Explorer v5.01	Prevents users from changing the default programs for messaging tasks. If you enable this policy, the E-mail, Newsgroups, and Internet Call options in the Internet Programs area appear dimmed. To display these options, users open the Internet Options dialog box, and then click the Programs tab. If you disable this policy or do not configure it, users can determine which programs to use for sending mail, viewing newsgroups, and placing Internet calls, if programs that perform these tasks are installed. The Disable the Programs page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing Profile Assistant settings	at least Internet Explorer v5.01	Prevents users from changing Profile Assistant settings. If you enable this policy, the My Profile button appears dimmed in the Personal Information area on the Content tab in the Internet Options dialog box. If you disable this policy or do not configure it, users can change their

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				profile information, such as their street and e-mail addresses. The Disable the Connections page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing proxy settings	at least Internet Explorer v5.01	Prevents users from changing proxy settings. If you enable this policy, the proxy settings appear dimmed. These settings are in the Proxy Server area of the Local Area Network (LAN) Settings dialog box, which appears when the user clicks the Connections tab and then clicks the LAN Settings button in the Internet Options dialog box. If you set the Disable the Connections page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the Disable the Connections page policy removes the Connections tab from the interface.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable changing ratings settings	at least Internet Explorer v5.01	Prevents users from changing ratings that help control the type of Internet content that can be viewed. If you enable this policy, the settings in the Content Advisor area on the Content tab in the Internet Options dialog box appear dimmed. If you disable this policy or do not configure it, users can change their ratings settings. The Disable the Ratings page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Ratings tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer	Disable the Reset Web Settings feature	at least Internet Explorer v5.01	Prevents users from restoring default settings for home and search pages. If you enable this policy, the Reset Web Settings button on the Programs tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can restore the default settings for home and search pages. The Disable the Programs page policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer	Search: Disable Find Files via F3 within the	at least Internet Explorer v5.01	Disables using the F3 key to search in Internet Explorer and Windows Explorer. If you enable this policy, the search functionality of the F3 key is disabled. Users cannot press F3 to search the Internet (from Internet

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
		browser		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. If you disable this policy or do not configure it, users can press F3 to search the Internet (from Internet Explorer) or the hard disk (from Windows Explorer). This policy is intended for situations in which administrators do not want users to explore the Internet or the hard disk. This policy can be used in coordination with the File Menu: Disable Open menu option policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser Menus), which prevents users from opening files by using the browser.
USER	Administrative Templates\Windows Components\Internet Explorer	Search: Disable Search Customization	at least Internet Explorer v5.01	Makes the Customize button in the Search Assistant appear dimmed. The Search Assistant is a tool that appears in the Search bar to help users search the Internet. If you enable this policy, users cannot change their Search Assistant settings, such as setting default search engines for specific tasks. If you disable this policy or do not configure it, users can change their settings for the Search Assistant. This policy is designed to help administrators maintain consistent settings for searching across an organization.
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Carpoint	at least Internet Explorer v5.01	Designates the Microsoft Network (MSN) Carpoint automatic pricing control as administrator-approved. This control enables enhanced pricing functionality on the Carpoint Web site, where users can shop for and obtain information about vehicles. If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run. If you disable this policy or do not configure it, this control will not be designated as administrator-approved. To specify how administrator-approved controls are handled for each security zone, carry out the following steps: 1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security. 2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings. 3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level. 4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	DHTML Edit Control	at least Internet Explorer v5.01	

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Shockwave Flash	at least Internet Explorer v5.01	
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Investor	at least Internet Explorer v5.01	Designates a set of Microsoft Network (MSN) Investor controls as administrator-approved. These controls enable users to view updated lists of stocks on their Web pages. If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run. If you disable this policy or do not configure it, these controls will not be designated as administrator-approved. Select the check boxes for the controls that you want to designate as administrator-approved. To specify how administrator-approved controls are handled for each security zone, carry out the following steps: 1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security. 2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings. 3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level. 4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Media Player	at least Internet Explorer v5.01	Designates the Media Player ActiveX control as administrator-approved. This control is used for playing sounds, videos, and other media. If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run. If you disable this policy or do not configure it, this control will not be designated as administrator-approved. To specify how administrator-approved controls are handled for each security zone, carry out the following steps: 1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security. 2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings. 3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level. 4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Menu Controls	at least Internet Explorer v5.01	Designates a set of Microsoft ActiveX controls used to manipulate pop-up menus in the browser as administrator-approved. If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run. If you disable this policy or do not configure it, these controls will not be designated as

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				administrator-approved. To specify a control as administrator-approved, click Enabled, and then select the check box for the control: -- MCSiMenu - enables Web authors to control the placement and appearance of Windows pop-up menus on Web pages -- Popup Menu Object - enables Web authors to add pop-up menus to Web pages To specify how administrator-approved controls are handled for each security zone, carry out the following steps: 1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security. 2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings. 3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level. 4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Microsoft Agent	at least Internet Explorer v5.01	Designates the Microsoft Agent ActiveX control as administrator-approved. Microsoft Agent is a set of software services that supports the presentation of software agents as interactive personalities within the Microsoft Windows interface. If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run. If you disable this policy or do not configure it, these controls will not be designated as administrator-approved. To specify how administrator-approved controls are handled for each security zone, carry out the following steps: 1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security. 2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings. 3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level. 4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Microsoft Chat	at least Internet Explorer v5.01	Designates the Microsoft Chat ActiveX control as administrator-approved. This control is used by Web authors to build text-based and graphical-based Chat communities for real-time conversations on the Web. If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run. If you disable this policy or do not configure it, this control will not be designated as administrator-approved. To specify how administrator-approved controls are handled for each security zone, carry out the following steps: 1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security. 2. Double-click Security Zones and Content Ratings, click Import the Current Security

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Zones Settings, and then click Modify Settings. 3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level. 4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	MSNBC	at least Internet Explorer v5.01	Designates a set of MSNBC controls as administrator-approved. These controls enable enhanced browsing of news reports on the MSNBC Web site. If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run. If you disable this policy or do not configure it, these controls will not be designated as administrator-approved. Select the check boxes for the controls that you want to designate as administrator-approved. To specify how administrator-approved controls are handled for each security zone, carry out the following steps: 1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security. 2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings. 3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level. 4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	NetShow File Transfer Control	at least Internet Explorer v5.01	
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Microsoft Scriptlet Component	at least Internet Explorer v5.01	
USER	Administrative Templates\Windows Components\Internet Explorer\Administrator Approved Controls	Microsoft Survey Control	at least Internet Explorer v5.01	
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	File menu: Disable closing the browser and Explorer windows	at least Internet Explorer v5.01	Prevents users from closing Microsoft Internet Explorer and Windows Explorer. If you enable this policy, the Close command on the File menu will appear dimmed. If you disable this policy or do not configure it, users are not prevented from closing the browser or Windows Explorer. Note: The Close button in the top right corner of the program will not work; if users click the Close button, they will be informed that the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				command is not available.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	File menu: Disable Save As... menu option	at least Internet Explorer v5.01	Prevents users from saving Web pages from the browser File menu to their hard disk or to a network share. If you enable this policy, the Save As command on the File menu will be removed. If you disable this policy or do not configure it, users can save Web pages for later viewing. This policy takes precedence over the File Menu: Disable Save As Web Page Complete policy, which prevents users from saving the entire contents that are displayed or run from a Web Page, such as graphics, scripts, and linked files, but does not prevent users from saving the text of a Web page. Caution: If you enable this policy, users are not prevented from saving Web content by pointing to a link on a Web page, clicking the right mouse button, and then clicking Save Target As.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	File menu: Disable Save As Web Page Complete	at least Internet Explorer v5.01	Prevents users from saving the complete contents that are displayed on or run from a Web page, including the graphics, scripts, linked files, and other elements. It does not prevent users from saving the text of a Web page. If you enable this policy, the Web Page, Complete file type option will be removed from the Save as Type box in the Save Web Page dialog box. Users can still save Web pages as hypertext markup language (HTML) files or as text files, but graphics, scripts, and other elements are not saved. To display the Save Web Page dialog box, users click the File menu, and then click the Save As command. If you disable this policy or do not configure it, users can save all elements on a Web page. The File menu: Disable Save As... menu option policy, which removes the Save As command, takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	File menu: Disable New menu option	at least Internet Explorer v5.01	Prevents users from opening a new browser window from the File menu. If this policy is enabled, users cannot open a new browser window by clicking the File menu, pointing to the New menu, and then clicking Window. The user interface is not changed, but a new window will not be opened, and users will be informed that the command is not available. If you disable this policy or do not configure it, users can open a new browser window from the File menu. Caution: This policy does not prevent users from opening a new browser window by right-clicking, and then clicking the Open in New Window command. To prevent users from using the shortcut menu to open new browser windows, you should also set the Disable Open in New Window menu option policy, which disables this command on the shortcut menu, or the Disable context menu policy, which disables the entire shortcut menu.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	File menu: Disable Open menu option	at least Internet Explorer v5.01	Prevents users from opening a file or Web page from the File menu in Internet Explorer. If you enable this policy, the Open dialog box will not appear when users click the Open command on the File menu. If users click the Open command, they will be notified that the command is not available. If you disable this policy or do not configure it, users can open a Web page from the browser File menu. Caution: This policy does not prevent users from right-clicking a link on a Web page, and then clicking the Open or Open in New Window command. To prevent users from opening Web pages by using the shortcut menu, set the Disable Open in New Window menu option policy, which disables this command on the shortcut menu, or the Disable context menu policy, which disables the entire shortcut menu.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Help menu: Remove 'Send Feedback' menu option	at least Internet Explorer v5.01	Prevents users from sending feedback to Microsoft by clicking the Send Feedback command on the Help menu. If you enable this policy, the Send Feedback command is removed from the Help menu. If you disable this policy or do not configure it, users can fill out an Internet form to provide feedback about Microsoft products.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Help menu: Remove 'For Netscape Users' menu option	at least Internet Explorer v5.01	Prevents users from displaying tips for users who are switching from Netscape. If you enable this policy, the For Netscape Users command is removed from the Help menu. If you disable this policy or do not configure it, users can display content about switching from Netscape by clicking the For Netscape Users command on the Help menu. Caution: Enabling this policy does not remove the tips for Netscape users from the Microsoft Internet Explorer Help file.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Help menu: Remove 'Tip of the Day' menu option	at least Internet Explorer v5.01	Prevents users from viewing or changing the Tip of the Day interface in Microsoft Internet Explorer. If you enable this policy, the Tip of the Day command is removed from the Help menu. If you disable this policy or do not configure it, users can enable or disable the Tip of the Day, which appears at the bottom of the browser.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Help menu: Remove 'Tour' menu option		Prevents users from running the Internet Explorer Tour from the Help menu in Internet Explorer. If you enable this policy, the Tour command is removed from the Help menu. If you disable this policy or do not configure it, users can run the tour from the Help menu.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Disable Context menu	at least Internet Explorer v5.01	Prevents the shortcut menu from appearing when users click the right mouse button while using the browser. If you enable this policy, the shortcut menu will not appear when users point to a Web page, and then click the right mouse button. If you disable this policy or do not configure

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				it, users can use the shortcut menu. This policy can be used to ensure that the shortcut menu is not used as an alternate method of running commands that have been removed from other parts of the interface.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Hide Favorites menu	at least Internet Explorer v5.01	Prevents users from adding, removing, or editing the list of Favorite links. The Favorites list is a way to store popular links for future use. If you enable this policy, the Favorites menu is removed from the interface, and the Favorites button on the browser toolbar appears dimmed. The Add to Favorites command on the shortcut menu is disabled; when users click it, they are informed that the command is unavailable. If you disable this policy or do not configure it, users can manage their Favorites list. This policy is intended to ensure that users maintain consistent lists of favorites across your organization. Note: If you enable this policy, users also cannot click Synchronize on the Tools menu to manage their favorite links that are set up for offline viewing.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Disable Open in New Window menu option	at least Internet Explorer v5.01	Prevents using the shortcut menu to open a link in a new browser window. If you enable this policy, users cannot point to a link, click the right mouse button, and then click the Open in New Window command. If you disable this policy or do not configure it, users can open a Web page in a new browser window by using the shortcut menu. This policy can be used in coordination with the File menu: Disable New menu option policy, which prevents users from opening the browser in a new window by clicking the File menu, pointing to New, and then clicking Window. Note: When users click the Open in New Window command, the link will not open in a new window and they will be informed that the command is not available.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Disable Save this program to disk option	at least Internet Explorer v5.01	Prevents users from saving a program or file that Microsoft Internet Explorer has downloaded to the hard disk. If you enable this policy, users cannot save a program to disk by clicking the Save This Program to Disk command while attempting to download a file. The file will not be downloaded and users will be informed that the command is not available. If you disable this policy or do not configure it, users can download programs from their browsers.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	Tools menu: Disable Internet Options... menu option	at least Internet Explorer v5.01	Prevents users from opening the Internet Options dialog box from the Tools menu in Microsoft Internet Explorer. If you enable this policy, users cannot change their Internet options, such as default home page, cache size, and connection and proxy settings, from the browser Tools menu. When users click the Internet Options command on the Tools menu, they are informed that the command is unavailable. If you disable

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				this policy or do not configure it, users can change their Internet settings from the browser Tools menu. Caution: This policy does not prevent users from viewing and changing Internet settings by clicking the Internet Options icon in Windows Control Panel. Also, see policies for Internet options in the \Administrative Templates\Windows Components\Internet Explorer and in \Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel folders.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	View menu: Disable Full Screen menu option	at least Internet Explorer v5.01	Prevents users from displaying the browser in full-screen (kiosk) mode, without the standard toolbar. If you enable this policy, the Full Screen command on the View menu will appear dimmed, and pressing F11 will not display the browser in a full screen. If you disable this policy or do not configure it, users can display the browser in a full screen. This policy is intended to prevent users from displaying the browser without toolbars, which might be confusing for some beginning users.
USER	Administrative Templates\Windows Components\Internet Explorer\Browser menus	View menu: Disable Source menu option	at least Internet Explorer v5.01	Prevents users from viewing the HTML source of Web pages by clicking the Source command on the View menu. If you enable this policy, the Source command on the View menu will appear dimmed. If you disable this policy or do not configure it, then users can view the HTML source of Web pages from the browser View menu. Caution: This policy does not prevent users from viewing the HTML source of a Web page by right-clicking a Web page to open the shortcut menu, and then clicking View Source. To prevent users from viewing the HTML source of a Web page from the shortcut menu, set the Disable context menu policy, which disables the entire shortcut menu.
USER	Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel	Disable the Advanced page	at least Internet Explorer v5.01	Removes the Advanced tab from the interface in the Internet Options dialog box. If you enable this policy, users are prevented from seeing and changing advanced Internet settings, such as security, multimedia, and printing. If you disable this policy or do not configure it, users can see and change these settings. When you set this policy, you do not need to set the Disable changing Advanced page settings policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\), because this policy removes the Advanced tab from the interface.
USER	Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel	Disable the Connections page	at least Internet Explorer v5.01	Removes the Connections tab from the interface in the Internet Options dialog box. If you enable this policy, users are prevented from seeing and changing connection and proxy settings. If you disable this policy or do not configure it, users can see and change these settings. When you set this policy, you do not need to set the following policies for the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Content tab, because this policy removes the Connections tab from the interface: Disable Internet Connection Wizard Disable changing connection settings Disable changing proxy settings Disable changing Automatic Configuration settings
USER	Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel	Disable the Content page	at least Internet Explorer v5.01	Removes the Content tab from the interface in the Internet Options dialog box. If you enable this policy, users are prevented from seeing and changing ratings, certificates, AutoComplete, Wallet, and Profile Assistant settings. If you disable this policy or do not configure it, users can see and change these settings. When you set this policy, you do not need to set the following policies for the Content tab, because this policy removes the Content tab from the interface: Disable changing ratings settings Disable changing certificate settings Disable changing Profile Assistant settings Disable AutoComplete for forms Do not allow AutoComplete to save passwords
USER	Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel	Disable the General page	at least Internet Explorer v5.01	Removes the General tab from the interface in the Internet Options dialog box. If you enable this policy, users are unable to see and change settings for the home page, the cache, history, Web page appearance, and accessibility. If you disable this policy or do not configure it, users can see and change these settings. When you set this policy, you do not need to set the following Internet Explorer policies (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\), because this policy removes the General tab from the interface: Disable changing home page settings Disable changing Temporary Internet files settings Disable changing history settings Disable changing color settings Disable changing link color settings Disable changing font settings Disable changing language settings Disable changing accessibility settings
USER	Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel	Disable the Privacy page	at least Internet Explorer v5.01	Removes the Privacy tab from the interface in the Internet Options dialog box. If you enable this policy, users are prevented from seeing and changing default settings for privacy. If you disable this policy or do not configure it, users can see and change these settings.
USER	Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel	Disable the Programs page	at least Internet Explorer v5.01	Removes the Programs tab from the interface in the Internet Options dialog box. If you enable this policy, users are prevented from seeing and changing default settings for Internet programs. If you disable this policy or do not configure it, users can see and change these settings. When you set this policy, you do not need to set the following policies for the Programs tab, because this policy removes the Programs tab from the interface: Disable changing Messaging settings Disable changing

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Calendar and Contact settings Disable the Reset Web Settings feature Disable changing default browser check
USER	Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel	Disable the Security page	at least Internet Explorer v5.01	Removes the Security tab from the interface in the Internet Options dialog box. If you enable this policy, it prevents users from seeing and changing settings for security zones, such as scripting, downloads, and user authentication. If you disable this policy or do not configure it, users can see and change these settings. When you set this policy, you do not need to set the following Internet Explorer policies, because this policy removes the Security tab from the interface: Security zones: Do not allow users to change policies Security zones: Do not allow users to add/delete sites
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Subscription Limits	at least Internet Explorer v5.01	Restricts the amount of information downloaded for offline viewing. If you enable this policy, you can set limits to the size and number of pages that users can download. If users attempt to exceed the number of subscriptions, a prompt will appear that states that they cannot set up more Web sites for offline viewing. If you disable this policy or do not configure it, then users can determine the amount of content that is searched for new information and downloaded. Caution: Although the Maximum Number of Offline Pages option determines how many levels of a Web site are searched for new information, it does not change the user interface in the Offline Favorites wizard. Note: The begin and end times for downloading are measured in minutes after midnight. The Maximum Offline Page Crawl Depth setting specifies how many levels of a Web site are searched for new information.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable adding channels	at least Internet Explorer v5.01	Prevents users from adding channels to Internet Explorer. Channels are Web sites that are updated automatically on your computer, according to a schedule specified by the channel provider. If you enable this policy, the Add Active Channel button, which appears on a channel that users haven't yet subscribed to, will be disabled. Users also cannot add content that is based on a channel, such as some of the Active Desktop items from Microsoft's Active Desktop Gallery, to their desktop. If you disable this policy or do not configure it, users can add channels to the Channel bar or to their desktop. Note: Most channel providers use the words Add Active Channel for this option; however, a few use different words, such as Subscribe.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline	Disable adding schedules for offline	at least Internet Explorer v5.01	Prevents users from specifying that Web pages can be downloaded for viewing offline. When users make Web pages available for offline viewing, they can view the content when their computer is not connected

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Pages	pages		to the Internet. If you enable this policy, users cannot add new schedules for downloading offline content. The Make Available Offline check box will be dimmed in the Add Favorite dialog box. If you disable this policy or do not configure it, users can add new offline content schedules. This policy is intended for organizations that are concerned about server load for downloading content. The Hide Favorites menu policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable offline page hit logging	at least Internet Explorer v5.01	Prevents channel providers from recording information about when their channel pages are viewed by users who are working offline. If you enable this policy, it disables any channel logging settings set by channel providers in the channel definition format (.cdf) file. The .cdf file determines the schedule and other settings for downloading Web content. If you disable this policy or do not configure it, channel providers can record information about when their channel pages are viewed by users who are working offline.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable channel user interface completely	at least Internet Explorer v5.01	Prevents users from viewing the Channel bar interface. Channels are Web sites that are automatically updated on their computer according to a schedule specified by the channel provider. If you enable this policy, the Channel bar interface will be disabled, and users cannot select the Internet Explorer Channel Bar check box on the Web tab in the Display Properties dialog box. If you disable this policy or do not configure it, users can view and subscribe to channels from the Channel bar interface.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable editing and creating of schedule groups	at least Internet Explorer v5.01	Prevents users from adding, editing, or removing schedules for offline viewing of Web pages and groups of Web pages that users have subscribed to. A subscription group is a favorite Web page plus the Web pages it links to. If you enable this policy, the Add, Remove, and Edit buttons on the Schedule tab in the Web page Properties dialog box are dimmed. To display this tab, users click the Tools menu, click Synchronize, select a Web page, click the Properties button, and then click the Schedule tab. If you disable this policy or do not configure it, users can add, remove, and edit schedules for Web sites and groups of Web sites. The Disable editing schedules for offline pages policy and the Hide Favorites menu policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) take precedence over this policy. If either policy is enabled, this

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable editing schedules for offline pages	at least Internet Explorer v5.01	Prevents users from editing an existing schedule for downloading Web pages for offline viewing. When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet. If you enable this policy, users cannot display the schedule properties of pages that have been set up for offline viewing. If users click the Tools menu, click Synchronize, select a Web page, and then click the Properties button, no properties are displayed. Users do not receive an alert stating that the command is unavailable. If you disable this policy or do not configure it, users can edit an existing schedule for downloading Web content for offline viewing. This policy is intended for organizations that are concerned about server load for downloading content. The Hide Favorites menu policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable removing channels	at least Internet Explorer v5.01	Prevents users from disabling channel synchronization in Microsoft Internet Explorer. Channels are Web sites that are automatically updated on your computer according to a schedule specified by the channel provider. If you enable this policy, users cannot prevent channels from being synchronized. If you disable this policy or do not configure it, users can disable the synchronization of channels. This policy is intended to help administrators ensure that users' computers are being updated uniformly across their organization. Note: This policy does not prevent users from removing active content from the desktop interface.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable removing schedules for offline pages	at least Internet Explorer v5.01	Prevents users from clearing the preconfigured settings for Web pages to be downloaded for offline viewing. When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet. If you enable this policy, the Make Available Offline check box in the Organize Favorites Favorite dialog box and the Make This Page Available Offline check box will be selected but dimmed. To display the Make This Page Available Offline check box, users click the Tools menu, click Synchronize, and then click the Properties button. If you disable this policy or do not configure it, users can remove the preconfigured settings for pages to be downloaded for offline viewing. This policy is intended for organizations that are concerned about server load for downloading content. The Hide

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Favorites menu policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable all scheduled offline pages	at least Internet Explorer v5.01	Disables existing schedules for downloading Web pages for offline viewing. When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet. If you enable this policy, the check boxes for schedules on the Schedule tab of the Web page properties are cleared and users cannot select them. To display this tab, users click the Tools menu, click Synchronize, select a Web page, click the Properties button, and then click the Schedule tab. If you disable this policy, then Web pages can be updated on the schedules specified on the Schedule tab. This policy is intended for organizations that are concerned about server load for downloading content. The Hide Favorites menu policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer\Offline Pages	Disable downloading of site subscription content	at least Internet Explorer v5.01	Prevents content from being downloaded from Web sites that users have subscribed to. When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet. If you enable this policy, content will not be downloaded from Web sites that users have subscribed to. However, synchronization with the Web pages will still occur to determine if any content has been updated since the last time the user synchronized with or visited the page. If you disable this policy or do not configure it, content will not be prevented from being downloaded. The Disable downloading of site subscription content policy and the Hide Favorites menu policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) take precedence over this policy. If either policy is enabled, this policy is ignored.
USER	Administrative Templates\Windows Components\Internet Explorer\Persistence Behavior	File size limits for Local Machine zone	at least Internet Explorer v5.01	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Local Computer security zone. If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone. If you disable this policy or do not configure it, you cannot set this limit. Note: This setting does not appear in the user interface.
USER	Administrative Templates\Windows Components\Internet	File size limits for	at least Internet	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Local Intranet security zone. If you

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Explorer\Persistence Behavior	Intranet zone	Explorer v5.01	enable this policy, you can specify the persistence storage amount per domain or per document for this security zone. If you disable this policy or do not configure it, you cannot set this limit. Note: This setting does not appear in the user interface.
USER	Administrative Templates\Windows Components\Internet Explorer\Persistence Behavior	File size limits for Trusted Sites zone	at least Internet Explorer v5.01	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Trusted Sites security zone. If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone. If you disable this policy or do not configure it, you cannot set this limit. Note: This setting does not appear in the user interface.
USER	Administrative Templates\Windows Components\Internet Explorer\Persistence Behavior	File size limits for Internet zone	at least Internet Explorer v5.01	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Internet security zone. If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone. If you disable this policy or do not configure it, you cannot set this limit. Note: This setting does not appear in the user interface.
USER	Administrative Templates\Windows Components\Internet Explorer\Persistence Behavior	File size limits for Restricted Sites zone	at least Internet Explorer v5.01	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Restricted Sites security zone. If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone. If you disable this policy or do not configure it, you cannot set this limit. Note: This setting does not appear in the user interface.
USER	Administrative Templates\Windows Components\Internet Explorer\Toolbars	Disable customizing browser toolbars	at least Internet Explorer v5.01	Prevents users from determining which toolbars are displayed in Microsoft Internet Explorer and Windows Explorer. If you enable this policy, the list of toolbars, which users can display by clicking the View menu and then pointing to the Toolbars command, will appear dimmed. If you disable this policy or do not configure it, users can determine which toolbars are displayed in Windows Explorer and Internet Explorer. This policy can be used in coordination with the Disable customizing browser toolbar buttons policy, which prevents users from adding or removing toolbars from Internet Explorer.
USER	Administrative Templates\Windows Components\Internet Explorer\Toolbars	Disable customizing browser toolbar buttons	at least Internet Explorer v5.01	Prevents users from determining which buttons appear on the Microsoft Internet Explorer and Windows Explorer standard toolbars. If you enable this policy, the Customize command on the Toolbars submenu of the View menu will be removed. If you disable this policy or do not configure it, users can customize which buttons appear on the Internet Explorer and Windows Explorer toolbars. This policy can be used in coordination

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				with the Disable customizing browser toolbars policy, which prevents users from determining which toolbars are displayed in Internet Explorer and Windows Explorer.
USER	Administrative Templates\Windows Components\Internet Explorer\Toolbars	Configure Toolbar Buttons	at least Internet Explorer v5.01	Specifies which buttons will be displayed on the standard toolbar in Microsoft Internet Explorer. If you enable this policy, you can specify whether or not each button will be displayed by selecting or clearing the check boxes for each button. If you disable this policy or do not configure it, the standard toolbar will be displayed with its default settings, unless users customize it.
USER	Administrative Templates\Windows Components\Microsoft Management Console	Restrict the user from entering author mode	At least Microsoft Windows 2000	Prevents users from entering author mode. This setting prevents users from opening the Microsoft Management Console (MMC) in author mode, explicitly opening console files in author mode, and opening any console files that open in author mode by default. As a result, users cannot create console files or add or remove snap-ins. Also, because they cannot open author-mode console files, they cannot use the tools that the files contain. This setting permits users to open MMC user-mode console files, such as those on the Administrative Tools menu in Windows 2000 Server family or Windows Server 2003 family. However, users cannot open a blank MMC console window on the Start menu. (To open the MMC, click Start, click Run, and type mmc.) Users also cannot open a blank MMC console window from a command prompt. If you disable this setting or do not configure it, users can enter author mode and open author-mode console files.
USER	Administrative Templates\Windows Components\Microsoft Management Console	Restrict users to the explicitly permitted list of snap-ins	At least Microsoft Windows 2000	Lets you selectively permit or prohibit the use of Microsoft Management Console (MMC) snap-ins. -- If you enable this setting, all snap-ins are prohibited, except those that you explicitly permit. Use this setting if you plan to prohibit use of most snap-ins. To explicitly permit a snap-in, open the Restricted/Permitted snap-ins setting folder and enable the settings representing the snap-in you want to permit. If a snap-in setting in the folder is disabled or not configured, the snap-in is prohibited. -- If you disable this setting or do not configure it, all snap-ins are permitted, except those that you explicitly prohibit. Use this setting if you plan to permit use of most snap-ins. To explicitly prohibit a snap-in, open the Restricted/Permitted snap-ins setting folder and then disable the settings representing the snap-ins you want to prohibit. If a snap-in setting in the folder is enabled or not configured, the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				prohibited snap-in, the console file opens, but the prohibited snap-in does not appear. Note: If you enable this setting, and you do not enable any settings in the Restricted/Permitted snap-ins folder, users cannot use any MMC snap-ins.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Active Directory Domains and Trusts	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Active Directory Sites and Services	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management	Active Directory Users and Computers	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Console\Restricted/Permitted snap-ins			If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	ActiveX Control	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	ADSI Edit	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Certification Authority	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Certificates	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Certificate Templates	At least Microsoft Windows Server 2003	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Component Services	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Computer Management	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Device Manager	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Distributed File System	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Disk Defragmenter	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Disk Management	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Event Viewer	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	FAX Service	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	FrontPage Server Extensions	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Internet Authentication Service (IAS)	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Internet Information Services	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows	Indexing Service	At least Microsoft	Permits or prohibits use of this snap-in. If you enable this setting, the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Microsoft Management Console\Restricted/Permitted snap-ins		Windows 2000	snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	IP Security Policy Management	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	IP Security Monitor	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Link to Web Address	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Local Users and Groups	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	.Net Framework Configuration	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Performance Logs and Alerts	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	QoS Admission Control	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Remote Desktops	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Routing and Remote Access	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Removable Storage Management	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Security Configuration and Analysis	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management	Security Templates	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Console\Restricted/Permitted snap-ins			If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Services	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Shared Folders	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	System Information	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Telephony	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Terminal Services Configuration	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	Wireless Monitor	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins	WMI Control	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	AppleTalk Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Authorization Manager	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Certification Authority Policy Settings	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Connection Sharing (NAT)	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	DCOM Configuration Extension	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Device Manager	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	DHCP Relay Management	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Event Viewer	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Extended View (Web View)	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows	IAS Logging	At least Microsoft	Permits or prohibits use of this snap-in. If you enable this setting, the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins		Windows 2000	snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	IGMP Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	IP Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	IPX RIP Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	IPX Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	IPX SAP Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Logical and Mapped Drives	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	OSPF Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Public Key Policies	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	RAS Dialin - User Node	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Remote Access	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Removable Storage	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management	RIP Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Console\Restricted/Permitted snap-ins\Extension snap-ins			If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Routing	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Send Console Message	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Service Dependencies	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	Shared Folders Ext	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	SMTP Protocol	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	SNMP	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Extension snap-ins	System Properties	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy	Group Policy Management	At least Microsoft Windows XP Professional with SP1 or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy	Group Policy Object Editor	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy	Group Policy tab for Active Directory Tools	At least Microsoft Windows 2000	Permits or prohibits use of the Group Policy tab in property sheets for the Active Directory Users and Computers and Active Directory Sites and Services snap-ins. If you enable this setting, the Group Policy tab is displayed in the property sheet for a site, domain, or organizational unit diplayed by the Active Directory Users and Computers and Active Directory Sites and Services snap-ins. If you disable the setting, the Group Policy tab is not displayed in those snap-ins. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this tab is displayed. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users will not have access to the Group Policy tab. To explicitly permit use of the Group Policy tab, enable this setting. If this setting is not configured (or disabled), the Group Policy tab is inaccessible. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users will have access to the Group Policy tab. To explicitly prohibit use of the Group Policy tab, disable this setting. If this setting is not configured (or enabled), the Group Policy tab is accessible. When the Group Policy tab is inaccessible, it does not appear in the site, domain, or organizational unit property sheets.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy	Resultant Set of Policy snap-in	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows	Administrative	At least Microsoft	Permits or prohibits use of this snap-in. If you enable this setting, the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Templates (Computers)	Windows 2000	snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Administrative Templates (Users)	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Folder Redirection	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Internet Explorer Maintenance	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Remote Installation Services	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Scripts (Startup/Shutdown)	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Scripts (Logon/Logoff)	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Security Settings	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Software Installation (Computers)	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Software Installation (Users)	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Group Policy snap-in extensions	Wireless Network (IEEE 802.11) Policies	At least Microsoft Windows 2000	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions	Administrative Templates (Computers)	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management	Administrative Templates (Users)	At least Microsoft Windows XP	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions		Professional or Windows Server 2003 family	If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions	Folder Redirection	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions	Internet Explorer Maintenance	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions	Scripts (Startup/Shutdown)	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions	Scripts (Logon/Logoff)	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions	Security Settings	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions	Software Installation (Computers)	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy\Resultant Set of Policy snap-in extensions	Software Installation (Users)	At least Microsoft Windows XP Professional or Windows Server 2003 family	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the Restrict users to the explicitly permitted list of snap-ins setting determines whether this snap-in is permitted or prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is enabled, users cannot use any snap-in except those explicitly permitted. To explicitly permit use of this snap-

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. -- If Restrict users to the explicitly permitted list of snap-ins is disabled or not configured, users can use any snap-in except those explicitly prohibited. To explicitly prohibit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.
USER	Administrative Templates\Windows Components\NetMeeting	Allow persisting automatic acceptance of Calls	at least Windows NetMeeting v3.0	Make the automatic acceptance of incoming calls persistent.
USER	Administrative Templates\Windows Components\NetMeeting	Disable Chat	at least Windows NetMeeting v3.0	Disables the Chat feature of NetMeeting.
USER	Administrative Templates\Windows Components\NetMeeting	Disable Whiteboard	at least Windows NetMeeting v3.0	Disables the T.126 whiteboard feature of NetMeeting.
USER	Administrative Templates\Windows Components\NetMeeting	Disable NetMeeting 2.x Whiteboard	at least Windows NetMeeting v3.0	Disables the 2.x whiteboard feature of NetMeeting. The 2.x whiteboard is available for compatibility with older versions of NetMeeting only. Deployers who do not need it can save bandwidth by disabling it.
USER	Administrative Templates\Windows Components\NetMeeting	Enable Automatic Configuration	at least Windows NetMeeting v3.0	Configures NetMeeting to download settings for users each time it starts. The settings are downloaded from the URL listed in the Configuration URL: text box. Group Policy based settings have precedence over any conflicting settings set by downloading them from this URL.
USER	Administrative Templates\Windows Components\NetMeeting	Prevent adding Directory servers	at least Windows NetMeeting v3.0	Prevents users from adding directory (ILS) servers to the list of those they can use for placing calls.
USER	Administrative Templates\Windows Components\NetMeeting	Prevent automatic acceptance of Calls	at least Windows NetMeeting v3.0	Prevents users from turning on automatic acceptance of incoming calls. This ensures that others cannot call and connect to NetMeeting when the user is not present. This policy is recommended when deploying NetMeeting to run always.
USER	Administrative Templates\Windows Components\NetMeeting	Prevent changing Call placement method	at least Windows NetMeeting v3.0	Prevents users from changing the way calls are placed, either directly or via a gatekeeper server.
USER	Administrative Templates\Windows Components\NetMeeting	Disable Directory services	at least Windows NetMeeting v3.0	Disables the directory feature of NetMeeting. Users will not logon to a directory (ILS) server when NetMeeting starts. Users will also not be able to view or place calls via a NetMeeting directory. This policy is for deployers who have their own location or calling schemes such as a

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Web site or an address book.
USER	Administrative Templates\Windows Components\NetMeeting	Prevent receiving files	at least Windows NetMeeting v3.0	Prevents users from receiving files from others in a conference.
USER	Administrative Templates\Windows Components\NetMeeting	Prevent sending files	at least Windows NetMeeting v3.0	Prevents users from sending files to others in a conference.
USER	Administrative Templates\Windows Components\NetMeeting	Prevent viewing Web directory	at least Windows NetMeeting v3.0	Prevents users from viewing directories as Web pages in a browser.
USER	Administrative Templates\Windows Components\NetMeeting	Limit the size of sent files	at least Windows NetMeeting v3.0	Limits the size of files users can send to others in a conference.
USER	Administrative Templates\Windows Components\NetMeeting	Set the intranet support Web page	at least Windows NetMeeting v3.0	Sets the URL NetMeeting will display when the user chooses the Help Online Support command.
USER	Administrative Templates\Windows Components\NetMeeting	Set Call Security options	at least Windows NetMeeting v3.0	Sets the level of security for both outgoing and incoming NetMeeting calls.
USER	Administrative Templates\Windows Components\NetMeeting\Application Sharing	Disable application Sharing	at least Windows NetMeeting v3.0	Disables the application sharing feature of NetMeeting completely. Users will not be able to host or view shared applications.
USER	Administrative Templates\Windows Components\NetMeeting\Application Sharing	Prevent Control	at least Windows NetMeeting v3.0	Prevents users from allowing others in a conference to control what they have shared. This enforces a read-only mode; the other participants cannot change the data in the shared application.
USER	Administrative Templates\Windows Components\NetMeeting\Application Sharing	Prevent Sharing	at least Windows NetMeeting v3.0	Prevents users from sharing anything themselves. They will still be able to view shared applications/desktops from others.
USER	Administrative Templates\Windows Components\NetMeeting\Application Sharing	Prevent Sharing Command Prompts	at least Windows NetMeeting v3.0	Prevents users from sharing command prompts. This prevents users from inadvertently sharing out applications, since command prompts can be used to launch other applications.
USER	Administrative Templates\Windows Components\NetMeeting\Application Sharing	Prevent Desktop Sharing	at least Windows NetMeeting v3.0	Prevents users from sharing the whole desktop. They will still be able to share individual applications.
USER	Administrative Templates\Windows Components\NetMeeting\Application Sharing	Prevent Sharing Explorer windows	at least Windows NetMeeting v3.0	Prevents users from sharing Explorer windows. This prevents users from inadvertently sharing out applications, since Explorer windows can be used to launch other applications.
USER	Administrative Templates\Windows	Prevent Application	at least Windows	Prevents users from sharing applications in true color. True color

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\NetMeeting\Application Sharing	Sharing in true color	NetMeeting v3.0	sharing uses more bandwidth in a conference.
USER	Administrative Templates\Windows Components\NetMeeting\Audio & Video	Disable Audio	at least Windows NetMeeting v3.0	Disables the audio feature of NetMeeting. Users will not be able to send or receive audio.
USER	Administrative Templates\Windows Components\NetMeeting\Audio & Video	Prevent changing DirectSound Audio setting	at least Windows NetMeeting v3.0	Prevents user from changing the DirectSound audio setting. DirectSound provides much better audio quality, but older audio hardware may not support it.
USER	Administrative Templates\Windows Components\NetMeeting\Audio & Video	Disable full duplex Audio	at least Windows NetMeeting v3.0	Disables full duplex mode audio. Users will not be able to listen to incoming audio while speaking into the microphone. Older audio hardware does not perform well when in full duplex mode.
USER	Administrative Templates\Windows Components\NetMeeting\Audio & Video	Prevent receiving Video	at least Windows NetMeeting v3.0	Prevents users from receiving video. Users will still be able to send video provided they have the hardware.
USER	Administrative Templates\Windows Components\NetMeeting\Audio & Video	Prevent sending Video	at least Windows NetMeeting v3.0	Prevents users from sending video if they have the hardware. Users will still be able to receive video from others.
USER	Administrative Templates\Windows Components\NetMeeting\Audio & Video	Limit the bandwidth of Audio and Video	at least Windows NetMeeting v3.0	Limits the bandwidth audio and video will consume when in a conference. This setting will guide NetMeeting to choose the right formats and send rate so that the bandwidth is limited.
USER	Administrative Templates\Windows Components\NetMeeting\Options Page	Disable the Advanced Calling button	at least Windows NetMeeting v3.0	Disables the Advanced Calling button on the General Options page. Users will not then be able to change the call placement method and the servers used.
USER	Administrative Templates\Windows Components\NetMeeting\Options Page	Hide the Audio page	at least Windows NetMeeting v3.0	Hides the Audio page of the Tools Options dialog. Users will not then be able to change audio settings.
USER	Administrative Templates\Windows Components\NetMeeting\Options Page	Hide the General page	at least Windows NetMeeting v3.0	Hides the General page of the Tools Options dialog. Users will not then be able to change personal identification and bandwidth settings.
USER	Administrative Templates\Windows Components\NetMeeting\Options Page	Hide the Security page	at least Windows NetMeeting v3.0	Hides the Security page of the Tools Options dialog. Users will not then be able to change call security and authentication settings.
USER	Administrative Templates\Windows Components\NetMeeting\Options	Hide the Video page	at least Windows	Hides the Video page of the Tools Options dialog. Users will not then be

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Page		NetMeeting v3.0	able to change video settings.
USER	Administrative Templates\Windows Components\Task Scheduler	Prohibit Browse	At least Microsoft Windows 2000	Limits newly scheduled to items on the user's Start menu, and prevents the user from changing the scheduled program for existing tasks. This setting removes the Browse button from the Schedule Task Wizard and from the Task tab of the properties dialog box for a task. Also, users cannot edit the Run box or the Start in box that determine the program and path for a task. As a result, when users create a task, they must select a program from the list in the Scheduled Task Wizard, which displays only the tasks that appear on the Start menu and its submenus. Once a task is created, users cannot change the program a task runs. Important: This setting does not prevent users from creating a new task by pasting or dragging any program into the Scheduled Tasks folder. To prevent this action, use the Prohibit Drag-and-Drop setting. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
USER	Administrative Templates\Windows Components\Task Scheduler	Hide Advanced Properties Checkbox in Add Scheduled Task Wizard	At least Microsoft Windows 2000	This setting removes the Open advanced properties for this task when I click Finish checkbox from the last page of the Scheduled Task Wizard. This policy is only designed to simplify task creation for beginning users. The checkbox, when checked, instructs Task Scheduler to automatically open the newly created task's property sheet upon completion of the Add Scheduled Task wizard. The task's property sheet allows users to change task characteristics such as: the program the task runs, details of its schedule, idle time and power management settings, and its security context. Beginning users will often not be interested or confused by having the property sheet displayed automatically. Note that the checkbox is not checked by default even if this setting is Disabled or Not Configured. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
USER	Administrative Templates\Windows Components\Task Scheduler	Prohibit Drag-and-Drop	At least Microsoft Windows 2000	Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder. This setting disables the Cut, Copy, Paste, and Paste shortcut items on the context menu and the Edit menu in Scheduled Tasks. It also disables the drag-and-drop features of the Scheduled Tasks folder. As a result, users cannot add new scheduled tasks by dragging, moving, or copying a document or program into the Scheduled tasks folder. This setting does not prevent users

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				from using other methods to create new tasks, and it does not prevent users from deleting tasks. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
USER	Administrative Templates\Windows Components\Task Scheduler	Prevent Task Run or End	At least Microsoft Windows 2000	Prevents users from starting and stopping tasks manually. This setting removes the Run and End Task items from the context menu that appears when you right-click a task. As a result, users cannot start tasks manually or force tasks to end before they are finished. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
USER	Administrative Templates\Windows Components\Task Scheduler	Hide Property Pages	At least Microsoft Windows 2000	Prevents users from viewing and changing the properties of an existing task. This setting removes the Properties item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview. This setting prevents users from viewing and changing characteristics such as the program the task runs, its schedule details, idle time and power management settings, and its security context. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Tip: This setting affects existing tasks only. To prevent users from changing the properties of newly created tasks, use the Remove Advanced Menu setting.
USER	Administrative Templates\Windows Components\Task Scheduler	Prohibit New Task Creation	At least Microsoft Windows 2000	Prevents users from creating new tasks. This setting removes the Add Scheduled Task item that starts the New Task Wizard. Also, the system does not respond when users try to move, paste, or drag programs or documents into the Scheduled Tasks folder. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Important: This setting does not prevent administrators of a computer from using At.exe to create new tasks or prevent administrators from submitting tasks from remote computers.
USER	Administrative Templates\Windows	Prohibit Task Deletion	At least Microsoft	Prevents users from deleting tasks from the Scheduled Tasks folder. This setting removes the Delete command from the Edit menu in the

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Task Scheduler		Windows 2000	Scheduled Tasks folder and from the menu that appears when you right-click a task. Also, the system does not respond when users try to cut or drag a task from the Scheduled Tasks folder. Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. Important: This setting does not prevent administrators of a computer from using At.exe to delete tasks.
USER	Administrative Templates\Windows Components\Terminal Services	Sets rules for remote control of Terminal Services user sessions	At least Microsoft Windows XP Terminal Services	Specifies the level of remote control permitted in a Terminal Services session. Remote control can be established with or without the session user's permission. You can use this setting to select one of two levels of remote control: View Session permits the remote control user to watch a session, Full Control permits the remote control user to interact with the session. If the status is set to Enabled, administrators can remotely interact with a user's Terminal Services session according to the specified rules. To set these rules, select the desired level of control and permission in the Options list. To disable remote control, select No remote control allowed. If the status is set to Disabled or Not Configured, remote control rules are determined by the server administrator using the Terminal Services Configuration tool (tscc.msc). By default, remote control users can have full control with the session user's permission. Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
USER	Administrative Templates\Windows Components\Terminal Services	Start a program on connection	At least Microsoft Windows XP Terminal Services	Configures Terminal Services to run a specified program automatically upon connection. You can use this setting to specify a program to run automatically when a user logs on to a remote computer. By default, Terminal Services sessions provide access to the full Windows desktop, unless otherwise specified with this setting, by the server administrator, or by the user in configuring the client connection. Enabling this setting overrides the Start Program settings set by the server administrator or user. The Start menu and Windows Desktop are not displayed, and when the user exits the program the session is automatically logged off. To use this setting, in Program path and file name, type the fully qualified path and file name of the executable file to be run when the user logs on. If necessary, in Working Directory, type the fully qualified path to the starting directory for the program. If you leave Working Directory blank, the program runs with its default working directory. If the specified program path, file name, or working directory is not the name of a valid

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				directory, the terminal server connection fails with an error message. If the status is set to Enabled, Terminal Services sessions automatically run the specified program and use the specified Working Directory (or the program default directory, if Working Directory is not specified) as the working directory for the program. If the status is set to Disabled or Not Configured, Terminal Services sessions start with the full desktop, unless the server administrator or user specify otherwise. (See Computer Config\Administrative templates\Windows Components\System\Logon\Run these programs at user logon setting.) Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
USER	Administrative Templates\Windows Components\Terminal Services\Client	Do not allow passwords to be saved	At least Microsoft Windows XP Professional with SP2 or Windows Server 2003 family with SP1	Controls whether a user can save passwords using a Terminal Services client. If you enable this setting the password saving checkbox in Terminal Services clients will be disabled and users will no longer be able to save passwords. When a user opens an RDP file using the Terminal Services client and saves his settings, any password that previously existed in the RDP file will be deleted. If you disable this setting or leave it not configured, the user will be able to save passwords using the Terminal Services client.
USER	Administrative Templates\Windows Components\Terminal Services\Sessions	Terminate session when time limits are reached	At least Microsoft Windows XP Terminal Services	Specifies whether to terminate a timed-out Terminal Services session instead of disconnecting it. You can use this setting to direct Terminal Services to terminate a session (that is, the user is logged off and the session is deleted from the server) after time limits for active or idle sessions are reached. By default, Terminal Services disconnects sessions that reach their time limits. Time limits are set locally by the server administrator or in Group Policy. See the Sets a time limit for active Terminal Services sessions and Sets a time limit for active but idle Terminal Services sessions settings. If the status is set to Enabled, Terminal Services terminates any session that reaches its time-out limit. If the status is set to Disabled, Terminal Services always disconnects a timed-out session, even if specified otherwise by the server administrator. If the status is set to Not Configured, Terminal Services disconnects a timed-out session, unless specified otherwise in local settings. Note: This setting only applies to time-out limits that are deliberately set (in the Terminal Services Configuration tool or Group Policy Object Editor), not to time-out events that occur due to connectivity or network conditions. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				configured, the Computer Configuration setting overrides.
USER	Administrative Templates\Windows Components\Terminal Services\Sessions	Set time limit for disconnected sessions	At least Microsoft Windows XP Terminal Services	Specifies a time limit for disconnected Terminal Services sessions. You can use this setting to specify the maximum amount of time that a disconnected session is kept active on the server. By default, Terminal Services allows users to disconnect from a remote session without logging off and ending the session. When a session is in a disconnected state, running programs are kept active even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server. If the status is set to Enabled, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select Never. If the status is set to Disabled or Not Configured, time limits for disconnected sessions are not specified at the Group Policy level. Note: This setting does not apply to console sessions such as Remote Desktop sessions with computers running Windows XP Professional. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
USER	Administrative Templates\Windows Components\Terminal Services\Sessions	Sets a time limit for active but idle Terminal Services sessions	At least Microsoft Windows XP Terminal Services	Specifies a time limit for active but idle Terminal Services sessions. You can use this setting to specify the maximum amount of time that an active session can be idle (that is, no user input) before it is automatically disconnected. By default, Terminal Services allows active sessions to remain idle for an unlimited time. To use this setting, select Enabled, and then select the desired time limit in the Idle session limit drop-down list. If the status is set to Enabled, active but idle sessions are automatically disconnected after the specified amount of time. The user receives a two-minute warning before the session ends, which allows the user to press a key or move the mouse to keep the session active. If the status is set to Disabled or Not Configured, the time limit for active but idle sessions is not specified at the Group Policy level. However, an administrator can specify time limits for idle sessions in the Terminal Services Configuration tool. Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides. Idle session limits do not apply to the console session. To specify that user sessions are terminated at time-out, enable the Terminate session when time limits are reached setting.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Terminal Services\Sessions	Sets a time limit for active Terminal Services sessions	At least Microsoft Windows XP Terminal Services	Specifies a time limit for active Terminal Services sessions. You can use this setting to specify the maximum amount of time a Terminal Services session can be active before it is automatically disconnected. To use this setting, select Enabled, and then select the desired limit in the Active session limit drop-down list. By default, Terminal Services allows sessions to remain active for an unlimited time. If the status is set to Enabled, Terminal Services ends active sessions after the specified amount of time. The user receives a two-minute warning before the Terminal Services session ends, which allows the user to save open files and close programs. If the status is set to Disabled or Not Configured, time limits for active sessions are not specified at the Group Policy level. However, an administrator can specify time limits for active sessions in the Terminal Services Configuration tool. Note: This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides. Active session limits do not apply to the console session. To specify user sessions to be terminated at time-out, enable the Terminate session when time limits are reached setting.
USER	Administrative Templates\Windows Components\Terminal Services\Sessions	Allow reconnection from original client only	At least Microsoft Windows XP Terminal Services	Specifies whether to allow users to reconnect to a disconnected Terminal Services session using a computer other than the original client computer. You can use this setting to prevent Terminal Services users from reconnecting to the disconnected session using a computer other than the client computer from which they originally created the session. By default, Terminal Services allows users to reconnect to disconnected sessions from any client computer. If the status is set to Enabled, users can reconnect to disconnected sessions only from the original client computer. If a user attempts to connect to the disconnected session from another computer, a new session is created instead. If the status is set to Disabled, users can always connect to the disconnected session from any computer. If the status is set to Not Configured, session reconnection from the original client computer is not specified at the Group Policy level. Important: This option is only supported for Citrix ICA clients that provide a serial number when connecting; this setting is ignored if the user is connecting with a Windows client. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
USER	Administrative Templates\Windows	Turn on Classic Shell	At least Microsoft	This setting allows you to remove the Active Desktop and Web view features. If you enable this setting, it will disable the Active Desktop and

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Windows Explorer		Windows 2000	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. Note: This setting takes precedence over the Enable Active Desktop setting. If both policies are enabled, Active Desktop is disabled. Also, see the Disable Active Desktop setting in User Configuration\Administrative Templates\Desktop\Active Desktop and the Remove the Folder Options menu item from the Tools menu setting in User Configuration\Administrative Templates\Windows Components\Windows Explorer.
USER	Administrative Templates\Windows Components\Windows Explorer	Display confirmation dialog when deleting files	At least Microsoft Windows XP Professional or Windows Server 2003 family	Allows you to have Windows Explorer display a confirmation dialog whenever a file is deleted or moved to the Recycle Bin. If you enable this setting, a confirmation dialog is displayed when a file is deleted or moved to the Recycle Bin by the user. If you disable or do not configure this setting, the default behavior of not displaying a confirmation dialog occurs.
USER	Administrative Templates\Windows Components\Windows Explorer	Allow only per user or approved shell extensions	At least Microsoft Windows 2000	This setting is designed to ensure that shell extensions can operate on a per-user basis. If you enable this setting, Windows is directed to only run those shell extensions that have either been approved by an administrator or that will not impact other users of the machine. A shell extension only runs if there is an entry in at least one of the following locations in registry. For shell extensions that have been approved by the administrator and are available to all users of the computer, there must be an entry at HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved. For shell extensions to run on a per-user basis, there must be an entry at HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved.
USER	Administrative Templates\Windows Components\Windows Explorer	Do not track Shell shortcuts during roaming	At least Microsoft Windows 2000	Determines whether Windows traces shortcuts back to their sources when it cannot find the target on the user's system. Shortcut files typically include an absolute path to the original target file as well as the relative path to the current target file. When the system cannot find the file in the current target path, then, by default, it searches for the target in the original path. If the shortcut has been copied to a different computer, the original path might lead to a network computer, including external resources, such as an Internet server. If you enable this setting,

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Windows only searches the current target path. It does not search for the original path even when it cannot find the target file in the current target path.
USER	Administrative Templates\Windows Components\Windows Explorer	Maximum number of recent documents	At least Microsoft Windows 2000	Determines how many shortcuts the system can display in the Documents menu on the Start menu. The Documents menu contains shortcuts to the nonprogram files the user has most recently opened. By default, the system displays shortcuts to the 10 most recently opened documents.
USER	Administrative Templates\Windows Components\Windows Explorer	Turn off caching of thumbnail pictures	At least Microsoft Windows XP Professional or Windows Server 2003 family	This settings controls whether the thumbnail views are cached. If you enable this setting, thumbnail views are not cached. If you disable or do not configure this setting, thumbnail views are cached. Note: For shared corporate workstations or computers where security is a top concern, you should enable this setting to turn off the thumbnail view cache, because the thumbnail cache can be read by everyone.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove CD Burning features	At least Microsoft Windows XP Professional or Windows Server 2003 family	Windows Explorer allows you to create and modify re-writable CDs if you have a CD writer connected to your PC. If you enable this setting, all features in the Windows Explorer that allow you to use your CD writer are removed. If you disable or do not configure this setting, users are able to use the Windows Explorer CD burning features. Note: This setting does not prevent users from using third-party applications to create or modify CDs using a CD writer.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove UI to change menu animation setting	At least Microsoft Windows 2000	Prevents users from selecting the option to animate the movement of windows, menus, and lists. If you enable this setting, the Use transition effects for menus and tooltips option in Display in Control Panel is disabled. Effects, such as animation, are designed to enhance the user's experience but might be confusing or distracting to some users.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove UI to change keyboard navigation indicator setting	At least Microsoft Windows 2000	Disables the Hide keyboard navigation indicators until I use the ALT key option in Display in Control Panel. When this Display Properties option is selected, the underlining that indicates a keyboard shortcut character (hot key) does not appear on menus until you press ALT. Effects, such as transitory underlines, are designed to enhance the user's experience but might be confusing or distracting to some users.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove DFS tab	At least Microsoft Windows 2000	Removes the DFS tab from Windows Explorer. This setting removes the DFS tab from Windows Explorer and from other programs that use the Windows Explorer browser, such as My Computer. As a result, users cannot use this tab to view or change the properties of the Distributed File System (DFS) shares available from their computer. This setting

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				does not prevent users from using other methods to configure DFS.
USER	Administrative Templates\Windows Components\Windows Explorer	Hide these specified drives in My Computer	At least Microsoft Windows 2000	Removes the icons representing selected hard drives from My Computer and Windows Explorer. Also, the drive letters representing the selected drives do not appear in the standard Open dialog box. To use this setting, select a drive or combination of drives in the drop-down list. To display all drives, disable this setting or select the Do not restrict drives option in the drop-down list. Note: This setting removes the drive icons. Users can still gain access to drive contents by using other methods, such as by typing the path to a directory on the drive in the Map Network Drive dialog box, in the Run dialog box, or in a command window. Also, this setting does not prevent users from using programs to access these drives or their contents. And, it does not prevent users from using the Disk Management snap-in to view and change drive characteristics. Also, see the Prevent access to drives from My Computer setting. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
USER	Administrative Templates\Windows Components\Windows Explorer	No Entire Network in My Network Places	At least Microsoft Windows 2000	Removes all computers outside of the user's workgroup or local domain from lists of network resources in Windows Explorer and My Network Places. If you enable this setting, the system removes the Entire Network option and the icons representing networked computers from My Network Places and from the browser associated with the Map Network Drive option. This setting does not prevent users from viewing or connecting to computers in their workgroup or domain. It also does not prevent users from connecting to remote computers by other commonly used methods, such as by typing the share name in the Run dialog box or the Map Network Drive dialog box. To remove computers in the user's workgroup or domain from lists of network resources, use the No Computers Near Me in My Network Places setting. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove File menu from Windows Explorer	At least Microsoft Windows 2000	Removes the File menu from My Computer and Windows Explorer. This setting does not prevent users from using other methods to perform tasks available on the File menu.
USER	Administrative Templates\Windows Components\Windows Explorer	Removes the Folder Options menu item from the Tools menu	At least Microsoft Windows 2000	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. The Folder Options dialog box lets users set many properties of Windows Explorer, such as Active Desktop, Web view, Offline Files, hidden system files, and file types.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Also, see the Enable Active Desktop setting in User Configuration\AdministrativeTemplates\Desktop\Active Desktop and the Prohibit user configuration of Offline Files setting in User Configuration\Administrative Templates\Network\Offline Files.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove Hardware tab	At least Microsoft Windows 2000	Removes the Hardware tab. This setting 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. As a result, users cannot use the Hardware tab to view or change the device list or device properties, or use the Troubleshoot button to resolve problems with the device.
USER	Administrative Templates\Windows Components\Windows Explorer	Hides the Manage item on the Windows Explorer context menu	At least Microsoft Windows 2000	Removes the Manage item from the Windows Explorer context menu. This context menu appears when you right-click Windows Explorer or My Computer. The Manage item opens Computer Management (Compmgmt.msc), a console tool that includes many of the primary Windows 2000 administrative tools, such as Event Viewer, Device Manager, and Disk Management. You must be an administrator to use many of the features of these tools. This setting does not remove the Computer Management item from the Start menu (Start, Programs, Administrative Tools, Computer Management), nor does it prevent users from using other methods to start Computer Management. Tip: To hide all context menus, use the Remove Windows Explorer's default context menu setting.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove Shared Documents from My Computer	Only works on Microsoft Windows XP Professional	Removes the Shared Documents folder from My Computer. When a Windows client in is a workgroup, a Shared Documents icon appears in the Windows Explorer Web view under Other Places and also under Files Stored on This Computer in My Computer. Using this policy setting, you can choose not to have these items displayed. If you enable this setting, the Shared Documents folder is not displayed in the Web view or in My Computer. If you disable or do not configure this setting, the Shared Documents folder is displayed in Web view and also in My Computer when the client is part of a workgroup. Note: The ability to remove the Shared Documents folder via Group Policy is only available on Windows XP Professional.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove Map Network Drive and Disconnect Network Drive	At least Microsoft Windows 2000	Prevents users from using Windows Explorer or My Network Places to map or disconnect network drives. If you enable this setting, the system removes the Map Network Drive and Disconnect Network Drive commands from the toolbar and Tools menus in Windows Explorer and

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				My Network Places and from menus that appear when you right-click the Windows Explorer or My Network Places icons. It also removes the Add Network Place option from My Network Places. This setting does not prevent users from connecting to another computer by typing the name of a shared folder in the Run dialog box. Note: This setting was documented incorrectly on the Explain tab in Group Policy for Windows 2000. The Explain tab states incorrectly that this setting prevents users from connecting and disconnecting drives. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
USER	Administrative Templates\Windows Components\Windows Explorer	Do not move deleted files to the Recycle Bin	At least Microsoft Windows XP Professional or Windows Server 2003 family	When a file or folder is deleted in Windows Explorer, a copy of the file or folder is placed in the Recycle Bin. Using this setting, you can change this behavior. If you enable this setting, files and folders that are deleted using Windows Explorer will not be placed in the Recycle Bin and will therefore be permanently deleted. If you disable or do not configure this setting, files and folders deleted using Windows Explorer will be placed in the Recyele Bin.
USER	Administrative Templates\Windows Components\Windows Explorer	Do not request alternate credentials	At least Microsoft Windows 2000	Prevents users from submitting alternate logon credentials to install a program. This setting suppresses the Install Program As Other User dialog box for local and network installations. This dialog box, which prompts the current user for the user name and password of an administrator, appears when users who are not administrators try to install programs locally on their computers. This setting allows administrators who have logged on as regular users to install programs without logging off and logging on again using their administrator credentials. Many programs can be installed only by an administrator. If you enable this setting and a user does not have sufficient permissions to install a program, the installation continues with the current user's logon credentials. As a result, the installation might fail, or it might complete but not include all features. Or, it might appear to complete successfully, but the installed program might not operate correctly. If you disable this setting or do not configure it, the Install Program As Other User dialog box appears whenever users install programs locally on the computer. By default, users are not prompted for alternate logon credentials when installing programs from a network share. If enabled, this setting overrides the Request credentials for network installations setting.
USER	Administrative Templates\Windows	Remove Security tab	At least Microsoft	Removes the Security tab from Windows Explorer. If you enable this

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Windows Explorer		Windows XP Professional or Windows Server 2003 family	setting, users opening the Properties dialog box for all file system objects, including folders, files, shortcuts, and drives, will not be able to access the Security tab. As a result, users will be able to neither change the security settings nor view a list of all users that have access to the resource in question. If you disable or do not configure this setting, users will be able to access the security tab.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove Search button from Windows Explorer	At least Microsoft Windows 2000	Removes the Search button from the Windows Explorer toolbar. This setting removes the Search button from the Standard Buttons toolbar that appears in Windows Explorer and other programs that use the Windows Explorer window, such as My Computer and My Network Places. It does not remove the Search button or affect any search features of Internet browser windows, such as the Internet Explorer window. This setting does not affect the Search items on the Windows Explorer context menu or on the Start menu. To remove Search from the Start menu, use the Remove Search menu from Start menu setting (in User Configuration\Administrative Templates\Start Menu and Taskbar). To hide all context menus, use the Remove Windows Explorer's default context menu setting.
USER	Administrative Templates\Windows Components\Windows Explorer	Remove Windows Explorer's default context menu	At least Microsoft Windows 2000	Removes shortcut menus from the desktop and Windows Explorer. Shortcut menus appear when you right-click an item. If you enable this setting, menus do not appear when you right-click the desktop or when you right-click the items in Windows Explorer. This setting does not prevent users from using other methods to issue commands available on the shortcut menus.
USER	Administrative Templates\Windows Components\Windows Explorer	Prevent access to drives from My Computer	At least Microsoft Windows 2000	Prevents users from using My Computer to gain access to the content of selected drives. If you enable this setting, users can browse the directory structure of the selected drives in My Computer or Windows Explorer, but they cannot open folders and access the contents. Also, they cannot use the Run dialog box or the Map Network Drive dialog box to view the directories on these drives. To use this setting, select a drive or combination of drives from the drop-down list. To allow access to all drive directories, disable this setting or select the Do not restrict drives option from the drop-down list. Note: The icons representing the specified drives still appear in My Computer, but if users double-click the icons, a message appears explaining that a setting prevents the action. Also, this setting does not prevent users from using programs to access local and network drives. And, it does not prevent them from using the Disk Management snap-in to view and change drive characteristics.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Also, see the Hide these specified drives in My Computer setting.
USER	Administrative Templates\Windows Components\Windows Explorer	Turn off Windows+X hotkeys	At least Microsoft Windows Server 2003	Turn off Windows+X hotkeys. Keyboards with a Windows key provide users with shortcuts to common shell features. For example, pressing the keyboard sequence Windows+R opens the Run dialog box; pressing Windows+E starts Windows Explorer. By using this setting, you can disable these Windows+X shortcut keys. If you enable this setting, the Windows+X shortcut keys are unavailable. If you disable or do not configure this setting, the Windows+X shortcut keys are available.
USER	Administrative Templates\Windows Components\Windows Explorer	No Computers Near Me in My Network Places	At least Microsoft Windows 2000	Removes computers in the user's workgroup and domain from lists of network resources in Windows Explorer and My Network Places. If you enable this setting, the system removes the Computers Near Me option and the icons representing nearby computers from My Network Places. This setting also removes these icons from the Map Network Drive browser. This setting does not prevent users from connecting to computers in their workgroup or domain by other commonly used methods, such as typing the share name in the Run dialog box or the Map Network Drive dialog box. To remove network computers from lists of network resources, use the No Entire Network in My Network Places setting.
USER	Administrative Templates\Windows Components\Windows Explorer	Request credentials for network installations	At least Microsoft Windows 2000	Prompts users for alternate logon credentials during network-based installations. This setting displays the Install Program As Other User dialog box even when a program is being installed from files on a network computer across a local area network connection. If you disable this setting or do not configure it, this dialog box appears only when users are installing programs from local media. The Install Program as Other User dialog box prompts the current user for the user name and password of an administrator. This setting allows administrators who have logged on as regular users to install programs without logging off and logging on again using their administrator credentials. If the dialog box does not appear, the installation proceeds with the current user's permissions. If these permissions are not sufficient, the installation might fail, or it might complete but not include all features. Or, it might appear to complete successfully, but the installed program might not operate correctly. Note: If it is enabled, the Do not request alternate credentials setting takes precedence over this setting. When that setting is enabled, users are not prompted for alternate logon credentials on any installation.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Windows Explorer	Maximum allowed Recycle Bin size	At least Microsoft Windows XP Professional or Windows Server 2003 family	Limits the percentage of a volume's disk space that can be used to store deleted files. If you enable this setting, the user has a maximum amount of disk space that may be used for the Recycle Bin on their workstation. If you disable or do not configure this setting, users can change the total amount of disk space used by the Recycle Bin. Note: This setting is applied to all volumes.
USER	Administrative Templates\Windows Components\Windows Explorer\Common Open File Dialog	Hide the common dialog back button	At least Microsoft Windows 2000	Removes the Back button from the Open dialog box. This setting, and others in this folder, lets you remove new features added in Windows 2000 Professional, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs. To see an example of the standard Open dialog box, run Notepad and, on the File menu, click Open. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
USER	Administrative Templates\Windows Components\Windows Explorer\Common Open File Dialog	Hide the dropdown list of recent files	At least Microsoft Windows 2000	Removes the list of most recently used files from the Open dialog box. If you disable this setting or do not configure it, the File name field includes a drop-down list of recently used files. If you enable this setting, the File name field is a simple text box. Users must browse directories to find a file or type a file name in the text box. This setting, and others in this folder, lets you remove new features added in Windows 2000 Professional, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs. To see an example of the standard Open dialog box, start Notepad and, on the File menu, click Open. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
USER	Administrative Templates\Windows Components\Windows Explorer\Common Open File Dialog	Hide the common dialog places bar	At least Microsoft Windows 2000	Removes the shortcut bar from the Open dialog box. This setting, and others in this folder, lets you remove new features added in Windows 2000 Professional, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs. To see an example of the standard Open dialog box, start Notepad and, on the File menu, click Open. Note: It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Windows Explorer\Common Open File Dialog	Items displayed in Places Bar	At least Microsoft Windows XP Professional or Windows Server 2003 family	Configures the list of items displayed in the Places Bar in the Windows File/Open dialog. If enable this setting you can specify from 1 to 5 items to be displayed in the Places Bar. The valid items you may display in the Places Bar are: 1) Shortcuts to a local folders -- (ex. C:\Windows) 2) Shortcuts to remote folders -- (\\server\share) 3) Common Shell folders. The list of Common Shell Folders that may be specified: CommonDocuments, CommonMusic, CommonPictures, Desktop, MyComputer, MyDocuments, MyFavorites, MyMusic, MyNetworkPlaces, MyPictures, Printers, ProgramFiles, Recent. If you disable or do not configure this setting the default list of items will be displayed in the Places Bar.
USER	Administrative Templates\Windows Components\Windows Installer	Always install with elevated privileges	At least Microsoft Windows 2000	Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer. Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure.
USER	Administrative Templates\Windows Components\Windows Installer	Prevent removable media source for any install	At least Microsoft Windows 2000	Prevents users from installing programs from removable media. If a user tries to install a program from removable media, such as CD-ROMs, floppy disks, and DVDs, a message appears, stating that the feature cannot be found. This setting applies even when the installation is running in the user's security context. If you disable this setting or do not configure it, users can install from removable media when the installation is running in their own security context, but only system administrators can use removable media when an installation is running with elevated system privileges, such as installations offered on the desktop or in Add or Remove Programs. Also, see the Enable user to use media source while elevated setting in Computer Configuration\Administrative

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				Templates\Windows Components\Windows Installer. Also, see the Hide the 'Add a program from CD-ROM or floppy disk' option setting in User Configuration\Administrative Templates\Control Panel\Add or Remove Programs.
USER	Administrative Templates\Windows Components\Windows Installer	Prohibit rollback	At least Microsoft Windows 2000	Prohibits Windows Installer from generating and saving the files it needs to reverse an interrupted or unsuccessful installation. This setting prevents Windows Installer from recording the original state of the system and sequence of changes it makes during installation. It also prevents Windows Installer from retaining files it intends to delete later. As a result, Windows Installer cannot restore the computer to its original state if the installation does not complete. This setting is designed to reduce the amount of temporary disk space required to install programs. Also, it prevents malicious users from interrupting an installation to gather data about the internal state of the computer or to search secure system files. However, because an incomplete installation can render the system or a program inoperable, do not use this setting unless it is essential. This setting appears in the Computer Configuration and User Configuration folders. If the setting is enabled in either folder, it is considered be enabled, even if it is explicitly disabled in the other folder.
USER	Administrative Templates\Windows Components\Windows Installer	Search order	At least Microsoft Windows 2000	Specifies the order in which Windows Installer searches for installation files. By default, the Windows Installer searches the network first, then removable media (floppy drive, CD-ROM, or DVD), and finally, the Internet (URL). To change the search order, enable the setting, and then type the letters representing each file source in the order that you want Windows Installer to search.: -- n represents the network; -- m represents media; -- u represents URL, or the Internet. To exclude a file source, omit or delete the letter representing that source type.
USER	Administrative Templates\Windows Components\Windows Media Player	Prevent CD and DVD Media Information Retrieval	Windows Media Player 9 Series and later.	Prevents media information for CDs and DVDs from being retrieved from the Internet. This policy prevents the Player from automatically obtaining media information from the Internet for CDs and DVDs played by users. In addition, the Retrieve media information for CDs and DVDs from the Internet check box on the Privacy Options tab in the first use dialog box and on the Privacy tab in the Player are not selected and are not available. When this policy is not configured or disabled, users can change the setting of the Retrieve media information for CDs and DVDs from the Internet check box.
USER	Administrative Templates\Windows	Prevent Music File Media Information	Windows Media Player 9 Series and	Prevents media information for music files from being retrieved from the Internet. This policy prevents the Player from automatically obtaining

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	Components\Windows Media Player	Retrieval	later.	media information for music files such as Windows Media Audio (WMA) and MP3 files from the Internet. In addition, the Update my music files (WMA and MP3 files) by retrieving missing media information from the Internet check box in the first use dialog box and on the Privacy and Media Library tabs in the Player are not selected and are not available. When this policy is not configured or disabled, users can change the setting of the Update my music files (WMA and MP3 files) by retrieving missing media information from the Internet check box.
USER	Administrative Templates\Windows Components\Windows Media Player	Prevent Radio Station Preset Retrieval	Windows Media Player 9 Series and later.	Prevents radio station presets from being retrieved from the Internet. This policy prevents the Player from automatically retrieving radio station presets from the Internet and displaying them in Media Library. In addition, presets that exist before the policy is configured will not be updated, and presets a user adds will not be displayed. When this policy is not configured or disabled, the Player automatically retrieves radio station presets from the Internet.
USER	Administrative Templates\Windows Components\Windows Media Player\Networking	Configure HTTP Proxy	Windows Media Player for Windows XP and later.	Specifies the HTTP proxy settings for Windows Media Player. This policy specifies the proxy settings for the HTTP protocol. When this policy is enabled, a proxy type (Autodetect, Custom, or Use browser proxy settings) must be selected. Autodetect means that the proxy settings are automatically detected. Custom means that unique proxy settings are used. Use browser proxy settings means that the proxy settings of the browser are used. If the Custom proxy type is selected, the rest of the options on the Setting tab must be specified because no default settings are used for the proxy. The options are ignored if Autodetect or Browser is selected. The Configure button on the Network tab in the Player is not available for the HTTP protocol and the proxy cannot be configured. If the Hide Network Tab policy is also enabled, the entire Network tab is hidden. This policy is ignored if the Streaming Media Protocols policy is enabled and HTTP is not selected. When this policy is disabled, the HTTP proxy server cannot be used and the user cannot configure the HTTP proxy. When this policy is not configured, users can configure the HTTP proxy settings.
USER	Administrative Templates\Windows Components\Windows Media Player\Networking	Configure MMS Proxy	Windows Media Player for Windows XP and later.	Specifies the MMS proxy settings for Windows Media Player. This policy specifies the proxy settings for the MMS protocol. When this policy is enabled, a proxy type (Autodetect or Custom) must be selected. Autodetect means that the proxy settings are automatically detected. Custom means that unique proxy settings are used. If the Custom proxy type is selected, the rest of the options on the Setting tab must be

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				specified; otherwise, the default settings are used. The options are ignored if Autodetect is selected. The Configure button on the Network tab in the Player is not available and the protocol cannot be configured. If the Hide Network Tab policy is also enabled, the entire Network tab is hidden. This policy is ignored if the Streaming Media Protocols policy is enabled and Multicast is not selected. When this policy is disabled, the MMS proxy server cannot be used and users cannot configure the MMS proxy settings. When this policy is not configured, users can configure the MMS proxy settings.
USER	Administrative Templates\Windows Components\Windows Media Player\Networking	Configure RTSP Proxy	Windows Media Player 9 Series and later.	Specifies the RTSP proxy settings for Windows Media Player. This policy specifies the proxy settings for the RTSP protocol. When this policy is enabled, a proxy type (Autodetect or Custom) must be selected. Autodetect means that the proxy settings are automatically detected. Custom means that unique proxy settings are used. If the Custom proxy type is selected, the rest of the options on the Setting tab must be specified; otherwise, the default settings are used. The options are ignored if Autodetect is selected. The Configure button on the Network tab in the Player is not available and the protocol cannot be configured. If the Hide Network Tab policy is also enabled, the entire Network tab is hidden. When this policy is disabled, the RTSP proxy server cannot be used and users cannot change the RTSP proxy settings. When this policy is not configured, users can configure the RTSP proxy settings.
USER	Administrative Templates\Windows Components\Windows Media Player\Networking	Hide Network Tab	Windows Media Player for Windows XP and later.	Hides the Network tab. This policy hides the Network tab in Windows Media Player. The default network settings are used unless the user has previously defined network settings for the Player. When this policy is not configured or disabled, the Network tab appears and users can use it to configure network settings.
USER	Administrative Templates\Windows Components\Windows Media Player\Networking	Configure Network Buffering	Windows Media Player for Windows XP and later.	Specifies whether network buffering uses the default or a specified number of seconds. This policy specifies that the default network buffering is used or specifies the number of seconds streaming media is buffered before it is played. If Custom is selected on the Setting tab, the number of seconds, up to 60, that streaming media is buffered, must be specified. If Default is selected, the default is used and the number of seconds that is specified is ignored. The Use default buffering and Buffer options on the Performance tab in the Player are not available. When this policy is not configured or disabled, users can change the buffering options on the Performance tab.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Windows Media Player\Networking	Streaming Media Protocols	Windows Media Player for Windows XP and later.	Specifies that the selected protocols are used when receiving streaming media from a server running Windows Media Services. This policy specifies that the protocols selected on the Setting tab can be used to receive streaming media from a Windows Media server. This policy also specifies that multicast streams can be received if the Multicast check box on the Setting tab is selected. If the UDP check box is selected on the Setting tab and the UDP Ports box is blank, Windows Media Player uses default ports when playing content from a Windows Media server. If the UDP check box is not selected, the information in the UDP Ports box is ignored. If none of the protocols are selected when this policy is enabled, content from a Windows Media server cannot be played. When this policy is enabled or disabled, the Streaming protocols area of the Network tab in the Player is not available. If the Hide Network Tab policy is enabled, the entire Network tab is hidden. If this policy is disabled, the Player cannot receive streaming media from a Windows Media Server. If it is necessary to control the kind of streaming media that is received, it is recommended that other methods, such as firewalls, be used. If this policy is not configured and the Hide Network Tab policy is not enabled, users can change the settings in the Streaming protocols section of the Network tab.
USER	Administrative Templates\Windows Components\Windows Media Player\Playback	Allow Screen Saver	Windows Media Player 9 Series and later.	Enables a screen saver to interrupt playback. This policy displays a screen saver during playback of digital media according to the options selected on the Screen Saver tab in the Display Properties dialog box in Control Panel. The Allow screen saver during playback check box on the Player tab in the Player is selected and is not available. When this policy is disabled, a screen saver does not interrupt playback even if users have selected a screen saver. The Allow screen saver during playback check box is cleared and is not available. When this policy is not configured, users can change the setting for the Allow screen saver during playback check box.
USER	Administrative Templates\Windows Components\Windows Media Player\Playback	Prevent Codec Download	Windows Media Player for Windows XP and later.	Prevents Windows Media Player from downloading codecs. This policy prevents the Player from automatically downloading codecs to your computer. In addition, the Download codecs automatically check box on the Player tab in the Player is not available. When this policy is disabled, codecs are automatically downloaded and the Download codecs automatically check box is not available. When this policy is not configured, users can change the setting for the Download codecs automatically check box.

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows Components\Windows Media Player\User Interface	Do Not Show Anchor	Windows Media Player for Windows XP and later.	Prevents the anchor window from being displayed when Windows Media Player is in skin mode. This policy hides the anchor window when the Player is in skin mode. In addition, the option on the Player tab in the Player that enables users to choose whether the anchor window displays is not available. When this policy is not configured or disabled, users can show or hide the anchor window when the Player is in skin mode by using the Player tab in the Player. When this policy is not configured and the Set and Lock Skin policy is enabled, some options in the anchor window are not available.
USER	Administrative Templates\Windows Components\Windows Media Player\User Interface	Hide Privacy Tab	Windows Media Player 9 Series and later.	Hides the Privacy tab. This policy hides the Privacy tab in Windows Media Player. The default privacy settings are used for the options on the Privacy tab unless the user changed the settings previously. The Update my music files (WMA and MP3 files) by retrieving missing media information from the Internet check box is on the Privacy and Media Library tabs. When this policy is enabled, the Update my music files (WMA and MP3 files) by retrieving missing media information from the Internet check box on the Media Library tab is available, even though the Privacy tab is hidden, unless the Prevent Music File Media Information Retrieval policy is enabled. When this policy is not configured or disabled, the Privacy tab is not hidden, and users can configure any privacy settings not configured by other polices.
USER	Administrative Templates\Windows Components\Windows Media Player\User Interface	Hide Security Tab	Windows Media Player 9 Series and later.	Hides the Security tab. This policy hides the Security tab in Windows Media Player. The default security settings for the options on the Security tab are used unless the user changed the settings previously. Even though this policy is enabled, users can still change security and zone settings by using Internet Explorer unless these settings have been hidden or disabled by Internet Explorer policies. When this policy is not configured or disabled, users can configure the security settings on the Security tab.
USER	Administrative Templates\Windows Components\Windows Media Player\User Interface	Set and Lock Skin	Windows Media Player for Windows XP and later.	Enables Windows Media Player to be shown only in skin mode, using a specified skin. This policy displays the Player only in skin mode by using the skin specified in the Skin box on the Setting tab. You must use the complete file name for the skin (for example, skin_name.wmz), and the skin must be installed in the %programfiles%\Windows Media Player\Skins Folder on a user's computer. If the skin is not installed on a user's computer, or if the Skin box is blank, the Player opens by using the Corporate skin. The only way to specify the Corporate skin is to leave the skin box blank. A user has access only to the Player features

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				that are available with the specified skin. Users cannot switch the Player to full mode and cannot choose a different skin. When this policy is not configured or disabled, users can display the Player in full or skin mode and have access to all available features of the Player.
USER	Administrative Templates\Windows Components\Windows Messenger	Do not automatically start Windows Messenger initially	At least Microsoft Windows XP Professional or Windows Server 2003 family	Windows Messenger is automatically loaded and running when a user logs on to a Windows XP computer. You can use this setting to stop Windows Messenger from automatically being run at logon. If you enable this setting, Windows Messenger will not be loaded automatically when a user logs on. If you disable or do not configure this setting, the Windows Messenger will be loaded automatically at logon. Note: This setting simply prevents Windows Messenger from running intially. If the user invokes and uses Windows Messenger from that point on, Windows Messenger will be loaded. The user can also configure this behavior on the Preferences tab on the Tools menu in the Windows Messenger user interface. Note: If you do not want users to use Windows Messenger, enable the Do not allow Windows Messenger to run setting. Note: This setting is available under both Computer Configuration and User Configuration. If both are present, the Computer Configuration version of this setting takes precedence.
USER	Administrative Templates\Windows Components\Windows Messenger	Do not allow Windows Messenger to be run	At least Microsoft Windows XP Professional or Windows Server 2003 family	Allows you to disable Windows Messenger. If you enable this setting, Windows Messenger will not run. If you disable or do not configure this setting, Windows Messenger can be used. Note: If you enable this setting, Remote Assistance also cannot use Windows Messenger. Note: This setting is available under both Computer Configuration and User Configuration. If both are present, the Computer Configuration version of this setting takes precedence.
USER	Administrative Templates\Windows Components\Windows Movie Maker	Do not allow Windows Movie Maker to run	At least Microsoft Windows XP Professional with SP2	Specifies whether Windows Movie Maker can run. Windows Movie Maker is a feature of the Windows XP operating system that can be used to capture, edit, and then save video as a movie to share with others. If you enable this setting, Windows Movie Maker will not run. If you disable or do not configure this setting, Windows Movie Maker can be run.
USER	Administrative Templates\Windows Components\Windows Update	Remove access to use all Windows Update features	At least Microsoft Windows XP Professional or Windows Server 2003 family	This setting allows you to remove access to Windows Update. If you enable this setting, all Windows Update features are removed. This includes blocking access to the Windows Update Web site at http://windowsupdate.microsoft.com, 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 will neither be notified

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
				about nor will you receive critical updates from Windows Update. This setting also prevents Device Manager from automatically installing driver updates from the Windows Update Web site.
USER	Administrative Templates\Windows NT Shell\Custom folders	Custom desktop icons		
USER	Administrative Templates\Windows NT Shell\Custom folders	Custom Network Neighborhood		
USER	Administrative Templates\Windows NT Shell\Custom folders	Custom Programs folder		
USER	Administrative Templates\Windows NT Shell\Custom folders	Custom Start menu		
USER	Administrative Templates\Windows NT Shell\Custom folders	Custom Startup folder		
USER	Administrative Templates\Windows NT Shell\Custom folders	Hide Start menu subfolders		
USER	Administrative Templates\Windows NT Shell\Custom user interface	Custom shell		
USER	Administrative Templates\Windows NT Shell\Restrictions	Only use approved shell extensions		
USER	Administrative Templates\Windows NT Shell\Restrictions	Disable link file tracking		
USER	Administrative Templates\Windows NT Shell\Restrictions	Remove common program groups from Start menu		
USER	Administrative Templates\Windows NT Shell\Restrictions	Remove Disconnect item from Start menu		
USER	Administrative Templates\Windows NT Shell\Restrictions	Prevent user from changing file type associations		
USER	Administrative Templates\Windows NT Shell\Restrictions	Remove File menu from Explorer		

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
USER	Administrative Templates\Windows NT Shell\Restrictions	Remove Tools->GoTo menu from Explorer		
USER	Administrative Templates\Windows NT Shell\Restrictions	Remove the Map Network Drive and Disconnect Network Drive options		
USER	Administrative Templates\Windows NT Shell\Restrictions	Remove NT Security item from Start menu		
USER	Administrative Templates\Windows NT Shell\Restrictions	Remove View->Options menu from Explorer		
USER	Administrative Templates\Windows NT Shell\Restrictions	Disable context menus for the taskbar		
USER	Administrative Templates\Windows NT Shell\Restrictions	Disable Explorer's default context menu		
USER	Administrative Templates\Windows NT System	Disable Change Password		
USER	Administrative Templates\Windows NT System	Disable Lock Workstation		
USER	Administrative Templates\Windows NT System	Disable Logoff		
USER	Administrative Templates\Windows NT System	Disable Task Manager		
USER	Administrative Templates\Windows NT System	Parse Autoexec.bat		
USER	Administrative Templates\Windows NT System	Run logon scripts synchronously.		
USER	Administrative Templates\Windows NT System	Show welcome tips at logon		
USER	Administrative Templates\Windows NT User Profiles	Exclude directories in roaming profile		
USER	Administrative Templates\Windows	Limit profile size		

Node	Policy Path	Full Policy Name	Supported on	Help/Explain Text
	NT User Profiles			