William Stanek's Training Seminars

Windows Vista

Group Policy

Administrator

Reference

Windows Vista Group Policy Administrator Reference for Administrative Templates

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

For policy node:

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

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Accessories	Do not allow Inkball to run	At least Windows Vista or later	Prevents start of InkBall game. If you enable this policy, the InkBall game will not run. If you disable this policy, the InkBall game will run. If you do not configure this policy, the InkBall game will run.
Computer/User	Accessories	Do not allow printing to Journal Note Writer	At least Windows Vista or later	Prevents printing to Journal Note Writer. If you enable this policy, the Journal Note Writer printer driver will not allow printing to it. It will remain displayed in the list of available printers, but attempts to print to it will fail. If you disable this policy, you will be able to use this feature to print to a Journal Note. If you do not configure this policy, users will be able to use this feature to print to a Journal Note.
Computer/User	Accessories	Do not allow Snipping Tool to run	At least Windows Vista or later	Prevents the snipping tool from running. If you enable this policy setting, the Snipping Tool will not run. If you disable this policy setting, the Snipping Tool will run. If you do not configure this policy setting, the Snipping Tool will run.
Computer/User	Accessories	Do not allow Sticky Notes to be run	At least Windows Vista or later	Prevents start of Sticky Notes. If you enable this policy, the Sticky Notes accessory will not run. If you disable this policy, the Sticky Notes accessory will run. If you do not configure this policy, the Sticky Notes accessory will run.
Computer/User	Accessories	Do not allow Windows Journal to be run	At least Windows Vista or later	Prevents start of Windows Journal. If you enable this policy, the Windows Journal accessory will not run. If you disable this policy, the Windows Journal accessory will run. If you do not configure this policy, the Windows Journal accessory will run.
Computer	ActiveX Installer Service	Approved Installation Sites for ActiveX Controls	At least Windows Vista or later	The ActiveX Installer Service is the solution to delegate the install of per-machine ActiveX controls to a Standard User in the enterprise. The list of Approved ActiveX Install sites contains the host URL and the policy settings for each host URL. Wild cards are not supported.
Computer	Advanced Error	Configure Corporate Windows	At least Windows	This setting determines the corporate server to which Windows Error Reporting will send

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Reporting Settings	Error Reporting	Vista or later	reports (instead of sending reports to Microsoft). Server port indicates the port to use on the target server. Connect using SSL determines whether Windows will send reports to the server using a secured connection.
Computer/User	Advanced Error Reporting Settings	Configure Report Archive	At least Windows Vista or later	This setting controls the behavior of the Windows Error Reporting archive. If Archive behavior is set to "Store all", all data collected for each report will be stored in the appropriate location. If Archive behavior is set to "Store parameters only", only the minimum information required to check for an existing solution will be stored. The setting for "Maximum number of reports to store" determines how many reports can be stored before old reports are automatically deleted. If this setting is disabled, no Windows Error Reporting information will be stored.
Computer/User	Advanced Error Reporting Settings	Configure Report Queue	At least Windows Vista or later	This setting determines the behavior of the Windows Error Reporting queue. If Queuing behavior is set to "Default", Windows will decide each time a problem occurs whether the report should be queued or the user should be prompted to send it immediately. If Queuing behavior is set to "Always queue", all reports will be queued until the user is notified to send them or until the user chooses to send them using the Solutions to Problems control panel. If Queuing behavior is set to "Always queue for administrator", reports will be queued until an administrator is notified to send them or chooses to send them using the Solutions to Problems control panel. The setting for "Maximum number of reports to queue" determines how many reports can be queued before old reports are automatically deleted. The setting for "Number of days between solution check reminders" determines the interval time between the display of system notifications which remind the user to check for solutions to problems. A setting of 0 will disable the reminder. If the Windows Error Reporting queue setting is disabled, no Windows Error Reporting information will be queued and users will be

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				able to send reports only at the time a problem occurs.
Computer/User	Advanced Error Reporting Settings	List of applications to be excluded	At least Windows Vista or later	This setting determines the behavior of the error reporting exclusion list. Windows will not send reports for any process added to this list. Click "Show" to display the exclusion list. Click "Add..." and type a process name to add a process to the list. Select a process name and click "Remove" to remove a process from the list. Click "OK" to save the list.
Computer	Application, Security, Setup, System	Backup log automatically when full	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size and takes effect only if the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled. If you enable this policy setting and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, the Event Log file is automatically closed and renamed when it is full. A new file is then started. If you disable this policy setting and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, then new events are discarded and the old events are retained. When this policy setting is not configured and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, new events are discarded and the old events are retained.
Computer	Application, Security, Setup, System	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer/User	Application Compatibility	Turn Off Program Compatibility Assistant	At least Windows Vista or later	This policy controls the state of the Program Compatibility Assistant in the system. The PCA monitors user initiated programs for known compatibility issues at run time. Whenever a potential issue with an application is detected, the PCA will prompt the user with pointers to recommended solutions. For more information on the various issue detection scenarios covered by PCA and the policies to configure them, refer to policies under System-

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				&gt;Troubleshooting and Diagnostics-&gt;Application Compatibility Diagnostics. The PCA is on by default. If you enable this policy setting, the PCA will be turned off. This option is useful for system administrators who require faster performance and are aware of the compatibility of the applications they are using. Note: With the PCA turned off, the user will not be presented with solutions to known compatibility issues when running applications. If you disable or do not configure this policy setting, the PCA will be turned on. Note: The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect application failures caused by deprecated Windows DLLs or COM objects	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose DLL load or COM object creation failures in programs. If you enable this policy setting, the PCA detects programs trying load legacy Microsoft Windows DLLs or creating legacy COM objects that are removed in this version of Windows. When this failure is detected, after the program is terminated, PCA will notify the user about this problem and provide an option to check the Microsoft Web site for solutions. If you disable this policy setting, the PCA does not detect programs trying to load legacy Windows DLLs or creating legacy COM objects. If you do not configure this policy setting, the PCA detects programs trying to load legacy Windows DLLs or creating legacy COM objects. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility	Detect application install failures	At least Windows	This policy setting configures the Program Compatibility Assistant (PCA) to diagnose

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Diagnostics		Vista or later	failures with application installations. If you enable this policy setting, the PCA is configured to detect failures in the execution of application installers through heuristics. When potential failures are detected, the PCA will provide the user with an option to restart the installer with Microsoft Windows XP compatibility mode. If you disable this policy setting, the PCA is not configured to detect failures in execution of program installers. If you do not configure this policy setting, the PCA will enable this diagnostic scenario by default. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect application installers that need to be run as administrator	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose failures with application installers that are not detected to run as administrator. If you enable this policy setting, the PCA is configured to detect application installers which do not have privileges to run as administrator by the User Access Control (UAC). When potential failures are detected, the PCA will provide the user with an option to restart the installer as administrator. If you disable this policy setting, the PCA will not detect application installers which do not have privileges to run as administrator by the UAC. If you do not configure this policy setting, the PCA will be configured to detect application installers which do not have privileges to run as administrator by the UAC. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Application Compatibility Diagnostics	Detect applications unable to launch installers under UAC	At least Windows Vista or later	This policy setting configures the Program Compatibility Assistant (PCA) to diagnose failures with programs under User Account Control (UAC). If you enable this policy setting, the PCA detects programs that failed to launch child processes that are installers (typically updaters). When this failure is detected, the PCA will apply the ELEVATECREATEPROCESS compatibility mode, which enables the program to successfully launch the installer as with administrator privileges the next time the program is run. If you disable this policy setting, the PCA will not detect applications that fail to launch installers run under UAC. If you do not configure this policy setting, the PCA detects programs that failed to launch child processes that are installers (typically updaters). Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Notify blocked drivers	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose drivers blocked due to compatibility issues. If you enable this policy setting, the PCA will notify the user of blocked driver issues with an option to check the Microsoft Web site for solutions. If you disable this policy setting, the PCA will not notify the user of blocked driver issues. Note: With this policy setting in a disabled state, the user will not be presented with solutions to blocked drivers. If you do not configure this policy setting, the PCA will notify the user of blocked driver issues with an option to check the Microsoft Web site for solutions. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application, Security, Setup, System	**Log Access**	At least Windows Vista or later	This policy setting specifies to use the security descriptor for the log using the Security Descriptor Definition Language (SDDL) string. If this policy setting is enabled, only those users matching the security descriptor can access the log. If this policy setting is disabled or not configured, then all authenticated users and system services can write/read/clear this log.
Computer	Application, Security, Setup, System	**Log File Path**	At least Windows Vista or later	This policy setting controls the location of the log file. The location of the file must be writable by the Event Log service and should only be accessible to administrators. If you enable this policy setting, the Event Log uses the specified path provided in this policy setting. If you disable or do not configure this policy setting, the Event Log uses the system32 or system64 subdirectory.
Computer	Application, Security, Setup, System	Maximum Log Size (KB)	At least Windows Vista or later	This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file maximum size will be set to the local configuration value. This value can be changed by the local administrator using the log properties dialog and it defaults to 20 megabytes.
Computer/User	AutoPlay Policies	Default behavior for AutoRun	At least Windows Vista or later	Sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior in

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog. If you enable this policy, an Administrator can change the default Windows Vista behavior for autorun to: A) Completely disable autorun commands, or B) Revert back to Pre-Windows Vista behavior of automatically executing the autorun command. If you disable or not configure this policy, Windows Vista will prompt the user whether autorun command is to be run.
Computer/User	AutoPlay Policies	Don't set the always do this checkbox	At least Windows Vista or later	If this policy is enabled, the "Always do this..." checkbox in Autoplay dialog will not be set by default when the dialog is shown.
Computer	Background Intelligent Transfer Service (BITS)	Allow BITS Peercaching	At least Windows Vista or later	This setting determines if the BITS Peer-caching feature is enabled on a specific computer. By default, the files in a BITS job are downloaded only from the originating server specified by the jobΓÇÖs owner. Each client computer will download its own copy of the files from the origin server. If BITS Peer-caching is enabled, BITS will cache download jobs and make the content available to other BITS peers. When running a download job, BITS will first request the files for the job from one of its peers in the same IP subnet. If none of the peers in the subnet have the requested files, BITS will download the files for the job from the original server. If you enable this setting, BITS will cache jobs, respond to content requests from peers, and download job content from peers if possible. If you disable this setting or do not configure it, the peer-caching feature will be disabled and BITS will download files directly from the original server.
Computer	Background Intelligent Transfer Service (BITS)	Do not allow the computer to act as a BITS Peercaching client	At least Windows Vista or later	This setting specifies whether the computer will act as a BITS peercaching client. By default, when BITS peercaching is enabled, the computer acts as both a peercaching server (offering files to its peers) and a peercaching client (downloading files from its peers). If you enable this setting, the computer will no longer use the BITS Peercaching feature to

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				download files; files will be downloaded only from the origin server. However, the computer will still make files available to its peers. If you disable or do not configure this setting, the computer attempts to download peer enabled BITS jobs from peer computers before reverting to the origin server. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Do not allow the computer to act as a BITS Peercaching server	At least Windows Vista or later	This setting specifies whether the computer will act as a BITS peercaching server. By default, when BITS peercaching is enabled, the computer acts as both a peercaching server (offering files to its peers) and a peercaching client (downloading files from its peers). If you enable this setting, the computer will no longer cache downloaded files and offer them to its peers. However, the computer will still download files from peers. If you disable or do not configure this setting, the computer will offer downloaded and cached files to its peers. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Limit age of items in the BITS Peercache	At least Windows Vista or later	This setting specifies the maximum age of files in the Peercache. In order to make the most efficient use of disk space, by default BITS removes any files in the cache older than 14 days. If you enable this setting, you can specify the maximum age of files in the cache in days. You can enter a value between 1 and 120 Days. If you disable this setting or do not configure it, files older than 14 days will be removed from the Peercache. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Limit the BITS Peercache size	At least Windows Vista or later	This setting specifies the maximum amount of disk space that can be used for the BITS Peercache, as a percentage of the total system disk size. BITS will add files to the Peercache and make those files available to peers until the cache content reaches the specified cache size. By default, BITS will use 1% of the total system disk for the peercache.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				If you enable this setting, you can enter the percentage of disk space to be used for the BITS peercache. You can enter a value between 1% and 80%. If you disable this setting or do not configure it, the default size of the BITS peercache is 1% of the total system disk size. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Maximum BITS job download time	At least Windows Vista or later	This setting limits the amount of time that BITS will take to download the files in a BITS job. The time limit applies only to the time that BITS is actively downloading files, not real-time. When the cumulative download time exceeds this limit, the job is placed in the error state. By default BITS uses a maximum download time of 15 days (54000 seconds). If you enable this setting, you can set the maximum job download time to the specified number of seconds. If you disable or do not configure this setting, the default value of 15 days (54000 seconds) will be used for the maximum job download time.
Computer	Background Intelligent Transfer Service (BITS)	Maximum network bandwidth used for Peercaching	At least Windows Vista or later	This setting limits the network bandwidth that BITS uses for peercache transfers (this setting does not affect transfers from the origin server). To prevent any negative impact to a computer caused by serving other peers, by default BITS will use up to 30% of the bandwidth of the slowest active network interface. For example, if a computer has both a 100Mbps network card, and a 56 Kbps modem, and both are active, BITS will use a maximum of 30% of 56Kbps. You can change the default behavior of BITS, and specify a fixed maximum bandwidth that BITS will use for Peercaching. If you enable this setting, you can enter a value in bits per second (bps) between 1048576 and 4294967200 to use as the maximum network bandwidth used for peer-caching. If you disable this setting or do not configure it, the default value of 30% of the slowest active network interface will be used. Note: This setting has no effect if the ΓÇ£Allow BITS peercachingΓÇ¥ setting is disabled or

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				not configured.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of BITS jobs for each user	At least Windows Vista or later	This setting specifies the maximum number of BITS jobs that can be created by a user. By default, BITS limits the total number of jobs that can be created by a user to 60 jobs. You can use this setting to raise or lower the maximum number of BITS jobs a user can create. If you enable this setting, BITS will limit the maximum number of BITS jobs a user can create to the specified number. If you disable or do not configure this setting, BITS will use the default user BITS job limit of 300 jobs. Note: This limit must be lower than the setting specified in ΓÇ£Maximum number of BITS jobs for this computerΓÇ¥, or 300 if the ΓÇ£Maximum number of BITS jobs for this computerΓÇ¥ setting is not configured. BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of BITS jobs for this computer	At least Windows Vista or later	This setting specifies the maximum number of BITS jobs that can be created for all users of the computer. By default, BITS limits the total number of jobs that can be created on the computer to 300 jobs. You can use this setting to raise or lower the maximum number of user BITS jobs. If you enable this setting, BITS will limit the maximum number of BITS jobs to the specified number. If you disable or do not configure this setting, BITS will use the default BITS job limit of 300 jobs. Note: BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of files allowed in a BITS job	At least Windows Vista or later	This setting specifies the maximum number of files that a BITS job can contain. By default, a BITS job is limited to 200 files. You can use this setting to raise or lower the maximum number of files a BITS jobs can contain. If you enable this setting, BITS will limit the maximum number of files a job can contain to the specified number. If you disable or do not configure this setting, BITS will use the default value of 200 for the maximum number of files a job can contain. Note: BITS Jobs created by services and the local administrator account

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				do not count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of ranges that can be added to the file in a BITS job	At least Windows Vista or later	This setting specifies the maximum number of ranges that can be added to a file in a BITS job. By default, files in a BITS job are limited to 500 ranges per file. You can use this setting to raise or lower the maximum number ranges per file. If you enable this setting, BITS will limit the maximum number of ranges that can be added to a file to the specified number. If you disable or do not configure this setting, BITS will limit ranges to 500 ranges per file. Note: BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	BitLocker Drive Encryption	Configure encryption method	At least Windows Vista or later	This policy setting allows you to configure the algorithm and key size used by BitLocker Drive Encryption. This policy setting applies on a fully-decrypted disk. Changing the encryption method has no effect if the disk is already encrypted or if encryption is in progress. If you enable this policy setting, you can configure the encryption method used on an unencrypted volume. Consult online documentation for more information about the available encryption methods. If you disable or do not configure this policy setting, BitLocker will use the default encryption method of AES 128 bit with Diffuser or the encryption method specified by a local administrator's setup script.
Computer	BitLocker Drive Encryption	Configure TPM platform validation profile	At least Windows Vista or later	This policy setting allows you to configure how the computer's Trusted Platform Module (TPM) security hardware secures the BitLocker encryption key. This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection. If you enable this policy setting before turning on BitLocker, you can configure the boot components that the TPM will validate before unlocking access to the BitLocker-encrypted OS volume. If any of these components change while BitLocker protection is in effect, the TPM will not release the encryption key to unlock the volume and

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the computer will enter into recovery mode during boot. If you disable or do not configure this policy setting, the TPM uses the default platform validation profile or the platform validation profile specified by a local administrator's setup script. The default platform validation profile secures the encryption key against changes to the Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions (PCR 0), the Option ROM Code (PCR 2), the Master Boot Record (MBR) Code (PCR 4), the NTFS Boot Sector (PCR 8), the NTFS Boot Block (PCR 9), the Boot Manager (PCR 10), and the BitLocker Access Control (PCR 11). WARNING: Changing from the default profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending upon inclusion or exclusion (respectively) of the PCRs.
Computer	BitLocker Drive Encryption	Control Panel Setup: Configure recovery folder	At least Windows Vista or later	This policy setting allows you to specify the default path that is displayed when the BitLocker Drive Encryption setup wizard prompts the user to enter the location of a folder in which to save the recovery password. If you enable this policy setting, you can specify the path that will be used as the default folder location when the user chooses the option to save the recovery password in a folder. You can specify either a fully-qualified path or include the target computer's environment variables in the path. If the path is not valid, the BitLocker setup wizard will display the computer's top-level folder view. If you disable or do not configure this policy setting, the BitLocker setup wizard will display the computer's top-level folder view when the user chooses the option to save the recovery password in a folder. Note: In all cases, the user will be able to select other folders in which to save the recovery password.
Computer	BitLocker Drive	Control Panel Setup: Configure	At least Windows	This policy setting allows you to configure whether the BitLocker Drive Encryption setup

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Encryption	recovery options	Vista or later	wizard will ask the user to save BitLocker recovery options. Two recovery options can unlock access to BitLocker-encrypted data. The user can type a random 48-digit numerical recovery password. The user can also insert a USB flash drive containing a random 256-bit recovery key. If you enable this policy setting, you can configure the options that the setup wizard exposes to users for recovering BitLocker. For example, disallowing the 48-digit recovery password will prevent users from being able to print or save recovery information to a folder. If you disable or do not configure this policy setting, the BitLocker setup wizard will present users with ways to store recovery options. Saving to a USB flash drive will store the 48-digit recovery password as a text file, and the 256-bit recovery key as a hidden file. Saving to a folder will store the 48-digit recovery password as a text file. Printing will provide the 48-digit recovery password. Note: If TPM initialization is needed during the BitLocker setup, TPM owner information will be saved or printed with the BitLocker recovery information. Note: The 48-digit recovery password will not be available in FIPS compliance mode. IMPORTANT: To prevent data loss, you must have a way to recover BitLocker. If you disallow both recovery options below, you must enable the policy setting to "Turn on BitLocker backup to Active Directory Domain Services". Otherwise, a policy error occurs.
Computer	BitLocker Drive Encryption	Control Panel Setup: Enable advanced startup options	At least Windows Vista or later	This policy setting allows you to configure whether the BitLocker Drive Encryption setup wizard will ask the user to set up an additional authentication that is requested each time the computer starts. On a computer with a compatible Trusted Platform Module (TPM), two types of startup authentications can work to provide added protection for encrypted data. When the computer starts, it can require users to insert a USB flash drive containing a startup key. It can also require users to enter a 4 to 20 digit startup PIN. A USB flash drive containing a startup key is needed on computers without a compatible Trusted Platform

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Module (TPM). Without a TPM, BitLocker-encrypted data is protected solely by the key material on this USB flash drive. If you enable this policy setting, the wizard will show the page to allow the user to configure advanced startup options for BitLocker. You can further configure setting options for computers with and without a TPM. If you disable or do not configure this policy setting, the BitLocker setup wizard will display basic steps that allow users to enable BitLocker on computers with a TPM. In this basic wizard, no additional startup key or startup PIN can be configured.
Computer	BitLocker Drive Encryption	Turn on BitLocker backup to Active Directory Domain Services	At least Windows Vista or later	This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of BitLocker Drive Encryption recovery information. If you enable this policy setting, BitLocker recovery information will be automatically and silently backed up to AD DS when BitLocker is turned on for a computer. BitLocker recovery information includes the recovery password and some unique identifier data. You can also include a package that contains a BitLocker-protected volume's encryption key. This key package is secured by one or more recovery passwords and may help perform specialized recovery when the disk is damaged or corrupted. If you select the option to "Require BitLocker backup to AD DS", BitLocker cannot be turned on unless the computer is connected to the domain and the AD DS backup succeeds. This option is selected by default to help ensure that BitLocker recovery is possible. Otherwise, AD DS backup is attempted but network or other backup failures do not impact BitLocker setup. Backup is not automatically retried and the recovery password may not have been stored in AD DS during BitLocker setup. If you disable or do not configure this policy setting, BitLocker recovery information will not be backed up to AD DS. IMPORTANT: To prevent data loss, you must have a way to recover BitLocker. Note: You must first set up appropriate schema extensions and access control settings on the domain

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				before AD DS backup can succeed. Consult online documentation for more information about setting up Active Directory Domain Services for BitLocker. Note: TPM initialization may be needed during BitLocker setup. Enable the policy setting to "Turn on TPM backup to Active Directory Domain Services" in "System\Trusted Platform Module Services\" to ensure that TPM information is also backed up.
Computer	Button Settings	Select the Lid Switch Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user closes the lid on a mobile PC. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Lid Switch Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user closes the lid on a mobile PC. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Power Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the power button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Power Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the power button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Sleep Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the sleep button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Sleep Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the sleep button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Start Menu Power Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the user interface sleep button. Possible actions include: -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Start Menu Power Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the user interface sleep button. Possible actions include: -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer/User	Client	Prevent backing up to local disks	At least Windows Vista or later	This setting lets you prevent users from selecting a local disk (internal or external) for storing file backups. If this setting is enabled, the user will be blocked from selecting a local disk as a file backup location. If this setting is disabled or not configured, users can select a local disk as a file backup location.
Computer/User	Client	Prevent backing up to network shared folder	At least Windows Vista or later	This setting lets you prevent users from selecting a network shared folder for storing file backups. If this setting is enabled, users will be blocked from selecting a network shared folder as a file backup location. If this setting is disabled or not configured, users can select a network shared folder as a file backup location.
Computer/User	Client	Prevent backing up to optical	At least Windows	This setting lets you prevent users from selecting optical media (CD/DVD) for storing file

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		media (CD/DVD)	Vista or later	backups. If this setting is enabled, users will be blocked from selecting optical media as a file backup location. If this setting is disabled or not configured, users can select optical media as a file backup location.
Computer/User	Client	Prevent the user from running the Backup Status and Configuration program	At least Windows Vista or later	This setting lets you disable the Backup Status and Configuration program, which links to the file backup, file restore, and Complete PC Backup applications and shows backup status. If this setting is enabled, a user cannot start the Backup Status and Configuration program. If this setting is disabled or not configured, users can start the Backup Status and Configuration program.
Computer/User	Client	Turn off backup configuration	At least Windows Vista or later	This setting lets you disable file backup functionality. If this setting is enabled, the file backup program is disabled. If this setting is disabled or not configured, the file backup program is enabled and users can create a file backup.
Computer/User	Client	Turn off Complete PC Backup functionality	At least Windows Vista or later	This setting lets you disable Complete PC Backup functionality. If this setting is enabled, the Complete PC Backup program is disabled. If this setting is disabled or not configured, the Complete PC Backup program is enabled and users can create a Complete PC Backup image.
Computer/User	Client	Turn off restore functionality	At least Windows Vista or later	This setting lets you disable file restore functionality. If this setting is enabled, the file restore program is disabled. If this setting is disabled or not configured, the file restore program is enabled and users can restore files.
Computer/User	Consent	Configure Default consent	At least Windows Vista or later	This setting determines the consent behavior of Windows Error Reporting. If Consent level is set to "Always ask before sending data", Windows will prompt the user for consent to send reports. If Consent level is set to "Send parameters", the minimum data required to check for an existing solution will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If Consent level is set to

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				"Send parameters and safe additional data", the minimum data required to check for an existing solution as well as data which Windows has determined does not contain (within a high probability) personally identifiable data will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If Consent level is set to "Send all data", any data requested by Microsoft will be sent automatically. If this setting is disabled or not configured then consent will default to "Always ask before sending data".
Computer/User	Consent	Customize consent settings	At least Windows Vista or later	This policy setting determines the consent behavior of Windows Error Reporting for specific event types. If this policy setting is enabled and the consent level is set to "0" (Disable), Windows Error Reporting will not send any data to Microsoft for this event. If the consent level is set to "1" (Always ask before sending data), Windows will prompt the user for consent to send reports. If the consent level is set to "2" (Send parameters), the minimum data required to check for an existing solution will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If the consent level is set to "3" (Send parameters and safe additional data), the minimum data required to check for an existing solution as well as data which Windows has determined does not contain (within a high probability) personally identifiable data will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If the consent level is set to "4" (Send all data), any data requested by Microsoft will be sent automatically. If this setting is disabled or not configured then consent will default to the default consent setting.
Computer/User	Consent	Ignore custom consent settings	At least Windows Vista or later	This setting determines the behavior of the default consent setting in relation to custom consent settings. If this setting is enabled, the default Consent level setting will always

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				override any other consent setting. If this setting is disabled or not configured, each custom consent setting will determine the consent level for that event type and the default consent setting will determine the consent level of any other reports.
Computer	Corrupted File Recovery	Configure Corrupted File Recovery Behavior	At least Windows Vista or later	This policy setting allows you to configure the recovery behavior for corrupted files to one of three states: Regular: Detection, troubleshooting, and recovery of corrupted files will automatically start with a minimal UI display. Windows will attempt to present you with a dialog box when a system restart is required. This is the default recovery behavior for corrupted files. Silent: Detection, troubleshooting, and recovery of corrupted files will automatically start with no UI. Windows will log an administrator event when a system restart is required. This behavior is recommended for headless operation. Troubleshooting Only: Detection and troubleshooting of corrupted files will automatically start with no UI. Recovery is not attempted automatically. Windows will log an administrator event with instructions if manual recovery is possible. If you enable this setting, the recovery behavior for corrupted files will be set to either the regular (default), silent, or troubleshooting only state. If you disable this setting, the recovery behavior for corrupted files will be disabled. No troubleshooting or resolution will be attempted. If you do not configure this setting, the recovery behavior for corrupted files will be set to the regular recovery behavior. No system or service restarts are required for changes to this policy to take immediate effect after a Group Policy refresh. Note: This policy setting will take effect only when the Diagnostic Policy Service (DPS) is in the running state. When the service is stopped or disabled, system file recovery will not be attempted. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Credential User	Do not enumerate administrator	At least Windows	By default all administrator accounts are displayed when attempting to elevate a running

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Interface	accounts on elevation.	Vista or later	application. If you enable this policy, users will be required to always type in a username and password to elevate. If you disable this policy, all local administrator accounts on the machine will be displayed so the user can choose one and enter the correct password.
Computer	Credential User Interface	Require trusted path for credential entry.	At least Windows Vista or later	This policy setting requires the user to enter Microsoft Windows credentials using a trusted path, to prevent a Trojan horse or other types of malicious code from stealing the userΓÇÖs Windows credentials. Note: This policy affects nonlogon authentication tasks only. As a security best practice, this policy should be enabled. If you enable this policy setting, users will be required to enter Windows credentials on the Secure Desktop by means of the trusted path mechanism. If you disable or do not configure this policy setting, users will enter Windows credentials within the userΓÇÖs desktop session, potentially allowing malicious code access to the userΓÇÖs Windows credentials.
Computer	Credentials Delegation	Allow Default Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can be delegated when the authentication mechanism is NTLM (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, delegation of default credentials is not permitted to any machine. Note that "Allow Delegating Default Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. Note: The "Allow Default Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Default Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can be delegated (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, delegation of default credentials is not permitted to any machine. Note: The "Allow Delegating Default Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Fresh Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's fresh credentials can be delegated when the authentication mechanism is NTLM (fresh credentials are those that you are prompted for when executing the application). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of fresh credentials is permitted to Terminal Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note: "Allow Delegating Fresh Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Fresh Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Saved Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can be delegated (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of saved credentials is permitted to Terminal Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note:The "Allow Delegating Saved Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Fresh Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				user's fresh credentials can be delegated when the authentication mechanism is NTLM (fresh credentials are those that you are prompted for when executing the application). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of fresh credentials is permitted to Terminal Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note: "Allow Delegating Fresh Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow Fresh Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Saved Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can be delegated to when the authentication mechanism is NTLM (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of saved credentials is permitted to Terminal Server running on any machine (TERMSRV/*) if the client machine is not a member of any domain. If the client is domain-joined, then by default the delegation of saved credentials is not permitted to any machine. If you disable this policy setting delegation of fresh credentials is

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				not permitted to any machine. Note: that "Allow Delegating Saved Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow Saved Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com
Computer	Credentials Delegation	Deny Delegating Default Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can NOT be delegated to (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, this setting does not specify any server. Note: "The Deny Delegating Default Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Default Credentials" to define exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Default Credentials"

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				server list.
Computer	Credentials Delegation	Deny Delegating Fresh Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's fresh credentials can NOT be delegated (fresh credentials are those that you are prompted for when executing the application). If you disable or do not configure (by default) this policy setting, this setting does not specify any server. Note: The "Deny Delegating Fresh Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Fresh Credentials" to define exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Fresh Credentials" server list.
Computer	Credentials Delegation	Deny Delegating Saved Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can NOT be delegated (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you disable or do not configure (by default) this policy setting, this setting does not specify any server. Note: The "Deny Delegating Saved Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Saved Credentials" to define exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Saved Credentials" server list.
Computer/User	Cursors	Turn off pen feedback	At least Windows Vista or later	Disables visual pen action feedback, except for press and hold feedback. If you enable this policy, all visual pen action feedback is disabled except for press and hold feedback. Additionally, the mouse cursors are shown instead of the pen cursors. If you disable or do not configure this policy, visual feedback and pen cursors will be shown unless the user disables them in Control Panel.
Computer	DC Locator DNS Records	Domain Controller Address Type Returned	At least Windows Vista or later	The Domain Controller (DC) Locator APIs return IP address of the DC with the other part of the information. Before the support of IPv6, the returned DC IP address was IPv4. But with the support of IPv6, the DC Locator APIs can return IPv6 DC address. The returned IPv6 DC address may not be correctly handled by some of the existing applications. So this policy is provided to support such scenarios. By default, DC Locator APIs can return IPv4/IPv6 DC address. But if some applications are broken due to the returned IPv6 DC address, this policy can be used to disable the default behavior and enforce to return ONLY IPv4 DC address. Once applications are fixed, this policy can be used to enable the default behavior. If you enable this policy setting, DC Locator APIs can return IPv4/IPv6 DC address. This is the default behavior of the DC Locator. If you disable this policy setting, DC

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Locator APIs will ONLY return IPv4 DC address if any. So if the domain controller supports both IPv4 and IPv6 addresses, DC Locator APIs will return IPv4 address. But if the domain controller supports only IPv6 address, then DC Locator APIs will fail. If you do not configure this policy setting, DC Locator APIs can return IPv4/IPv6 DC address. This is the default behavior of the DC Locator.
Computer	DC Locator DNS Records	Force Rediscovery Interval	At least Windows Vista or later	The Domain Controller Locator (DC Locator) service is used by clients to find domain controllers for their Active Directory domain. When DC Locator finds a domain controller, it caches domain controllers to improve the efficiency of the location algorithm. As long as the cached domain controller meets the requirements and is running, DC Locator will continue to return it. If a new domain controller is introduced, existing clients will only discover it when a Force Rediscovery is carried out by DC Locator. To adapt to changes in network conditions DC Locator will by default carry out a Force Rediscovery according to a specific time interval and maintain efficient load-balancing of clients across all available domain controllers in all domains or forests. The default time interval for Force Rediscovery by DC Locator is 12 hours. Force Rediscovery can also be triggered if a call to DC Locator uses the DS_FORCE_REDISCOVERY flag. Rediscovery resets the timer on the cached domain controller entries. If you enable this policy setting, DC Locator on the machine will carry out Force Rediscovery periodically according to the configured time interval. The minimum time interval is 3600 seconds (1 hour) to avoid excessive network traffic from rediscovery. The maximum allowed time interval is 4294967200 seconds, while any value greater than 4294967 seconds (~49 days) will be treated as infinity. If you disable this policy setting, Force Rediscovery will be used by default for the machine at every 12 hour interval. If you do not configure this policy setting, Force Rediscovery will be used by default for the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				machine at every 12 hour interval, unless the local machine setting in the registry is a different value.
Computer	DC Locator DNS Records	Try Next Closest Site	At least Windows Vista or later	The Domain Controller Locator (DC Locator) service is used by clients to find domain controllers for their Active Directory domain. The default behavior for DC Locator is to find a DC in the same site. If none are found in the same site, a DC in another site, which might be several site-hops away, could be returned by DC Locator. Site proximity between two sites is determined by the total site-link cost between them. A site is closer if it has a lower site link cost than another site with a higher site link cost. The Try Next Closest Site feature enables DC Locator to attempt to locate a DC in the nearest site based on the site link cost if a DC in same the site is not found. In scenarios with multiple sites, failing over to the try next closest site during DC Location streamlines network traffic more effectively. If you enable this policy setting, Try Next Closest Site DC Location will be turned on for the machine across all available but un-configured network adapters. If you disable this policy setting, Try Next Closest Site DC Location will not be used by default for the machine across all available but un-configured network adapters. However, if a DC Locator call is made using the DS_TRY_NEXTCLOSEST_SITE flag explicitly, the Try Next Closest Site behavior is honored. If you do not configure this policy setting, Try Next Closest Site DC Location will not be used by default for the machine across all available but un-configured network adapters. If the DS_TRY_NEXTCLOSEST_SITE flag is used explicitly, the Next Closest Site behavior will be used.
User	Desktop	Desktop Wallpaper	At least Windows Vista or later	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)

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				or JPEG (*.jpg) 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: This setting does not apply to Terminal Server sessions.
Computer/User	Desktop Window Manager	Do not allow desktop composition	At least Windows Vista or later	This policy setting controls how some graphics are rendered and facilitates other features, including Flip, Flip3D, and Taskbar Thumbnails. If you enable this setting, the desktop compositor visual experience will be turned off. If you disable or do not configure this policy setting, desktop composition will be turned on, if the required hardware is in place.
Computer/User	Desktop Window Manager	Do not allow Flip3D invocation	At least Windows Vista or later	Flip3D is a 3D window switcher. If you enable this setting, Flip3D will be inaccessible. If you disable or do not configure this policy setting, Flip3D will be accessible, if desktop composition is turned on.
Computer/User	Desktop Window Manager	Do not allow window animations	At least Windows Vista or later	This policy setting controls the appearance of window animations such as those found when restoring, minimizing, and maximizing windows. If you enable this setting, window animations will be turned off. If you disable or do not configure this setting, window animations will be turned on.
Computer	Device and Resource Redirection	Do not allow supported Plug and Play device redirection	At least Windows Vista or later	This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Terminal Services session.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				By default, Terminal Services allows redirection of supported Plug and Play devices. Users can use the ΓÇ£MoreΓÇ¥ option on the Local Resources tab of Remote Desktop Connection to choose the supported Plug and Play devices to redirect to the remote computer. If you enable this policy setting, users cannot redirect their supported Plug and Play devices to the remote computer. If you disable this policy setting or do not configure this policy setting, users can redirect their supported Plug and Play devices to the remote computer. Note: You can also disallow redirection of supported Plug and Play devices on the Client Settings tab in the Terminal Services Configuration tool. You can disallow redirection of specific types of supported Plug and Play devices by using the ΓÇ£Computer Configuration\Administrative Templates\System\Device Installation\Device Installation RestrictionsΓÇ¥ policy settings.
Computer	Device Installation	Allow remote access to the PnP interface	At least Windows Vista or later	Specifies whether or not remote access to the Plug and Play interface is allowed. If you enable this setting, remote connections to the PnP interface will be allowed. If you disable or do not configure this setting, PnP interface will not be available remotely.
Computer	Device Installation	Configure device installation timeout	At least Windows Vista or later	Specifies the number of seconds the system will wait for a device installation task to complete. If the task is not complete within the specified number of seconds, the system will terminate the installation. If you enable this setting, the system will wait for the number of seconds specified before forcibly terminating the installation. If you disable or do not configure this setting, the system will wait 300 seconds (5 minutes) for any device installation task to complete before terminating installation.
Computer/User	Device Installation	Do not create system restore point when new device driver installed	At least Windows Vista or later	Specifies whether or not a system restore point is created when a new device driver is installed on your machine. If you enable this setting, system restore points will not be created when a new device driver is installed or updated. If you disable or do not configure

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this setting, a system restore point will be created whenever a new driver is installed or an existing device driver is updated.
Computer	Device Installation	Do not send a Windows Error Report when a generic driver is installed on a device	At least Windows Vista or later	Specifies whether or not to send a Windows Error Report when a generic driver is installed on a device. If you enable this setting, a Windows Error Report will not be sent when a generic driver is installed. If you disable or do not configure this setting, a Windows Error Report will be sent when a generic driver is installed.
Computer	Device Installation	Treat all digitally signed drivers equally in the driver ranking and selection process	At least Windows Vista or later	When selecting which driver to install, do not distinguish between drivers that are signed by a Microsoft Windows Publisher certificate and drivers that are signed by others. If you enable this setting, all valid Authenticode signatures are treated equally for the purpose of selecting a device driver to install. Selection is based on other criteria (such as version number or when the driver was created) rather than whether the driver was signed by a Microsoft Windows Publisher certificate or by another Authenticode certificate. A signed driver is still preferred over a driver that is not signed at all. However, drivers that are signed by Microsoft Windows Publisher certificates are not preferred over drivers signed by other Authenticode certificates. If you disable or do not configure this setting, drivers that are signed by a Microsoft Windows Publisher certificate are selected for installation over drivers that are signed by other Authenticode certificates.
Computer	Device Installation	Turn off "Found New Hardware" balloons during device installation	At least Windows Vista or later	Do not display "Found New Hardware" balloons during device installation. If you enable this setting, "Found New Hardware" balloons will not appear while a device is being installed. If you disable or do not configure this setting, "Found New Hardware" balloons will appear while a device is being installed unless the driver for the device has suppressed the balloons.
Computer	Device Installation	Allow administrators to override	At least Windows	Allows members of the Administrators group to install and update the drivers for any device,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Restrictions	Device Installation Restriction policies	Vista or later	regardless of other policy settings. If you enable this setting, administrators can use "Add Hardware Wizard" or "Update Driver Wizard" to install and update the drivers for any device. If you disable or do not configure this setting, administrators are subject to all policies that restrict device installation. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Allow installation of devices that match any of these device IDs	At least Windows Vista or later	Specifies a list of Plug and Play hardware IDs and compatible IDs that describe devices that can be installed. This setting is intended to be used only when the "Prevent installation of devices not described by other policy settings" setting is enabled and does not take precedence over any policy setting that would prevent a device from being installed. If you enable this setting, any device with a hardware ID or compatible ID that matches an ID in this list can be installed or updated, if that installation has not been specifically prevented by the "Prevent installation of devices that match these device IDs," "Prevent installation of devices for these device classes," or "Prevent installation of removable devices" policy setting. If another policy setting prevents a device from being installed, the device cannot be installed even if it is also described by a value in this policy setting. If you disable or do not configure this setting and no other policy describes the device, the "Prevent installation of devices not described by other policy settings" setting determines whether the device can be installed. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Allow installation of devices using drivers that match these device setup classes		

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Device Installation Restrictions	Display a custom message when installation is prevented by policy (balloon text)	At least Windows Vista or later	Specifies a custom message that is displayed to the user in the text of the notification balloon when policy prevents the installation of a device. If you enable this setting, then this text is displayed as the main body text of the message displayed by Windows whenever device installation is prevented by policy. If you disable or do not configure this setting, then Windows displays a default message whenever device installation is prevented by policy.
Computer	Device Installation Restrictions	Display a custom message when installation is prevented by policy (balloon title)	At least Windows Vista or later	Specifies a custom message that is displayed to the user in the title of the notification balloon when policy prevents the installation of a device. If you enable this setting, then this text is displayed as the title text of the message displayed by Windows whenever device installation is prevented by policy. If you disable or do not configure this setting, then Windows displays a default title whenever device installation is prevented by policy.
Computer	Device Installation Restrictions	Prevent installation of devices not described by other policy settings	At least Windows Vista or later	This setting controls the installation policy for devices that are not specifically described by any other policy. If you enable this setting, any device that is not described by either the "Allow installation of devices that match these device IDs" or "Allow installation of devices for these device classes" cannot be installed or have its driver updated. If you disable or do not configure this setting, any device that is not described by the "Prevent installation of devices that match these device IDs," "Prevent installation of devices for these device classes," or "Deny installation of removable devices" policies can be installed and have its driver updated. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Device Installation Restrictions	Prevent installation of devices that match any of these device IDs	At least Windows Vista or later	Specifies a list of Plug and Play hardware IDs and compatible IDs for devices that cannot be installed. If you enable this setting, a device cannot be installed or updated if its hardware ID or compatible ID matches one in this list. If you disable or do not configure this setting, new devices can be installed and existing devices can be updated, as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Prevent installation of devices using drivers that match these device setup classes	At least Windows Vista or later	Specifies a list of Plug and Play device setup class GUIDs for devices that cannot be installed. If you enable this setting, new devices cannot be installed and existing devices cannot be updated if they use drivers that belong to any of the listed device setup classes. If you disable or do not configure this setting, new devices can be installed and existing devices can be updated as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Device Installation Restrictions	Prevent installation of removable devices	At least Windows Vista or later	Prevents removable devices from being installed. If you enable this setting, removable devices may not be installed, and existing removable devices cannot have their drivers updated. If you disable or do not configure this setting, removable devices can be installed and existing removable devices can be updated as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. For this policy, a device is considered to be removable when the drivers for the device to which it is connected indicate that the device is removable. For example, a Universal Serial Bus (USB) device is reported to be removable by the drivers for the USB hub to which the device is connected. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer/User	Digital Locker	Do not allow Digital Locker to run	At least Windows Vista or later	Specifies whether Digital Locker can run. Digital Locker is a dedicated download manager associated with Windows Marketplace and a feature of Windows that can be used to manage and download products acquired and stored in the user's Windows Marketplace Digital Locker. If you enable this setting, Digital Locker will not run. If you disable or do not configure this setting, Digital Locker can be run.
Computer	Disk Diagnostic	Disk Diagnostic: Configure custom alert text	At least Windows Vista or later	Substitutes custom alert text in the disk diagnostic message shown to users when a disk reports a S.M.A.R.T. fault. If you enable this policy setting, Windows will display custom alert text in the disk diagnostic message. The custom text may not

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				exceed 512 characters. nIf you disable or do not configure this policy setting, Windows will display the default alert text in the disk diagnostic message. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect if the Disk Diagnostic scenario policy is enabled or not configured and the Diagnostic Policy Service (DPS) is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Disk Diagnostic	Disk Diagnostic: Configure execution level	At least Windows Vista or later	Determines the execution level for S.M.A.R.T.-based disk diagnostics. Self-Monitoring And Reporting Technology (S.M.A.R.T.) is a standard mechanism for storage devices to report faults to Windows. A disk that reports a S.M.A.R.T. fault may need to be repaired or replaced. The Diagnostic Policy Service (DPS) will detect and log S.M.A.R.T. faults to the event log when they occur. If you enable this policy setting, the DPS will also warn users of S.M.A.R.T. faults and guide them through backup and recovery to minimize potential data loss. If you disable this policy, S.M.A.R.T. faults will still be detected and logged, but no corrective action will be taken. If you do not configure this policy setting, the DPS will enable S.M.A.R.T. fault resolution by default. This policy setting takes effect only if the diagnostics-wide scenario execution policy is not configured. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Services snap-in to the Microsoft Management Console.
Computer	Disk NV Cache	Turn Off Boot and Resume Optimizations	At least Windows Vista or later	Turns off the boot and resume optimizations for the hybrid hard disks in the system. If you enable this policy setting, the system does not use the non-volatile (NV) cache to optimize boot and resume. If you disable this policy setting, the system uses the NV cache to achieve faster boot and resume. The system determines the data that will be stored in the NV cache to optimize boot and resume. The required data is stored in the NV cache during shutdown and hibernate respectively. This might cause a slight increase in the time taken for shutdown and hibernate. If you do not configure this policy, the default behavior is observed and the NV cache is used for boot and resume optimizations. NOTE: This policy is applicable only if the NV Cache Feature is on.
Computer	Disk NV Cache	Turn Off Cache Power Mode	At least Windows Vista or later	Turns off the power save mode on the hybrid hard disks in the system. If you enable this policy, the disks will not be put into NV cache power save mode and no power savings would be achieved. If you disable this policy setting, then the hard disks are put into a NV cache power saving mode. In this mode, the system tries to save power by aggressively spinning down the disk. If you do not configure this policy setting, the default behavior is to allow the hybrid hard disks to be in power save mode. NOTE: This policy is applicable only if the NV Cache feature is on.
Computer	Disk NV Cache	Turn Off Non Volatile Cache Feature	At least Windows Vista or later	Turns off all support for the non-volatile (NV) cache on all hybrid hard disks in the system. To check if you have hybrid hard disks in the system, from the device manager, right click the disk drive and select Properties. The NV cache can be used to optimize boot and resume by reading data from the cache while the disks

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				are spinning up. The NV cache can also be used to reduce the power consumption of the system by keeping the disks spun down while satisfying reads and writes from the cache. If you enable this policy setting, the system will not manage the NV cache and will not enable NV cache power saving mode. If you disable this policy setting, the system will manage the NV cache on the disks provided the other policy settings for the NV cache are appropriately configured. NOTE: This setting will take effect on next boot. If you do not configure this policy, the default behavior is to turn on support for the NV cache.
Computer	Disk NV Cache	Turn Off Solid State Mode	At least Windows Vista or later	Turns off the solid state mode for the hybrid hard disks. If you enable this policy setting, frequently written files such as the file system metadata and registry may not be stored in the NV cache. If you disable this policy setting, the system will store frequently written data into the non-volatile (NV) cache. This allows the system to exclusively run out of the NV cache and power down the disk for longer periods to save power. Note that this can cause increased wear of the NV cache. If you do not configure this policy, the default behavior of the system is observed and frequently written files will be stored in the NV cache. NOTE: This policy is applicable only if the NV Cache Feature is on.
Computer	DNS Client	Allow DNS Suffix Appending to Unqualified Multi-Label Name Queries	At least Windows Vista or later	Specifies whether the computers to which this setting is applied may attach suffixes to an unqualified multi-label name before sending subsequent DNS queries, if the original name query fails. A name containing dots, but not dot-terminated, is called an unqualified multi-label name, for example "server.corp". A fully qualified name would have a terminating dot, for example "server.corp.contoso.com.". If you enable this setting, suffixes are allowed to be

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				appended to an unqualified multi-label name, if the original name query fails. For example, an unqualified multi-label name query for "server.corp" will be queried by the DNS Client first. If the query succeeds, the response is returned to the client. If the query fails, the unqualified multi-label name is appended with DNS Suffixes configured for the computer for queries. These suffixes can be derived from a combination of the local DNS Client's primary domain suffix, a connection-specific domain suffix and/or DNS Suffix Search List. For example, if the local DNS Client receives a query for "server.corp", and a primary domain suffix is configured as "contoso.com", with this setting the DNS Client will send a query for "server.corp.contoso.com." if the original name query for "server.corp" fails. If you disable this setting, no suffixes are appended to unqualified multi-label name queries if the original name query fails. If you do not configure this setting, computers will use their local DNS Client configuration to determine the query behavior for unqualified multi-label names.
Computer	DNS Client	Turn off Multicast Name Resolution	At least Windows Vista or later	Local Link Multicast Name Resolution (LLMNR) is a secondary name resolution protocol. Queries are sent over the Local Link, a single subnet, from a client machine using Multicast to which another client on the same link, which also has LLMNR enabled, can respond. LLMNR provides name resolution in scenarios in which conventional DNS name resolution is not possible. If you enable this policy setting, Multicast name resolution or LLMNR, will be turned off for the machine across all available but un-configured network adapters. If you disable this policy setting, Multicast name resolution or LLMNR, will be turned on for the machine across all available but un-configured network adapters. If you do not configure

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this policy setting, Multicast name resolution or LLMNR, will be turned on for the machine across all available but un-configured network adapters by default.
Computer	Driver Installation	Allow non-administrators to install drivers for these device setup classes	At least Windows Vista or later	Specifies a list of device setup class GUIDs describing device drivers that non-administrator members of the built-in Users group may install on the system. If you enable this setting, members of the Users group may install new drivers for the specified device setup classes. The drivers must be signed according to Windows Driver Signing Policy, or be signed by publishers already in the TrustedPublisher store. If you disable or do not configure this setting, only members of the Administrators group are allowed to install new device drivers on the system.
User	Explorer Frame Pane	Turn off Details Pane		
User	Explorer Frame Pane	Turn off Preview Pane	At least Windows Vista or later	Hides the Preview Pane in Windows Explorer. If you enable this policy setting, the Preview Pane in Windows Explorer is hidden and cannot be turned on by the user. If you disable, or do not configure this setting, the Preview Pane is displayed by default and can be hidden by the user.
Computer/User	Folder Redirection	Use localized subfolder names when redirecting Start and My Documents	At least Windows Vista or later	This policy setting allows the administrator to define whether Folder Redirection should use localized names for the All Programs, Startup, My Music, My Pictures, and My Videos subfolders when redirecting the parent Start menu and legacy My Documents folder respectively. If you enable this policy setting, Windows Vista will use localized folder names for these subfolders when redirecting the Start Menu or legacy My Documents folder. If you disable or not configure this policy setting, Windows Vista will use the standard English names for these subfolders when redirecting the Start Menu or legacy My Documents folder. Note: This policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				is valid only on Windows Vista when it processes a legacy redirection policy already deployed for these folders in your existing localized environment.
Computer	Game Explorer	Turn off downloading of game information	At least Windows Vista or later	Manages download of game box art and ratings from the Windows Metadata Services. If you enable this setting, game information including box art and ratings will not be downloaded. If you disable or do not configure this setting, game information will be downloaded from Windows Metadata Services.
Computer	Game Explorer	Turn off tracking of last play time of games in the Games folder	At least Windows Vista or later	Tracks the last play time of games in the Games folder. If you enable this setting the last played time of games will not be recorded in Games folder. This setting only affects the Games folder. If you disable or do not configure this setting, the last played time will be displayed to the user.
Computer	General iSCSI	Do not allow additional session logins	At least Windows Vista or later	If enabled then only those sessions that are established via a persistent login will be established and no new persistent logins may be created. If disabled then additional persistent and non persistent logins may be established.
Computer	General iSCSI	Do not allow changes to initiator iqn name	At least Windows Vista or later	If enabled then do not allow the initiator iqn name to be changed. If disabled then the initiator iqn name may be changed.
Computer	Group Policy	Startup policy processing wait time	At least Windows Vista or later	This policy setting specifies how long Group Policy should wait for network availability notifications during startup policy processing. If the startup policy processing is synchronous, the computer is blocked until the network is available or the default wait time is reached. If the startup policy processing is asynchronous, the computer is not blocked and policy processing will occur in the background. In either case, configuring this policy setting overrides any system-computed wait times. If you enable this policy setting, Group Policy will use this administratively configured maximum wait time and override any default or

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				system-computed wait time. If you disable or do not configure this policy setting, Group Policy will use the default wait time of 30 seconds on computers running the Microsoft Windows Vista operating system.
Computer	Group Policy	Turn off Local Group Policy objects processing	At least Windows Vista or later	This policy setting prevents Local Group Policy objects (Local GPOs) from being applied. By default, the policy settings in Local GPOs are applied before any domain-based GPO policy settings. These policy settings can apply to both users and the local computer. You can disable the processing and application of all Local GPOs to ensure that only domain-based GPOs are applied. If you enable this policy setting, the system will not process and apply any Local GPOs. If you disable or do not configure this policy setting, Local GPOs will continue to be applied. Note: For computers joined to a domain, it is strongly recommended that you only configure this policy setting in domain-based GPOs. This setting will be ignored on computers that are joined to a workgroup.
User	Group Policy snap-in extensions	Windows Firewall with Advanced Security	At least Windows Vista or later	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

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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	Group Policy snap-in extensions, mmc	**NAP Client Configuration**	At least Windows Vista or later	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.
Computer/User	Handwriting personalization	Turn off automatic learning	At least Windows Vista or later	Turns off the automatic learning component of handwriting recognition personalization. Automatic learning enables the collection and storage of text and/or ink written by the user in order to help adapt handwriting recognition to the vocabulary and handwriting style of the user. Text that is collected includes all outgoing messages in Windows Mail, and MAPI enabled e-mail clients, plus URLs

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				from the Internet Explorer browser history. The information that is stored includes word frequency and new words not already known to the handwriting recognition engines (for example proper names and acronyms). Deleting e-mail content or the browser history will not delete the stored personalization data. Ink entered through Input Panel is collected and stored. Note: Automatic learning of both text and ink might not be available for all languages, even when handwriting personalization is available. See Tablet PC Help for more information. If you enable this policy, automatic learning stops and any stored data is deleted. Users will not be able to configure this setting in Control Panel. If you disable this policy, automatic learning is turned on. Users will not be able to configure this setting in Control Panel. Collected data is only used for handwriting recognition if handwriting personalization is turned on. If you do not configure this policy, users can choose to enable or disable automatic learning either from the Handwriting tab in the Tablet Settings in Control Panel or from the opt-in dialog. Related to ΓÇ£Turn off handwriting personalizationΓÇ¥ policy. Note: The amount of stored ink is limited to 50 MB and the amount of text information to about 5 MB. When these limits are reached and new data is collected, old data is deleted to make room for more recent data. Note: Handwriting personalization in Microsoft Windows VistaΓäó works only for Microsoft handwriting recognizers, not with third-party recognizers.
Computer/User	Handwriting personalization	Turn off handwriting personalization	At least Windows Vista or later	Turns off handwriting recognition personalization so the handwriting recognition engine that ships with Windows VistaΓäó is used instead of the personalized handwriting recognizer. Handwriting personalization allows the handwriting recognizer to adapt to the writing style and vocabulary of a user by using

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				automatic learning and the handwriting recognition personalization tool. Handwriting personalization is not available for all languages that have handwriting recognition. See Tablet PC Help for more information. If you enable this policy, handwriting personalization is turned off. The handwriting recognition that ships with Windows VistaΓäó is used. The information collected for handwriting personalization is not deleted, but it will not be used for handwriting recognition. Users will not be able to configure this setting in Control Panel. If you disable this policy, handwriting personalization is turned on. Users will not be able to configure this setting in Control Panel. If you do not configure this policy, handwriting personalization is turned on. Users will be able to configure this setting on the Handwriting tab of Tablet Settings, in Control Panel. Related to ΓÇ£Turn off automatic learningΓÇ¥ policy. Note: Handwriting personalization in Microsoft Windows VistaΓäó works only for Microsoft handwriting recognizers, not with third-party recognizers.
Computer	Hard Disk Settings	Turn Off the Hard Disk (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the hard disk. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the hard disk. If you disable this policy or do not configure it, users can see and change this setting.
Computer	Hard Disk Settings	Turn Off the Hard Disk (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the hard disk. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the hard disk. If you disable this policy or do not configure it, users can see and change this setting.
Computer/User	Hardware Buttons	Prevent Back-ESC mapping	At least Windows Vista or later	Removes the Back-&gt;ESC mapping that normally occurs when menus are

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				visible, and for applications that subscribe to this behavior. If you enable this policy, a button assigned to Back will not map to ESC. If you disable this policy, Back-&gt;ESC mapping will occur. If you do not configure this policy, Back-&gt;ESC mapping will occur.
Computer/User	Hardware Buttons	Prevent launch an application	At least Windows Vista or later	Prevents the user from launching an application from a Tablet PC hardware button. If you enable this policy, applications cannot be launched from a hardware button, and "Launch an application" is removed from the drop down menu for configuring button actions (in the Tablet PC Control Panel buttons tab). If you disable this policy, applications can be launched from a hardware button. If you do not configure this policy, applications can be launched from a hardware button.
Computer/User	Hardware Buttons	Prevent press and hold	At least Windows Vista or later	Prevents press and hold actions on hardware buttons, so that only one action is available per button. If you enable this policy, press and hold actions are unavailable, and the button configuration dialog will display the following text: "Some settings are controlled by Group Policy. If a setting is unavailable, contact your system administrator." If you disable this policy, press and hold actions for buttons will be available. If you do not configure this policy, press and hold actions will be available.
Computer/User	Hardware Buttons	Turn off hardware buttons	At least Windows Vista or later	Turns off Tablet PC hardware buttons. If you enable this policy, no actions will occur when the buttons are pressed, and the buttons tab in Tablet PC Control Panel will be removed. If you disable this policy, user and OEM defined button actions will occur when the buttons are pressed. If you do not configure this policy, user and OEM defined button actions will occur when the buttons are pressed.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Import Video	Do not allow Import Video to run	At least Windows Vista or later	Specifies whether Import Video can run. Import Video is a feature of Windows Vista that can be used to import video from a digital video device where the video is encoded and saved as a video file on your computer. If you enable this setting, Import Video will not run. If you disable or do not configure this setting, Import Video can be run.
Computer/User	Input Panel	For tablet pen input, donΓÇÖt show the Input Panel icon	At least Windows Vista or later	Prevents the Tablet PC Input Panel icon from appearing next to any text entry area in applications where this behavior is available. This policy applies only when using a tablet pen as an input device. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel will never appear next to text entry areas when using a tablet pen as an input device. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel will appear next to any text entry area in applications where this behavior is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will be able to configure this setting on the Opening tab in Input Panel Options. Caution: If you enable both the ΓÇ£Prevent Input Panel from appearing next to text entry areasΓÇ¥ policy and the ΓÇ£Prevent Input Panel tab from appearingΓÇ¥ policy, and disable the ΓÇ£Show Input Panel taskbar iconΓÇ¥ policy, the user will then have no way to access Input Panel.
Computer/User	Input Panel	For touch input, donΓÇÖt show the	At least Windows Vista or later	Prevents the Tablet PC Input Panel icon from appearing next to any text entry

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		Input Panel icon		area in applications where this behavior is available. This policy applies only when a user is using touch input. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel will never appear next to any text entry area when a user is using touch input. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will be able to configure this setting on the Opening tab in Input Panel Options.
Computer/User	Input Panel	Include rarely used Chinese, Kanji, or Hanja characters	At least Windows Vista or later	Includes rarely used Chinese, Kanji, and Hanja characters when handwriting is converted to typed text. This policy applies only to the use of the Microsoft recognizers for Chinese (Simplified), Chinese (Traditional), Japanese, and Korean. This setting appears in Input Panel Options only when these input languages or keyboards are installed. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, rarely used Chinese, Kanji, and Hanja characters will be included in recognition results when handwriting is converted to typed text. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, rarely used Chinese, Kanji, and Hanja characters will not be included in recognition

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				results when handwriting is converted to typed text. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, rarely used Chinese, Kanji, and Hanja characters will not be included in recognition results when handwriting is converted to typed text. Users will be able to configure this setting on the Advanced tab in the Input Panel Options dialog box.
Computer/User	Input Panel	Prevent Input Panel tab from appearing	At least Windows Vista or later	Prevents Input Panel tab from appearing on the edge of the Tablet PC screen. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel tab will not appear on the edge of the Tablet PC screen. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel tab will appear on the edge of the Tablet PC screen. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel tab will appear on the edge of the Tablet PC screen. Users will be able to configure this setting on the Opening tab in Input Panel Options. Caution: If you enable both the ΓÇ£Prevent Input Panel from appearing next to text entry areasΓÇ¥ policy and the ΓÇ£Prevent Input Panel tab from appearingΓÇ¥ policy, and disable the ΓÇ£Show Input Panel taskbar iconΓÇ¥ policy, the user will then have no way to access Input Panel.
Computer/User	Input Panel	Switch to the Simplified Chinese (PRC) gestures	At least Windows Vista or later	Switches the gesture set used for editing from the common handheld computer gestures to the Simplified Chinese (PRC) standard gestures. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, the Simplified Chinese (PRC) editing gestures will be used. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, the common handheld editing gesture set will be used. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, the common handheld editing gesture set will be used. Users will be able to configure this setting on the Gestures tab in Input Panel Options.
Computer/User	Input Panel	Turn off AutoComplete integration with Input Panel	At least Windows Vista or later	Turns off the integration of application auto complete lists with Tablet PC Input Panel in applications where this behavior is available. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, application auto complete lists will never appear next to Input Panel. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, application auto complete lists will appear next to Input Panel in applications where the functionality is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, application auto complete lists will appear next to Input Panel in applications where the functionality is available. Users will be able to configure this setting on the Settings tab in Input Panel Options.
Computer/User	Input Panel	Turn off password security in Input Panel	At least Windows Vista or later	Adjusts password security settings in Tablet PC Input Panel. These settings include using the on-screen keyboard by default, preventing users from switching to another Input Panel skin (the writing pad or character pad), and not showing

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				what keys are tapped when entering a password. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy and choose ΓÇ£LowΓÇ¥ from the drop-down box, password security is set to ΓÇ£Low.ΓÇ¥ At this setting, all password security settings are turned off. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£Medium-LowΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium-Low.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel displays the cursor and which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£MediumΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is not allowed, and Input Panel displays the cursor and which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose to ΓÇ£Medium-HighΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium-High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£HighΓÇ¥ from the drop-down box, password security is set

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				to ΓÇ£High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is not allowed, and Input Panel does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, password security is set to ΓÇ£Medium-High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, password security is set to ΓÇ£Medium-HighΓÇ¥ by default. At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel does not display the cursor or which keys are tapped. Users will be able to configure this setting on the Advanced tab in Input Panel Options. Caution: If you lower password security settings, people who can see the userΓÇÖs screen might be able to see their passwords.
Computer/User	Input Panel	Turn off tolerant and Z-shaped scratch-out gestures	At least Windows Vista or later	Turns off both the more tolerant scratch-out gestures that were added in Windows Vista and the Z-shaped scratch-out gesture that was available in Microsoft Windows XP Tablet PC Edition. The tolerant gestures let users scratch out ink in Input Panel by using strikethrough and other scratch-out gesture shapes. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy and choose ΓÇ£AllΓÇ¥ from the drop-down menu, no

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				scratch-out gestures will be available in Input Panel. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£Tolerant," users will be able to use the Z-shaped scratch-out gesture that was available in Microsoft Windows XP Tablet PC Edition. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£None,ΓÇ¥ users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will be able to configure this setting on the Gestures tab in Input Panel Options.
User	Instant Search	Custom Instant Search Internet search provider	At least Windows Vista or later	Set up the menu name and URL for the custom Internet search provider. If you enable this setting, the specified menu name and URL will be used for Internet searches. If you disable or not configure this setting, the default Internet search provider will be used.
Computer/User	Internet Communication settings	Turn off handwriting recognition error reporting	At least Windows Vista or later	Turns off the handwriting recognition error reporting tool. The handwriting recognition error reporting tool enables users to report errors encountered in Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows. If you enable this policy,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft. If you disable this policy, Tablet PC users can report handwriting recognition errors to Microsoft. If you do not configure this policy Tablet PC users can report handwriting recognition errors to Microsoft.
User	Internet Communication settings	Turn off Help Experience Improvement Program	At least Windows Vista or later	Specifies whether users can participate in the Help Experience Improvement program. The Help Experience Improvement program collects information about how customers use Windows Help so that Microsoft can improve it. If this setting is enabled, this policy prevents users from participating in the Help Experience Improvement program. If this setting is disabled or not configured, users will be able to turn on the Help Experience Improvement program feature from the Help and Support settings page.
User	Internet Communication settings	Turn off Help Ratings	At least Windows Vista or later	Specifies whether users can provide ratings for Help content. If this setting is enabled, this policy setting prevents ratings controls from being added to Help content. If this setting is disabled or not configured, a rating control will be added to Help topics. Users can use the control to provide feedback on the quality and usefulness of the Help and Support content.
Computer/User	Internet Communication settings	Turn off Windows Movie Maker online Web links	At least Windows Vista or later	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. 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. If you enable this setting, the previously mentioned links to Web sites from

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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	Internet Communication settings	Turn off Windows Online	At least Windows Vista or later	Specifies whether users can search and view content from Windows Online in Help and Support. Windows Online provides the most up-to-date Help content for Windows. If this settings is enabled, users will be prevented from accessing online assistance content from Windows Online. If this setting is disabled or not configured, users will be able to access online assistance if they have a connection to the Internet and have not disabled Windows Online from the Help and Support Options page.
Computer	iSCSI Security	Do not allow changes to initiator CHAP secret	At least Windows Vista or later	If enabled then do not allow the initiator CHAP secret to be changed. If disabled then the initiator CHAP secret may be changed.
Computer	iSCSI Security	Do not allow connections without IPSec	At least Windows Vista or later	If enabled then only those connections that are configured for IPSec may be established. If disabled then connections that are configured for IPSec or connections not configured for IPSec may be established.
Computer	iSCSI Security	Do not allow sessions without mutual CHAP	At least Windows Vista or later	If enabled then only those sessions that are configured for mutual CHAP may be established. If disabled then sessions that are configured for mutual CHAP or sessions not configured for mutual CHAP may be established.
Computer	iSCSI Security	Do not allow sessions without one way CHAP	At least Windows Vista or later	If enabled then only those sessions that are configured for one-way CHAP may be established. If disabled then sessions that are configured for one-way CHAP or sessions not configured for one-way CHAP may be established. Note that if the "Do not allow sessions without mutual CHAP" setting is enabled then that setting overrides this one.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	iSCSI Target Discovery	Do not allow adding new targets via manual configuration	At least Windows Vista or later	If enabled then new targets may not be manually configured by entering the target name and target portal; already discovered targets may be manually configured. If disabled then new and already discovered targets may be manually configured. Note: if enabled there may be cases where this will break VDS.
Computer	iSCSI Target Discovery	Do not allow manual configuration of discovered targets	At least Windows Vista or later	If enabled then discovered targets may not be manually configured. If disabled then discovered targets may be manually configured. Note: if enabled there may be cases where this will break VDS.
Computer	iSCSI Target Discovery	Do not allow manual configuration of iSNS servers	At least Windows Vista or later	If enabled then new iSNS servers may not be added and thus new targets discovered via those iSNS servers; existing iSNS servers may not be removed. If disabled then new iSNS servers may be added and thus new targets discovered via those iSNS servers; existing iSNS servers may be removed.
Computer	iSCSI Target Discovery	Do not allow manual configuration of target portals	At least Windows Vista or later	If enabled then new target portals may not be added and thus new targets discovered on those portals; existing target portals may not be removed. If disabled then new target portals may be added and thus new targets discovered on those portals; existing target portals may be removed.
Computer	Kerberos	Define host name-to-Kerberos realm mappings	At least Windows Vista or later	This policy setting allows you to specify which DNS host names and which DNS suffixes are mapped to a Kerberos realm. If you enable this policy setting, you can view and change the list of DNS host names and DNS suffixes mapped to a Kerberos realm as defined by Group Policy. To view the list of mappings, enable the policy setting and then click the Show button. To add a mapping, enable the policy setting, note the syntax, click the Show button, click the Add button, and then type a realm name in the Value Name and the list of DNS host names and DNS suffixes in the Value using the syntax format. To remove a mapping, click its

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				entry, and then click the Remove button. To edit a mapping, remove the current entry from the list and add a new one with different parameters. If you disable this policy setting, the host name-to-Kerberos realm mappings list defined by Group Policy is deleted. If you do not configure this policy setting, the system will use the host name-to-Kerberos realm mappings that are defined in the local registry, if they exist.
Computer	Kerberos	Define interoperable Kerberos V5 realm settings	At least Windows Vista or later	This policy setting configures the Kerberos client so that it can authenticate with interoperable Kerberos V5 realms, as defined by this policy setting. If you enable this policy setting, you can view and change the list of interoperable Kerberos V5 realms and their settings. To view the list of interoperable Kerberos V5 realms, enable the policy setting and then click the Show button. To add an interoperable Kerberos V5 realm, enable the policy setting, note the syntax, click the Show button, click the Add button, and then type the interoperable Kerberos V5 realm name in the Value Name field, and type the definition of settings using the syntax format in the Value field. To remove an interoperable Kerberos V5 realm, click its entry, and then click the Remove button. To edit a mapping, remove the current entry from the list and add a new one with different parameters. If you disable this policy setting, the interoperable Kerberos V5 realm settings defined by Group Policy are deleted. If you do not configure this policy setting, the system will use the interoperable Kerberos V5 realm settings that are defined in the local registry, if they exist.
Computer	Kerberos	Require strict KDC validation	At least Windows Vista or later	This policy setting controls the Kerberos client's behavior in validating the KDC certificate. If you enable this policy setting, the Kerberos client requires that the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				KDC's X.509 certificate contains the KDC key purpose object identifier in the Extended Key Usage (EKU) extensions, and that the KDC's X.509 certificate contains a dNSName subjectAltName (SAN) extension that matches the DNS name of the domain. If the computer is joined to a domain, the Kerberos client requires that the KDC's X.509 certificate must be signed by a Certificate Authority (CA) in the NTAUTH store. If the computer is not joined to a domain, the Kerberos client allows the root CA certificate on the smart card to be used in the path validation of the KDC's X.509 certificate. If you disable or do not configure this policy setting, the Kerberos client will require only that the KDC certificate contain the Server Authentication purpose object identifier in the EKU extensions.
Computer	Link-Layer Topology Discovery	Turn on Mapper I/O (LLTDIO) driver	At least Windows Vista or later	This policy setting turns on the Mapper I/O network protocol driver. LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis. If you enable this policy setting, additional options are available to fine-tune your selection. You may choose the "Allow operation while in domain" option to allow LLTDIO to operate on a network interface that's connected to a managed network. On the other hand, if a network interface is connected to an unmanaged network, you may choose the "Allow operation while in public network" and "Prohibit operation while in private network" options instead. If you disable this policy setting, LLTDIO will not participate in any of the activities described above. If you do not configure this policy setting, LLTDIO will be enabled with all options turned on at all times.
Computer	Link-Layer Topology	Turn on Responder (RSPNDR)	At least Windows Vista or later	This policy setting turns on the Responder network protocol driver. The

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Discovery	driver		Responder allows a computer to participate in Link Layer Topology Discovery requests so that it can be discovered and located on the network. It also allows a computer to participate in Quality-of-Service activities such as bandwidth estimation and network health analysis. If you enable this policy setting, additional options are available to fine-tune your selection. You may choose the "Allow operation while in domain" option to allow the Responder to operate on a network interface that's connected to a managed network. On the other hand, if a network interface is connected to an unmanaged network, you may choose the "Allow operation while in public network" and "Prohibit operation while in private network" options instead. If you disable this policy setting, the Responder will not participate in any of the activities described above. If you do not configure this policy setting, the Responder will be enabled with all options turned on at all times.
Computer/User	Locale Services	Disallow changing of geographic location	At least Windows Vista or later	This policy prevents users from changing their user geographical location (GeoID). If this policy is Enabled, then the user cannot change their geographical location (GeoID) If the policy is Disabled or Not Configured, then the user may select any GeoID. If this policy is Enabled at the Machine level, then it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer/User	Locale Services	Disallow selection of Custom Locales	At least Windows Vista or later	This policy prevents a user from selecting a supplemental custom locale as their user locale. The user is restricted to the set of locales that shipped with the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				operating system. Note that this does not affect the selection of replacement locales. To prevent the selection of replacement locales, adjust the permissions of the %windir%\Globalization directory to prevent the installation of locales by unauthorized users. Note that "Restrict user locales" can also be enabled to disallow selection of a custom locale, even if this policy is not configured. If this policy is Enabled, then the user cannot select a custom locale as their user locale, but they may still select a replacement locale if one is installed. If the policy is Disabled or Not Configured, then the user may select a custom locale as their user locale. If this policy is Enabled at the Machine level, it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer/User	Locale Services	Disallow user override of locale settings	At least Windows Vista or later	This policy prevents the user from customizing their locale by changing their user overrides. Any existing overrides in place when this policy is enabled will be frozen. To remove existing user override, first reset the user(s) values to the defaults and then apply this policy. When this policy is enabled, users may still choose alternate locales installed on the system unless prevented by other policies, however they will be unable to customize those choices. If this policy is Enabled, then the user cannot customize their user locale with user overrides. If this policy is Disabled or Not Configured, then the user can customize their user locale overrides. If this policy is Enabled at the Machine level, then it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer	Locale Services	Restrict system locales	At least Windows Vista or later	This policy restricts the permitted system locales to the specified list. If the list is empty, it locks the system locale to its current value. This policy does not change the existing system locale; however, the next time that an admin attempts to change the machine's system locale they will be restricted to the specified list. The locale list is specified using language names, separated by a semi-colon (;). For example, en-US is English (United States). Specifying "en-US;en-CA" would restrict the system locale to English (United States) and English (Canada). If this policy is Enabled, then administrators may select a system locale only from the specified system locale list. If this policy is Disabled or Not Configured, then administrators may select any system locale shipped with the operating system.
Computer/User	Locale Services	Restrict user locales	At least Windows Vista or later	This policy restricts users on a machine to the specified list of user locales. If the list is empty, it locks all user locales to their current values. This policy does not change existing user locale settings; however, the next time a user attempts to change their user locale, their choices will be restricted to locales in this list. To set this policy on a per-user basis, make sure that the per-machine policy is set to not configured. The locale list is specified using language tags, separated by a semicolon (;). For example, en-US is English (United States). Specifying "en-CA;fr-CA" would restrict the system locale to English (Canada) and French (Canada). If this policy is enabled, then only locales in the enabled list may be selected by users. If this policy is disabled or not configured, then users may

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				select any locale installed on the machine, unless restricted by the "Disallow selection of Custom Locales" policy. If this policy is enabled at the machine level, it cannot be disabled by a per-user policy. If this policy is disabled at the machine level, then the per-user policy will be ignored. If this policy is not configured at the machine level, then restrictions will be based on per-user policies. Note that if an administrator has enabled the "Disallow selection of custom locales" policy, then users will be prevented from selecting supplemental custom locales, even if they are in the acceptable locale list for this policy.
Computer	Logon	Hide entry points for Fast User Switching	At least Windows Vista or later	By enabling the policy, Administrators hide the Switch user button in the Logon UI, the Start menu and the Task Manager.
Computer	logon:Logon	Assign a default domain for logon	At least Windows Vista or later	This policy setting specifies a default logon domain which may be a different domain than the machine joined domain. Without this policy, at logon, if a user does not specify a domain for logon, the domain to which the machine belongs is assumed as the default domain. For example if the machine belongs to the Fabrikam domain, the default domain for user logon is Fabrikam. If you enable this policy setting, the a default logon domain will be set to the specified domain which may not be the machine joined domain. If you disable or do not configure this policy setting, the default logon domain will always be set to the machine joined domain.
Computer	logon:Logon	Exclude credential providers	At least Windows Vista or later	This policy setting allows the administrator to exclude the specified credential providers from use during authentication. Note: credential providers are used to process and validate user credentials during logon or when authentication is required. Windows Vista provides two default credential providers: Password and

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Smart Card. An administrator can install additional credential providers for different sets of credentials (for example, to support biometric authentication). If you enable this policy, an administrator can specify the CLSIDs of the credential providers to exclude from the set of installed credential providers available for authentication purposes. If you disable or do not configure this policy, all installed credential providers will be available for authentication purposes.
Computer	Microsoft Peer-to-Peer Networking Services	Disable password strength validation for Peer Grouping	At least Windows Vista or later	By default, when a Peer Group is created that allows for password-authentication (or the password for such a Group is changed), Peer Grouping validates that the password meets the password complexity requirements for the local system. Thus, it will not allow any passwords to be used for a Peer Group that are weaker than what would be allowed for a login password. This setting controls this validation behavior. If set to 1, then this validation will not be performed and any password will be allowed. If set to 0, the validation will be performed.
Computer	Microsoft Support Diagnostic Tool	Microsoft Support Diagnostic Tool: Configure execution level	At least Windows Vista or later	Determines the execution level for Microsoft Support Diagnostic Tool. Microsoft Support Diagnostic Tool (MSDT) gathers diagnostic data for analysis by support professionals. If you enable this policy setting, administrators will be able to use MSDT to collect and send diagnostic data to a support professional to resolve a problem. If you disable this policy, MSDT will not be able to gather diagnostic data. If you do not configure this policy setting, MSDT will be enabled by default. This policy setting takes effect only if the diagnostics-wide scenario execution policy is not configured. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service (DPS) is in the running state. When the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Microsoft Support Diagnostic Tool	Microsoft Support Diagnostic Tool: Restrict tool download	At least Windows Vista or later	Restricts the tool download policy for Microsoft Support Diagnostic Tool. Microsoft Support Diagnostic Tool (MSDT) gathers diagnostic data for analysis by support professionals. For some problems, MSDT may prompt the user to download additional tools for troubleshooting. These tools are required to completely troubleshoot the problem. If tool download is restricted, it may not be possible to find the root cause of the problem. If you enable this policy setting for remote troubleshooting, MSDT will prompt the user to download additional tools to diagnose problems on remote computers only. If the setting is enabled for local and remote troubleshooting, MSDT will always prompt for additional tool download. If you disable this policy, MSDT will never download tools, and will be unable to diagnose problems on remote computers. If you do not configure this policy setting, MSDT will prompt the user before downloading any additional tools. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when MSDT is enabled. This policy setting will only take effect when the Diagnostic Policy Service (DPS) is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
User	mmc:MMC_RESTRICT	Failover Clusters Manager	At least Windows Vista or later	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

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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	mmc:MMC_RESTRICT	TPM Management	At least Windows Vista or later	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

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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	mmc:MMC_RESTRICT	Windows Firewall with Advanced Security	At least Windows Vista or later	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.
Computer/User	Network Projector	Turn off Connect to a Network Projector	At least Windows Vista or later	Disables the Connect to a Network Projector wizard so that users cannot connect to a network projector. If you enable this policy, users cannot use the Connect to a Network Projector wizard to connect to a projector. If you disable this policy or do not configure it, users can run the Connect to a Network Projector wizard to connect to a projector.
User	Network Projector	Turn off Connect to a Network	At least Windows Vista or later	Disables the Connect to a Network Projector wizard so that users cannot connect

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		Projector		to a network projector. If you enable this policy, users cannot use the Connect to a Network Projector wizard to connect to a projector. If you disable this policy or do not configure it, users can run the Connect to a Network Projector wizard to connect to a projector.
User	Network Sharing	Prevent users from sharing files within their profile.	At least Windows Vista or later	By default users are allowed to share files within their profile to other users on their network once an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile. If you enable this policy, users will not be able to share files within their profile using the sharing wizard. Also, the sharing wizard will not create a share at %root%\users and can only be used to create SMB shares on folders. If you disable or donΓÇÖt configure this policy, then users will be able to share files out of their user profile once an administrator has opted in the computer.
Computer	Notification Settings	Critical Battery Notification Action	At least Windows Vista or later	Specifies the action that Windows takes when battery capacity reaches the critical battery notification level. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Critical Battery Notification Level	At least Windows Vista or later	Specifies the percentage of battery capacity remaining that triggers the critical battery notification action. If you enable this policy, you must enter a numeric value (percentage) to set the battery level that triggers the critical notification. To set the action that is triggered, see the "Critical Battery Notification Action" policy setting. If you disable this policy setting or do not configure it, users can see and change this setting.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Notification Settings	Low Battery Notification Action	At least Windows Vista or later	Specifies the action that Windows takes when battery capacity reaches the low battery notification level. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Low Battery Notification Level	At least Windows Vista or later	Specifies the percentage of battery capacity remaining that triggers the low battery notification action. If you enable this policy, you must enter a numeric value (percentage) to set the battery level that triggers the low notification. To set the action that is triggered, see the "Low Battery Notification Action" policy setting. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Turn Off Low Battery User Notification	At least Windows Vista or later	Disables a user notification when the battery capacity remaining equals the low battery notification level. If you enable this policy, Windows will not show a notification when the battery capacity remaining equals the low battery notification level. To configure the low battery notification level, see the "Low Battery Notification Level" policy setting. The notification will only be shown if the "Low Battery Notification Action" policy setting is configured to "No Action". If you do not configure this policy setting, users can see and change this setting.
Computer	NTFS Filesystem	Selectively allow the evaluation of a symbolic link.	At least Windows Vista or later	Symbolic links can introduce vulnerabilities in certain applications. To mitigate this issue, you can selectively enable or disable the evaluation of these types of symbolic links: Local Link to a Local Target Local Link to a Remote Target Remote Link to Remote Target Remote Link to Local Target For further information please refer to the Windows Help section NOTE: If this policy is

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Disabled or Not Configured, local administrators may select the types of symbolic links to be evaluated.
Computer	Offline Files	Configure slow-link mode	At least Windows Vista or later	This policy setting allows you to enable and configure the slow-link mode of Offline Files. When Offline Files is operating in slow-link mode, all file requests are satisfied from the Offline Files cache, just as when the user is working offline. However, the user can manually initiate synchronization on demand. Once the synchronization completes, the system continues to operate in the slow-link mode until the user transitions the share to online mode. If you enable this policy setting, Offline Files will operate in slow-link mode if the end-to-end network throughput between the client and the server is below the throughput threshold parameter, or if the network latency is above the latency threshold parameter. You can configure slow-link mode by specifying thresholds for Throughput (bits per second) and Latency (in milliseconds) for specific UNC paths. You can specify one or both threshold parameters. When a share is transitioned to slow-link mode, the user can force the share to transition to online mode. However, the system periodically checks to see if a connection to a server is slow. If the connection is slow then the share will again be transitioned to slow-link mode. Note: You can use wildcards (*) for specifying UNC paths. If you disable or do not configuring this policy setting, Offline Files will not transition to slow-link mode.
Computer	Offline Files	Turn on economical application of administratively assigned Offline Files	At least Windows Vista or later	This policy setting allows you to turn on economical application of administratively assigned Offline Files. If you enable this policy setting, only new files and folders in administratively assigned folders are synchronized at logon. Files and folders that are already available offline are skipped and are synchronized later. If you

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				disable or do not configure this policy setting, all administratively assigned folders are synchronized at logon.
Computer	Online Assistance	Turn off Active Help	At least Windows Vista or later	Specifies whether active content links in trusted assistance content are rendered. By default, the Help viewer renders trusted assistance content with active elements such as ShellExecute links and Guided Help links. If you enable this policy, such links are not rendered. The text is displayed but there are no clickable links for these elements. If you Disable or do not configure this setting, the default behavior (Help viewer renders trusted assistance content with active elements) applies.
Computer	Online Assistance	Turn off Untrusted Content	At least Windows Vista or later	Specifies whether untrusted content is rendered. By default, the Help viewer renders untrusted assistance content pages with the exception of active links. Active links, such as ShellExecute and Guided Help, are rendered as text and are not clickable. If you enable this policy, untrusted content is not rendered at all, and a navigation error page is displayed to the user. If you Disable or do not configure this setting, the default behavior (untrusted content is rendered with the exception of active links, which are rendered as text only) applies.
Computer	Parental Controls	Make Parental Controls control panel visible on a Domain	At least Windows Vista or later	Configure the Parental Controls feature. If you turn on this setting, the Parental Controls control panel will be visible on a domain joined computer. If you turn off or do not configure this setting, the Parental Controls control panel will not be visible on a domain joined computer.
Computer/User	Pen Flicks Learning	Prevent Flicks Learning Mode	At least Windows Vista or later	Makes pen flicks learning mode unavailable. If you enable this policy, pen flicks are still available but learning mode is not. Pen flicks are off by default and can be turned on system-wide, but cannot be restricted to learning mode applications.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				This means that the pen flicks training triggers in Internet Explorer are disabled and that the pen flicks notification will never be displayed. However, pen flicks, the pen flicks tray icon and pen flicks training (that can be accessed through CPL) are still available. Conceptually this policy is a subset of the Disable pen flicks policy. If you disable or do not configure this policy, all the features described above will be available.
Computer/User	Pen UX Behaviors	Prevent flicks	At least Windows Vista or later	Makes pen flicks and all related features unavailable. If you enable this policy, pen flicks and all related features are unavailable. This includes: pen flicks themselves, pen flicks training, pen flicks training triggers in Internet Explorer, the pen flicks notification and the pen flicks tray icon. If you disable or do not configure this policy, pen flicks and related features are available.
Computer/User	Performance Control Panel	Turn off access to the OEM and Microsoft branding section	At least Windows Vista or later	Removes access to the performance center control panel OEM and Microsoft branding links. If you enable this setting, the OEM and Microsoft web links within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel OEM and Microsoft branding links will be displayed to the user.
Computer/User	Performance Control Panel	Turn off access to the performance center core section	At least Windows Vista or later	Removes access to the performance center control panel page. If you enable this setting, some settings within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel core section will be displayed to the user.
Computer/User	Performance Control	Turn off access to the solutions to	At least Windows Vista or later	Removes access to the performance center control panel solutions to

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Panel	performance problems section		performance problems. If you enable this setting, the solutions and issue section within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel solutions to performance problems section will be displayed to the user.
Computer	Power Management	Select an Active Power Plan	At least Windows Vista or later	Specifies the active power plan from a list of default Windows power plans. To specify a custom power plan, use the Custom Active Power Plan setting. To enable this setting, select "Enabled" and choose a power plan from the Active Power Plan list. If you disable this policy or do not configure it, users can see and change this setting.
Computer	Power Management	Specify a Custom Active Power Plan	At least Windows Vista or later	Specifies an active power plan when you enter a power planΓÇÖs GUID. Retrieve the custom power plan GUID by using powercfg, the power configuration command line tool. Enter the GUID using the following format: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX. (For example, enter 103eea6e-9fcd-4544-a713-c282d8e50083.) To specify a plan for the list of default Windows power plans, use the Active Power Plan policy setting. If you disable this policy or do not configure it, users can see and change this setting.
Computer/User	Presentation Settings	Turn off Windows presentation settings	At least Windows Vista or later	This policy setting turns off Windows presentation settings. If you enable this policy setting, Windows presentation settings cannot be invoked. If you disable this policy setting, Windows presentation settings can be invoked. The presentation settings icon will be displayed in the notification area. This will give users a quick and easy way to configure their system settings before a presentation to block system notifications and screen blanking, adjust speaker

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				volume, and apply a custom background image. Note: Users will be able to customize their system settings for presentations in Windows Mobility Center. If you do not configure this policy setting, Windows presentation settings can be invoked.
Computer/User	Previous Versions	Hide previous versions list for local files	At least Windows Vista or later	This policy setting lets you hide the list or restore of previous versions of files that are on local disks. The previous versions could come from the on-disk shadow copies or from backup media. If this policy setting is enabled, users will not be able to list or restore previous versions of files on local disks. If this policy setting is disabled, users will be able to list and restore previous versions of files on local disks. If this policy setting is not configured, it will default to disabled.
Computer/User	Previous Versions	Hide previous versions list for remote files	At least Windows Vista or later	This policy setting lets you hide the list or restore of previous versions of files that are on file shares. The previous versions could come from the on-disk shadow copies on the file share. If this policy setting is enabled, users will not be able to list or restore previous versions of files on file shares. If this policy setting is disabled, users will be able to list and restore previous versions of files on file shares. If this policy setting is not configured, it will default to disabled.
Computer/User	Previous Versions	Hide previous versions of files on backup location	At least Windows Vista or later	This setting lets you hide entries in the list of previous versions of a file in which the previous version is located on backup media. Previous versions can come from the on-disk shadow copies or the backup media. If this setting is enabled, users will not see any previous versions corresponding to backup copies, and will only see previous versions corresponding to on-disk shadow copies. If this setting is disabled, users will be able to see previous versions corresponding to backup copies as well as previous versions corresponding to on-disk shadow copies. If

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this setting is not configured, it will default to disabled.
Computer/User	Previous Versions	Prevent restoring local previous versions	At least Windows Vista or later	This setting lets you suppress the Restore button in the previous versions property page when the user has selected a previous version of a local file. If this setting is enabled, then the Restore button will be disabled when the user selects a previous version corresponding to a local file. If this setting is disabled, then the Restore button will remain active for a previous version corresponding to a local file. If the user clicks the Restore button, then Windows will attempt to restore the file from the local disk. If this setting is not configured, it will default to disabled - the Restore button will be active when the previous version is of a local file.
Computer/User	Previous Versions	Prevent restoring previous versions from backups	At least Windows Vista or later	This setting lets you suppress the Restore button in the previous versions property page when the user has selected a previous version of a local file, in which the previous version is stored on a backup. If this setting is enabled, then the Restore button will be disabled when the user selects a previous version corresponding to a backup. If this setting is disabled, then the Restore button will remain active for a previous version corresponding to a backup. If the user clicks the Restore button, then Windows will attempt to restore the file from the backup media. If this setting is not configured, it will default to disabled - the Restore button will be active when the previous version is of a local file and stored on the backup.
Computer/User	Previous Versions	Prevent restoring remote previous versions	At least Windows Vista or later	This setting lets you suppress the Restore button in the previous versions property page when the user has selected a previous version of a file on a file share. If this setting is enabled, then the Restore button will be disabled when the user selects a previous version corresponding to a file on a file share. If this

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting is disabled, then the Restore button will remain active for a previous version corresponding to a file on a file share. If the user clicks the Restore button, then Windows will attempt to restore the file from the file share. If this setting is not configured, it will default to disabled - the Restore button will be active when the previous version is of a file on a file share.
Computer	Printers	Add Printer wizard - Network scan page (Managed network)	At least Windows Vista or later	This policy sets the maximum number of printers (of each type) that the Add Printer wizard will display on a computer on a managed network (when the computer is able to reach a domain controller, e.g. a domain-joined laptop on a corporate network.) If this setting is disabled, the network scan page will not be displayed. If this setting is not configured, the Add Printer wizard will display the default number of printers of each type: Directory printers: 20 TCP/IP printers: 0 Web Services Printers: 0 Bluetooth printers: 10 If you would like to not display printers of a certain type, enable this policy and set the number of printers to display to 0.
Computer	Printers	Always render print jobs on the server	At least Windows Vista or later	When printing through a print server, determines whether the print spooler on the client will process print jobs itself, or pass them on to the server to do the work. This policy setting only effects printing to a Windows print server. If you enable this policy setting on a client machine, the client spooler will not process print jobs before sending them to the print server. This decreases the workload on the client at the expense of increasing the load on the server. If you disable this policy setting on a client machine, the client itself will process print jobs into printer device commands. These commands will then be sent to the print server, and the server will simply pass the commands to the printer. This increases the workload

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				of the client while decreasing the load on the server. If you do not enable this policy setting, the behavior is the same as disabling it. Note: This policy does not determine whether offline printing will be available to the client. The client print spooler can always queue print jobs when not connected to the print server. Upon reconnecting to the server, the client will submit any pending print jobs. Note: Some printer drivers require a custom print processor. In some cases the custom print processor may not be installed on the client machine, such as when the print server does not support transferring print processors during point-and-print. In the case of a print processor mismatch, the client spooler will always send jobs to the print server for rendering. Disabling the above policy setting does not override this behavior. Note: In cases where the client print driver does not match the server print driver (mismatched connection), the client will always process the print job, regardless of the setting of this policy.
User	Printers	Only use Package Point and print	At least Windows Vista or later	This policy restricts clients computers to use package point and print only. If this setting is enabled, users will only be able to point and print to printers that use package-aware drivers. When using package point and print, client computers will check the driver signature of all drivers that are downloaded from print servers. If this setting is disabled, or not configured, users will not be restricted to package-aware point and print only.
User	Printers	Package Point and print - Approved servers	At least Windows Vista or later	Restricts package point and print to approved servers. If this setting is enabled, users will only be able to package point and print to print servers approved by the network administrator. When using package point and print, client computers will check the driver signature of all drivers that are downloaded from print servers. If

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this setting is disabled, or not configured, package point and print will not be restricted to specific print servers.
User	Programs	Hide "Get Programs" page	At least Windows Vista or later	Prevents users from viewing or installing published programs from the network. This setting prevents users from accessing the "Get Programs" page from the Programs Control Panel in Category View, Programs and Features in Classic View and the "Install a program from the netowrk" task. The "Get Programs" page 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 of their availability, to recommend their use, or to enable users to install them without having to search for installation files. If this setting is enabled, users cannot view the programs that have been published by the system administrator, and they cannot use the "Get Programs" page to install published programs. Enabling this feature does not prevent users from installing programs by using other methods. Users will still be able to view and installed assigned (partially installed) programs that are offered on the desktop or on the Start menu. If this setting is disabled or is not configured, the "Install a program from the network" task to the "Get Programs" page will be available to all users. Note: If the "Hide Programs Control Panel" setting is enabled, this setting is ignored.
User	Programs	Hide "Installed Updates" page	At least Windows Vista or later	This setting prevents users from accessing "Installed Updates" page from the "View installed updates" task. "Installed Updates" allows users to view and uninstall updates currently installed on the computer. The updates are often

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				downloaded directly from Windows Update or from various program publishers. If this setting is disabled or not configured, the "View installed updates" task and the "Installed Updates" page will be available to all users. This setting does not prevent users from using other tools and methods to install or uninstall programs.
User	Programs	Hide "Programs and Features" page	At least Windows Vista or later	This setting prevents users from accessing "Programs and Features" to view, uninstall, change, or repair programs that are currently installed on the computer. If this setting is disabled or not configured, "Programs and Features" will be available to all users. This setting does not prevent users from using other tools and methods to view or uninstall programs. It also does not prevent users from linking to related Programs Control Panel Features including Windows Features, Get Programs, or Windows Marketplace.
User	Programs	Hide "Set Program Access and Computer Defaults" page	At least Windows Vista or later	This setting removes the Set Program Access and Defaults page from the Programs Control Panel. As a result, users cannot view or change the associated page. The Set Program Access and Computer Defaults page allows administrators to specify default programs for certain activities, such as Web browsing or sending e-mail, as well as specify the programs that are accessible from the Start menu, desktop, and other locations. If this setting is disabled or not configured, 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 Default Programs icon from appearing on the Start menu.
User	Programs	Hide "Windows Features"	At least Windows Vista or later	This setting prevents users from accessing the "Turn Windows features on or off" task from the Programs Control Panel in Category View, Programs and Features

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				in Classic View, and Get Programs. As a result, users cannot view, enable, or disable various Windows features and services. If this setting is disabled or is not configured, the "Turn Windows features on or off" task will be available to all users. This setting does not prevent users from using other tools and methods to configure services or enable or disable program components.
User	Programs	Hide "Windows Marketplace"	At least Windows Vista or later	This setting prevents users from access the "Get new programs from Windows Marketplace" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs. Windows Marketplace allows users to purchase and/or download various programs to their computer for installation. Enabling this feature does not prevent users from navigating to Windows Marketplace using other methods. If this feature is disabled or is not configured, the "Get new programs from Windows Marketplace" task link will be available to all users. Note: If the "Hide Programs control Panel" setting is enabled, this setting is ignored.
User	Programs	Hide the Programs Control Panel	At least Windows Vista or later	This setting prevents users from using the Programs Control Panel in Category View and Programs and Features in Classic View. The Programs Control Panel allows users to uninstall, change, and repair programs, enable and disable Windows Features, set program defaults, view installed updates, and purchase software from Windows Marketplace. Programs published or assigned to the user by the system administrator also appear in the Programs Control Panel. If this setting is disabled or not configured, the Programs Control Panel in Category View and Programs and Features in Classic View will be available to all users. When enabled, this setting takes precedence over the other settings in this folder.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				This setting does not prevent users from using other tools and methods to install or uninstall programs.
Computer	Regional and Language Options	Force selected machine UI language to overwrite the user UI language	At least Windows Vista or later	This is a setting for computers with more than one UI language installed. If you enable this setting, the UI language of Windows menus and dialogs language for systems with more than one language will follow the language specified by the administrator as the machine UI languages. The user UI language will be ignored.
User	Regional and Language Options	Hide Regional and Language Options administrative options	At least Windows Vista or later	This policy removes the Administrative options from the Regional and Language Options control panel. Administrative options include interfaces for setting system locale and copying settings to the default user. This policy does not, however, prevent an administrator or another application from changing these values programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not be able to see the Administrative options. If the policy is Disabled or Not Configured, then the user will see the Administrative options. Note that even if a user can see the Administrative options, other policies may prevent them from modifying the values.
User	Regional and Language Options	Hide the geographic location option	At least Windows Vista or later	This policy removes the option to change the user's geographical location (GeoID) from the Language and Regional Options control panel. This does not, however, prevent the user or an application from changing the GeoID programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the option to change the user geographical location (GeoID). If the policy is Disabled or Not Configured, then the user will see the option for changing the user location (GeoID). Note that even if a user can see

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the GeoID Option, the "Disallow changing of geographical location" option may prevent them from actually changing their current geographical location.
User	Regional and Language Options	Hide the select language group options	At least Windows Vista or later	This policy removes the option to change the user's menus and dialogs (UI) language from the Language and Regional Options control panel. This does not, however, prevent the user or an application from changing the UI language programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the option for changing the UI language. If the policy is Disabled or Not Configured, then the user will see the option for changing the UI language. Note that even if a user can see the option to change the UI language, other policies may prevent them from changing their UI language.
User	Regional and Language Options	Hide user locale selection and customization options	At least Windows Vista or later	This policy removes the regional formats interface from the Regional and Language Options control panel. This does not, however, prevent the user or an application from changing their user locale or user overrides programmatically. The policy is only used to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the regional formats options. If the policy is Disabled or Not Enabled, then the user will see the regional formats options for changing and customizing the user locale.
Computer/User	Regional and Language Options	Restricts the Machine UI languages Windows uses for all logged users	At least Windows Vista or later	This is a setting for computers with more than one UI language installed. If you enable this setting the UI language of Windows menus and dialogs language for systems with more than one language is restricted to the specific language. If the specified language is not installed on the target computer or the policy is disabled, the language selection defaults to the language selected by the local

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				administrator.
Computer	Remote Assistance	Allow only Vista or later connections	At least Windows Vista or later	This policy setting enables Remote Assistance invitations to be generated with improved encryption so that only computers running this version (or later versions) of the operating system can connect. This setting does not affect Remote Assistance connections that are initiated by instant messaging contacts or the unsolicited Offer Remote Assistance. If you enable this policy setting, only computers running this version (or later versions) of the operating system can connect to this computer. If you disable this policy setting, computers running this version and a previous version of the operating system can connect to this computer. If you do not configure this setting, computers running this version and a previous version of the operating system can connect to this computer.
Computer	Remote Assistance	Customize Warning Messages	At least Windows Vista or later	The "Display warning message before sharing control" policy setting allows you to specify a custom message to display before a user shares control of his or her computer. The "Display warning message before connecting" policy setting allows you to specify a custom message to display before a user allows a connection to his or her computer. If you enable this policy setting, the warning message you specify will override the default message that is seen by the novice. If you disable this policy setting, the user will see the default warning message. If you do not configure this setting, the user will see the default warning message.
Computer	Remote Assistance	Turn on bandwidth optimization	At least Windows Vista or later	This policy setting allows you to improve performance in low bandwidth scenarios. This setting is incrementally scaled from "No optimization" to "Full optimization". Each incremental setting includes the previous optimization setting. For example: "Turn off background" will include the following optimizations: No full window drag

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Turn off background "Full optimization (no 8-bit color)" will include the following optimizations: Use 8-bit color No full window drag Turn off background If you enable this policy setting, bandwidth optimization will occur at the level specified. If you disable this policy setting, application-based settings will be used. If you do not configure this policy setting, application-based settings will be used.
Computer	Remote Assistance	Turn on session logging	At least Windows Vista or later	This policy setting allows you to turn logging on or off. Log files are located in the user's Documents folder under Remote Assistance. If you enable this policy setting, log files will be generated. If you disable this policy setting, log files will not be generated. If you do not configure this setting, application-based settings will be used.
Computer/User	Removable Storage Access	All Removable Storage classes: Deny all access	At least Windows Vista or later	Configure access to all removable storage classes. This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class. If you enable this policy setting, no access is allowed to any removable storage class. If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.
Computer	Removable Storage Access	All Removable Storage: Allow direct access in remote sessions	At least Windows Vista or later	This policy setting grants normal users direct access to removable storage devices in remote sessions. If you enable this policy setting, remote users will be able to open direct handles to removable storage devices in remote sessions. If you disable or do not configure this policy setting, remote users will not be able to open direct handles to removable storage devices in remote sessions.
Computer/User	Removable Storage Access	CD and DVD: Deny read access	At least Windows Vista or later	This policy setting denies read access to the CD and DVD removable storage class. If you enable this policy setting, read access will be denied to this

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	CD and DVD: Deny write access	At least Windows Vista or later	This policy setting denies write access to the CD and DVD removable storage class. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Custom Classes: Deny read access	At least Windows Vista or later	This policy setting denies read access to custom removable storage classes. If you enable this policy setting, read access will be denied to these removable storage classes. If you disable or do not configure this policy setting, read access will be allowed to these removable storage classes.
Computer/User	Removable Storage Access	Custom Classes: Deny write access	At least Windows Vista or later	This policy setting denies write access to custom removable storage classes. If you enable this policy setting, write access will be denied to these removable storage classes. If you disable or do not configure this policy setting, write access will be allowed to these removable storage classes.
Computer/User	Removable Storage Access	Floppy Drives: Deny read access	At least Windows Vista or later	This policy setting denies read access to the Floppy Drives removable storage class, including USB Floppy Drives. If you enable this policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Floppy Drives: Deny write access	At least Windows Vista or later	This policy setting denies write access to the Floppy Drives removable storage class, including USB Floppy Drives. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer/User	Removable Storage	Removable Disks: Deny read	At least Windows Vista or later	This policy setting denies read access to removable disks. If you enable this

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Access	access		policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Removable Disks: Deny write access	At least Windows Vista or later	This policy setting denies write access to removable disks. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Tape Drives: Deny read access	At least Windows Vista or later	This policy setting denies read access to the Tape Drive removable storage class. If you enable this policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Tape Drives: Deny write access	At least Windows Vista or later	This policy setting denies write access to the Tape Drive removable storage class. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Time (in seconds) to force reboot	At least Windows Vista or later	Set the amount of time (in seconds) that the system will wait to reboot in order to enforce a change in access rights to removable storage devices. If you enable this setting, set the amount of seconds you want the system to wait until a reboot. If you disable or do not configure this setting, the system will not force a reboot. NOTE: If no reboot is forced, the access right will not take effect until the system is restarted.
Computer/User	Removable Storage Access	WPD Devices: Deny read access	At least Windows Vista or later	This policy setting denies read access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices. If you enable

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	WPD Devices: Deny write access	At least Windows Vista or later	This policy setting denies write access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer	Scripts	Allow logon scripts when NetBIOS or WINS is disabled	At least Windows Vista or later	This policy setting allows user logon scripts to run when the logon cross-forest, DNS suffixes are not configured and NetBIOS or WINS is disabled. This policy setting affects all user accounts interactively logging on to the computer. If you enable this policy setting, user logon scripts will run if NetBIOS or WINS is disabled during cross-forest logons without the DNS suffixes being configured. If you disable or do not configure this policy setting, no user account cross-forest, interactive logging will be able to run logon scripts if NetBIOS or WINS is disabled and the DNS suffixes are not configured.
Computer	Search	Allow indexing of encrypted files	At least Windows Vista or later	This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing disregards encryption flags (access restrictions still apply though) and will attempt to decrypt and index the content. If you disable this policy setting, the search service components (including the ones from 3rd parties) are expected not to index encrypted items such as emails or files, and to avoid indexing encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				control panel, will be respected. Note: By default, the control panel setting is set to not index encrypted content. Note: Enabling this policy setting will not allow encrypted files in the local file system to be indexed.
Computer	Search	Allow using diacritics	At least Windows Vista or later	This policy setting allows words that contain diacritic characters to be treated as separate words. If you enable this policy setting, words that only differ in diacritics are treated as different words. If you disable this policy setting, words with diacritics and words without diacritics are treated as identical words. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through the control panel, will be respected. Note: By default, the control panel setting is set to treat words that differ only because of diacritics as the same word.
Computer	Search	Indexer data location	At least Windows Vista or later	Store indexer database in this directory. This directory must be located on a local fixed drive.
Computer	Search	Prevent displaying advanced indexing options in the Control Panel	At least Windows Vista or later	If enabled, Search and Indexing Options control panel applet does not allow opening the advanced options dialog. Otherwise it can be opened. This policy setting is not configured by default.
Computer	Search	Prevent indexing e-mail attachments	At least Windows Vista or later	Enable this policy setting to prevent the indexing of the content of e-mail attachments. If enabled, indexing service components (including the ones from 3rd parties) are expected not to index e-mail attachments. Consider enabling this policy setting if you are concerned about the security or indexing performance of 3rd party document filters (iFilters). This policy setting is disabled by default.
Computer	Search	Prevent indexing files in Offline Files cache	At least Windows Vista or later	If enabled, files on network shares made available offline are not indexed. Otherwise they are indexed. This policy setting is not configured by default.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Search	Prevent indexing Microsoft Office Outlook	At least Windows Vista or later	Enable this policy setting to prevent indexing of any Microsoft Outlook items. The default behavior is to automatically index Outlook items. This policy setting is not configured by default. If this policy setting is enabled then the user's Outlook items will not be added to the index and the user will not see them in search results.
Computer	Search	Prevent indexing public folders	At least Windows Vista or later	Enable this policy setting to prevent indexing public folders in Microsoft Office Outlook. When this policy setting is disabled or not configured, the user has the option to index cached public folders in Outlook. Public folders are only indexed when using Outlook 2003 or later. The user must be running in cached mode and the Download Public Folder Favorites option must be turned on.
Computer	Search	Prevent indexing uncached Exchange folders	At least Windows Vista or later	Enabling this policy setting prevents indexing of mail items on a Microsoft Exchange server when Microsoft Outlook is run in uncached mode. This is the default behavior and so for uncached items to be indexed this policy setting must be disabled. Note that versions of Outlook prior to 2003 do not support cached mode and so only local items such as PST files will be indexed if this policy setting is enabled or left in the not configured state.
Computer	Security	Require use of specific security layer for remote (RDP) connections	At least Windows Vista or later	Specifies whether to require the use of a specific security layer to secure communications between clients and terminal servers during Remote Desktop Protocol (RDP) connections. If you enable this setting, all communications between clients and terminal servers during remote connections must use the security method specified in this setting. The following security methods are available: * Negotiate: The Negotiate method enforces the most secure method that is supported by the client. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the terminal server. If TLS is not supported,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				native Remote Desktop Protocol (RDP) encryption is used to secure communications, but the terminal server is not authenticated. * RDP: The RDP method uses native RDP encryption to secure communications between the client and terminal server. If you select this setting, the terminal server is not authenticated. * SSL (TLS 1.0): The SSL method requires the use of TLS 1.0 to authenticate the terminal server. If TLS is not supported, the connection fails. If you disable or do not configure this setting, the security method to be used for remote connections to terminal servers is not enforced through Group Policy. However, you can configure a required security method for these connections by using Terminal Services Configuration.
Computer	Security	Require user authentication using RDP 6.0 for remote connections	At least Windows Vista or later	Specifies whether to require user authentication using Remote Desktop Protocol (RDP) version 6.0 before allowing remote connections to terminal servers. This option enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this setting, only computers running Windows Vista or later can connect to terminal servers. If you disable this setting, RDP 6.0 is not required for user authentication before allowing remote connections to terminal servers. Instead, user authentication as implemented by earlier versions of RDP can be used. If you do not configure this setting, you can specify that RDP 6.0 be required for user authentication by using Terminal Services Configuration or the Remote tab in System Properties. Disabling or not configuring this setting provides less security, because user authentication will occur later in the remote connection process.
Computer	Security	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer	Security	Server Authentication Certificate Template	At least Windows Vista or later	This policy setting allows you to specify the name of the certificate template that determines which certificate is automatically selected to authenticate a terminal server. A certificate is needed to authenticate a terminal server when SSL (TLS 1.0) is used to secure communication between a client and a terminal server during RDP connections. If you enable this policy setting, you need to specify a certificate template name. Only certificates created by using the specified certificate template will be considered when a certificate to authenticate the terminal server is automatically selected. Automatic certificate selection only occurs when a specific certificate has not been selected. If no certificate can be found that was created with the specified certificate template, the terminal server will issue a certificate enrollment request and will use the current certificate until the request is completed. If more than one certificate is found that was created with the specified certificate template, the certificate that will expire latest and that matches the current name of the terminal server will be selected. If you disable or do not configure this policy setting, a self-signed certificate will be used by default to authenticate the terminal server. You can select a specific certificate to be used to authenticate the terminal server on the General tab of the Terminal Services Configuration tool. Note: If you select a specific certificate to be used to

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				authenticate the terminal server, that certificate will take precedence over this policy setting.
Computer	Server	Allow only system backup		
Computer	Server	Disallow locally attached storage as backup target		
Computer	Server	Disallow network as backup target	At least Windows Vista or later	This policy setting allows you to manage whether backups of a machine can run to a network share or not. If you enable this policy setting, machine administrator/backup operator cannot user Windows Server Backup to run backups to a network share. If you disable or do not configure this policy setting, there is no restriction on network share being backup target.
Computer	Server	Disallow optical media as backup target	At least Windows Vista or later	This policy setting allows you to manage whether backups of a machine can run to an optical media or not. If you enable this policy setting, machine administrator/backup operator cannot user Windows Server Backup to run backups to an optical media. If you disable or do not configure this policy setting, there is no restriction on optical media being backup target.
Computer	Server	Disallow run-once backups	At least Windows Vista or later	This policy setting allows you to manage whether run-once backups of a machine can be run or not. If you enable this policy setting, machine administrator/backup operator cannot user Windows Server Backup to run non-scheduled run-once backups. If you disable or do not configure this policy setting, there is no restriction on running run-once backups.
Computer	Setup	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer	Setup	Turn on logging	At least Windows Vista or later	This policy setting turns on logging. If you enable or do not configure this policy setting, then events can be written to this log. If the policy setting is disabled, then no new events can be logged. Events can always be read from the log, regardless of this policy setting.
Computer	Shutdown Options	Turn off automatic termination of applications that block or cancel shutdown	At least Windows Vista or later	This policy setting specifies whether Windows will allow console applications and GUI applications without visible top-level windows to block or cancel shutdown. By default, such applications are automatically terminated if they attempt to cancel shutdown or block it indefinitely. If you enable this setting, console applications or GUI applications without visible top-level windows that block or cancel shutdown will not be automatically terminated during shutdown. If you disable or do not configure this setting, these applications will be automatically terminated during shutdown, helping to ensure that Windows can shut down faster and more smoothly.
Computer	Sleep Settings	Allow Standby States (S1-S3) When Sleeping (On Battery)	At least Windows Vista or later	Dictates whether or not Windows is allowed to use standby states when sleeping the computer. When this policy is enabled, Windows may use standby states to sleep the computer. If this policy is disabled, the only sleep state a computer may enter is hibernate. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Sleep Settings	Allow Standby States (S1-S3)	At least Windows Vista or later	Dictates whether or not Windows is allowed to use standby states when sleeping

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		When Sleeping (Plugged In)		the computer. When this policy is enabled, Windows may use standby states to sleep the computer. If this policy is disabled, the only sleep state a computer may enter is hibernate. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Sleep Settings	Require a Password When a Computer Wakes (On Battery)	At least Windows Vista or later	Specifies whether or not the user is prompted for a password when the system resumes from sleep. If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep. If you disable this policy, the user is not prompted for a password when the system resumes from sleep.
Computer	Sleep Settings	Require a Password When a Computer Wakes (Plugged In)	At least Windows Vista or later	Specifies whether or not the user is prompted for a password when the system resumes from sleep. If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep. If you disable this policy, the user is not prompted for a password when the system resumes from sleep.
Computer	Sleep Settings	Specify the System Hibernate Timeout (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows transitions the system to hibernate. If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to hibernate. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Specify the System Hibernate Timeout (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows transitions the system to hibernate. If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				hibernate. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Specify the System Sleep Timeout (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows transitions the system to sleep. If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to sleep. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Specify the System Sleep Timeout (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows transitions the system to sleep. If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to sleep. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Turn Off Hybrid Sleep (On Battery)	At least Windows Vista or later	Disables Hybrid Sleep. If you enable this policy setting, a hiberfile is not generated when the system transitions to sleep (Stand By). If you do not configure this policy setting, users can see and change this setting. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Sleep Settings	Turn Off Hybrid Sleep (Plugged In)	At least Windows Vista or later	Disables Hybrid Sleep. If you enable this policy setting, a hiberfile is not generated when the system transitions to sleep (Stand By). If you do not configure this policy setting, users can see and change this setting. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				precedence over "User Configuration" policy.
Computer	Sleep Settings	Turn on Applications to Prevent Sleep Transitions (On Battery)	At least Windows Vista or later	Enables applications and services to prevent the system from sleeping. If you enable this policy setting, an application or service may prevent the system from sleeping (Hybrid Sleep, Stand By, or Hibernate). If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Turn on Applications to Prevent Sleep Transitions (Plugged In)	At least Windows Vista or later	Enables applications and services to prevent the system from sleeping. If you enable this policy setting, an application or service may prevent the system from sleeping (Hybrid Sleep, Stand By, or Hibernate). If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Smart Card	Allow certificates with no extended key usage certificate attribute	At least Windows Vista or later	This policy setting lets you allow certificates without an Extended Key Usage (EKU) set to be used for logon. Under previous versions of Microsoft Windows, the EKU extension was required to have the smart card logon Object Identifier (OID) present. This setting controls that restriction. If you enable this policy setting, only those smart card based certificates that contain the smart card logon OID or no EKU extension will be listed on the logon screen. If you disable or do not configure this policy setting then only those smart card based certificates that contain the smart card logon OID will be listed on the logon screen.
Computer	Smart Card	Allow Integrated Unblock screen to be displayed at the time of logon	At least Windows Vista or later	This policy setting lets you determine whether the integrated unblock feature will be available in the logon User Interface (UI). In order to use the integrated unblock feature your smart card must support this feature. Please check with your hardware manufacturer to see if your smart card supports this feature. If you enable this policy setting, the integrated unblock feature will be available. If you disable or do not configure this policy setting then the integrated unblock feature

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				will not be available.
Computer	Smart Card	Allow signature keys valid for Logon	At least Windows Vista or later	This policy setting lets you allow signature key-based certificates to be enumerated and available for logon. If you enable this policy setting then any certificates available on the smart card with a signature only key will be listed on the logon screen. If you disable or do not configure this policy setting, any available smart card signature key-based certificates will not be listed on the logon screen.
Computer	Smart Card	Allow time invalid certificates	At least Windows Vista or later	This policy setting permits those certificates to be displayed for logon that are either expired or not yet valid. Under previous versions of Microsoft Windows, certificates were required to contain a valid time and not be expired. The certificate must still be accepted by the domain controller in order to be used. This setting only controls the displaying of the certificate on the client machine. If you enable this policy setting certificates will be listed on the logon screen regardless of whether they have an invalid time or their time validity has expired. If you disable or do not configure this policy setting, certificates which are expired or not yet valid will not be listed on the logon screen.
Computer	Smart Card	Allow user name hint	At least Windows Vista or later	This policy setting lets you determine whether an optional field will be displayed during logon and elevation that allows a user to enter his or her user name or user name and domain, thereby associating a certificate with that user. If you enable this policy setting then an optional field that allows a user to enter their user name or user name and domain will be displayed. If you disable or do not configure this policy setting, an optional field that allows a users to enter their user name or user name and domain will not be displayed.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Smart Card	Configure root certificate clean up	At least Windows Vista or later	This policy setting allows you to manage the clean up behavior of root certificates. If you enable this policy setting then root certificate cleanup will occur according to the option selected. If you disable or do not configure this setting then root certificate clean up will occur on log off.
Computer	Smart Card	Display string when smart card is blocked	At least Windows Vista or later	This policy setting allows you to manage the displayed message when a smart card is blocked. If you enable this policy setting, the specified message will be displayed to the user when the smart card is blocked. Note: The following policy setting must be enabled - Allow Integrated Unblock screen to be displayed at the time of logon. If you disable or do not configure this policy setting, the default message will be displayed to the user when the smart card is blocked, if the integrated unblock feature is enabled.
Computer	Smart Card	Filter duplicate logon certificates	At least Windows Vista or later	This policy settings lets you configure if all your valid logon certificates are displayed. During the certificate renewal period, a user can have multiple valid logon certificates issued from the same certificate template. This can cause confusion as to which certificate to select for logon. The common case for this behavior is when a certificate is renewed and the old one has not yet expired. Two certificates are determined to be the same if they are issued from the same template with the same major version and they are for the same user (determined by their UPN). If there are two or more of the "same" certificate on a smart card and this policy is enabled then the certificate that is used for logon on Windows 2000, Windows XP, and Windows 2003 Server will be shown, otherwise the the certificate with the expiration time furthest in the future will be shown. Note: This setting will be applied after the following policy: "Allow time invalid certificates" If

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				you enable or do not configure this policy setting, filtering will take place. If you disable this policy setting, no filtering will take place.
Computer	Smart Card	Force the reading of all certificates from the smart card	At least Windows Vista or later	This policy setting allows you to manage the reading of all certificates from the smart card for logon. During logon Windows will by default only read the default certificate from the smart card unless it supports retrieval of all certificates in a single call. This setting forces Windows to read all the certificates from the card. This can introduce a significant performance decrease in certain situations. Please contact your smart card vendor to determine if your smart card and associated CSP supports the required behavior. If you enable this setting, then Windows will attempt to read all certificates from the smart card regardless of the feature set of the CSP. If you disable or do not configure this setting, Windows will only attempt to read the default certificate from those cards that do not support retrieval of all certificates in a single call. Certificates other than the default will not be available for logon.
Computer	Smart Card	Reverse the subject name stored in a certificate when displaying	At least Windows Vista or later	This policy setting lets you reverse the subject name from how it is stored in the certificate when displaying it during logon. By default the user principal name (UPN) is displayed in addition to the common name to help users distinguish one certificate from another. For example, if the certificate subject was CN=User1, OU=Users, DN=example, DN=com and had an UPN of user1@example.com then "User1" will be displayed along with "user1@example.com." If the UPN is not present then the entire subject name will be displayed. This setting controls the appearance of that subject name and might need to be adjusted per organization. If you enable this policy setting or do not configure this setting, then the subject

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				name will be reversed. If you disable , the subject name will be displayed as it appears in the certificate.
Computer	Smart Card	Turn on certificate propagation from smart card	At least Windows Vista or later	This policy setting allows you to manage the certificate propagation that occurs when a smart card is inserted. If you enable or do not configure this policy setting then certificate propagation will occur when you insert your smart card. If you disable this policy setting, certificate propagation will not occur and the certificates will not be made available to applications such as Outlook.
Computer	Smart Card	Turn on root certificate propagation from smart card	At least Windows Vista or later	This policy setting allows you to manage the root certificate propagation that occurs when a smart card is inserted. If you enable or do not configure this policy setting then root certificate propagation will occur when you insert your smart card. Note: For this policy setting to work the following policy setting must also be enabled: Turn on certificate propagation from smart card. If you disable this policy setting then root certificates will not be propagated from the smart card.
Computer/User	Sound Recorder	Do not allow Sound Recorder to run	At least Windows Vista or later	Specifies whether Sound Recorder can run. Sound Recorder is a feature of Microsoft Windows Vista that can be used to record sound from an audio input device where the recorded sound is encoded and saved as an audio file. If you enable this policy setting, Sound Recorder will not run. If you disable or do not configure this poliyc setting, Sound Recorder can be run.
Computer	SSL Configuration Settings	SSL Cipher Suite Order	At least Windows Vista or later	Determines the cipher suites used by the Secure Socket Layer (SSL). If this setting is enabled, SSL cipher suites will be prioritized in the order specified. If this setting is disabled or not configured, the factory default cipher suite order will be used. All available cipher suites: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_SHA

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521 TLS_DHE_DSS_WITH_AES_128_CBC_SHA TLS_DHE_DSS_WITH_AES_256_CBC_SHA TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 SSL_CK_RC4_128_WITH_MD5 SSL_CK_DES_192_EDE3_CBC_WITH_MD5 TLS_RSA_WITH_NULL_MD5 TLS_RSA_WITH_NULL_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_DHE_DSS_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_SHA TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				TLS_RSA_EXPORT_WITH_RC4_40_MD5 SSL_CK_DES_64_CBC_WITH_MD5 SSL_CK_RC4_128_EXPORT40_WITH_MD5 How to modify this setting: 1. Open a blank notepad document. 2. Copy and paste the list of available suites into it. 3. Arrange the suites in the correct order; remove any suites you don't want to use. 4. Place a comma at the end of every suite name except the last. Make sure there are NO embedded spaces. 5. Remove all the line breaks so that the cipher suite names are on a single, long line. 6. Copy the cipher-suite line to the clipboard, then paste it into the edit box. The maximum length is 1023 characaters.
User	Start Menu and Taskbar	Add the Run command to the Start Menu	At least Windows Vista or later	If you enable this setting, the Run command is added to the Start menu. If you disable or do not configure this setting, the Run command is not visible on the Start menu by default, but it can be added from the Taskbar and Start menu properties. If the Remove Run link from Start Menu policy is set, the Add the Run command to the Start menu policy has no effect.
User	Start Menu and Taskbar	Clear the recent programs list for new users	At least Windows Vista or later	If you enable this policy setting, the recent programs list in the start menu will be blank for each new user. If you disable or do not configure this policy, the start menu recent programs list will be pre-populated with programs for each new user.
User	Start Menu and Taskbar	Do not search communications	At least Windows Vista or later	If you enable this policy the start menu search box will not search for communications. If you disable or do not configure this policy, the start menu will search for communications, unless the user chooses not to in the start menu control panel.
User	Start Menu and Taskbar	Do not search files	At least Windows Vista or later	If you enable this policy the start menu search box will not search for files. If you disable or do not configure this policy, the start menu will search for files, unless the user chooses not to in the start menu control panel.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
User	Start Menu and Taskbar	Do not search Internet	At least Windows Vista or later	If you enable this policy the start menu search box will not search for internet history or favorites. If you disable or do not configure this policy, the start menu will search for for internet history or favorites, unless the user chooses not to in the start menu control panel.
User	Start Menu and Taskbar	Do not search programs	At least Windows Vista or later	If you enable this policy the start menu search box will not search for programs. If you disable or do not configure this policy, the start menu will search for programs, unless the user chooses not to in the start menu control panel.
User	Start Menu and Taskbar	Lock all taskbar settings	At least Windows Vista or later	Prevents the user from making any changes to the taskbar settings through the Taskbar Properties dialog. If you enable this setting the user cannot access the taskbar control panel, unlock, resize, move or rearrange items on their taskbar. If you disable or do not configure this setting the user will be able to set any taskbar setting that is not disallowed by another policy setting.
User	Start Menu and Taskbar	Prevent users from adding or removing toolbars	At least Windows Vista or later	Prevents users from adding or removing toolbars. If you enable this policy setting the user will not be allowed to add or remove any toolbars to the taskbar. Applications will not be able to add toolbars either. If you disable or do not configure this policy setting, the users and applications will be able to add toolbars to the taskbar.
User	Start Menu and Taskbar	Prevent users from moving taskbar to another screen dock location	At least Windows Vista or later	Prevents users from moving taskbar to another screen dock location. If you enable this policy setting the user will not be able to drag their taskbar to another side of the monitor(s). If you disable or do not configure this policy setting the user may be able to drag their taskbar to other sides of the monitor unless disallowed by another policy setting.
User	Start Menu and Taskbar	Prevent users from rearranging	At least Windows Vista or later	Prevents users from rearranging toolbars. If you enable this setting the user will

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		toolbars		not be able to drag or drop toolbars to the taskbar. If you disable or do not configure this policy setting, users will be able to rearrange the toolbars on the taskbar.
User	Start Menu and Taskbar	Prevent users from resizing the taskbar	At least Windows Vista or later	Prevent users from resizing the taskbar. If you enable this policy setting the user will not be able to resize their taskbar to be any other size. If you disable or do not configure this policy setting, the user will be able to resize their taskbar to be any other size unless disallowed by another setting.
User	Start Menu and Taskbar	Remove Games link from Start Menu	At least Windows Vista or later	If you enable this policy the start menu will not show a link to the Games folder. If you disable or do not configure this policy, the start menu will show a link to the Games folder, unless the user chooses to remove it in the start menu control panel.
User	Start Menu and Taskbar	Remove Search Computer link	At least Windows Vista or later	If you enable this policy, the "See all results" link will not be shown when the user performs a search in the start menu search box. If you disable or do not configure this policy, the "See all results" link will be shown when the user performs a search in the start menu search box.
User	Start Menu and Taskbar	Remove the battery meter	At least Windows Vista or later	Prevents the battery meter in the system control area from being displayed. If you enable this setting, the battery meter will not be displayed in the system notification area. If you disable or do not configure this setting, the battery meter will be displayed in the system notification area.
User	Start Menu and Taskbar	Remove the networking icon	At least Windows Vista or later	Prevents the networking icon in the system control area from being displayed. If you enable this setting, the networking icon will not be displayed in the system notification area. If you disable or do not configure this setting, the networking icon will be displayed in the system notification area.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
User	Start Menu and Taskbar	Remove the volume control icon	At least Windows Vista or later	Prevents the volume control icon in the system control area from being displayed. If you enable this setting, the volume control icon will not be displayed in the system notification area. If you disable or do not configure this setting, the volume control icon will be displayed in the system notification area.
User	Start Menu and Taskbar	Remove user folder link from Start Menu	At least Windows Vista or later	If you enable this policy the start menu will not show a link to the user's storage folder. If you disable or do not configure this policy, the start menu will display a link, unless the user chooses to remove it in the start menu control panel.
User	Start Menu and Taskbar	Show QuickLaunch on Taskbar	At least Windows Vista or later	This policy setting controls whether the QuickLaunch bar is displayed in the Taskbar. If you enable this policy setting, the QuickLaunch bar will be visible and cannot be turned off. If you disable this policy setting, the QuickLaunch bar will be hidden and cannot be turned on. If you do not configure this policy setting, then users will be able to turn the QuickLaunch bar on and off.
User	Start Menu and Taskbar	Turn off all balloon notifications	At least Windows Vista or later	If you enable this setting no notification balloons will be shown to the user. If you disable or do not configure this setting balloon notifications will be displayed.
User	Start Menu and Taskbar	Turn off taskbar thumbnails	At least Windows Vista or later	If you enable this setting the taskbar thumbnails will not be shown, and the system will use standard text for the tooltips. If you disable or do not configure this setting the user will see the taskbar thumbnails.
User	Start Menu and Taskbar	Use folders instead of library	At least Windows Vista or later	User folders links launch a folder view of users files instead of a library view.
Computer	System	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer/User	Tablet PC Pen Training	Turn off Tablet PC Pen Training	At least Windows Vista or later	Turns off Tablet PC Pen Training. If you enable this policy setting, users cannot open Tablet PC Pen Training. If you disable or do not configure this policy setting, users can open Tablet PC Pen Training.
Computer/User	Touch Input	Turn off Tablet PC touch input	At least Windows Vista or later	Turn off Tablet PC touch input Turns off touch input, which allows the user to interact with their computer using their finger. If you enable this setting, the user will not be able to produce input with touch. They will not be able to use touch input or touch gestures such as tap and double tap, the touch pointer, and other touch-specific features. If you disable this setting, the user can produce input with touch, by using gestures, the touch pointer, and other-touch specific features. If you do not configure this setting, touch input is on by default. Note: Changes to this setting will not take effect until the user logs off.
Computer	Troubleshooting and Diagnostics	Diagnostics: Configure scenario execution level	At least Windows Vista or later	Determines the execution level for Diagnostic Policy Service (DPS) scenarios. If you enable this policy setting, you must select an execution level from the dropdown menu. If you select problem detection and troubleshooting only, the DPS will detect problems and attempt to determine their root causes. These root causes will be logged to the event log when detected, but no corrective action will be taken. If you select detection, troubleshooting and resolution, the DPS will attempt to automatically fix problems it detects or indicate to the user that assisted resolution is available. If you disable this policy setting, Windows will not be able to detect, troubleshoot or resolve any problems that are handled by the DPS. If you do not configure this policy setting, the DPS will enable all scenarios for resolution by default, unless you configure separate scenario-specific policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				settings. This policy setting takes precedence over any scenario-specific policy settings when it is enabled or disabled. Scenario-specific settings only take effect if this policy is not configured. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Troubleshooting and Diagnostics	Diagnostics: Configure scenario retention	At least Windows Vista or later	Determines the data retention limit for Diagnostic Policy Service (DPS) scenario data. If you enable this policy setting, you must enter the maximum size of scenario data that should be retained in megabytes. Detailed troubleshooting data related to scenarios will be retained until this limit is reached. If you disable this setting, or if you do not configure this policy setting, the DPS will delete scenario data once it exceeds 128 megabytes in size. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service is in the running state. When the service is stopped or disabled, diagnostic scenario data will not be deleted. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Trusted Platform Module Services	Configure the list of blocked TPM commands	At least Windows Vista or later	This policy setting allows you to manage the Group Policy list of Trusted Platform Module (TPM) commands blocked by Windows. If you enable this policy setting, Windows will block the specified commands from being sent to the TPM on the computer. TPM commands are referenced by a command number. For example,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				command number 129 is TPM_OwnerReadInternalPub, and command number 170 is TPM_FieldUpgrade. To find the command number associated with each TPM command, run "tpm.msc" and navigate to the "Command Management" section. If you disable or do not configure this policy setting, only those TPM commands specified through the default or local lists may be blocked by Windows. The default list of blocked TPM commands is pre-configured by Windows. You can view the default list by running "tpm.msc", navigating to the "Command Management" section, and making visible the "On Default Block List" column. The local list of blocked TPM commands is configured outside of Group Policy by running "tpm.msc" or through scripting against the Win32_Tpm interface. See related policy settings to enforce or ignore the default and local lists of blocked TPM commands.
Computer	Trusted Platform Module Services	Ignore the default list of blocked TPM commands	At least Windows Vista or later	This policy setting allows you to enforce or ignore the computer's default list of blocked Trusted Platform Module (TPM) commands. If you enable this policy setting, Windows will ignore the computer's default list of blocked TPM commands and will only block those TPM commands specified by Group Policy or the local list. The default list of blocked TPM commands is pre-configured by Windows. You can view the default list by running "tpm.msc", navigating to the "Command Management" section, and making visible the "On Default Block List" column. The local list of blocked TPM commands is configured outside of Group Policy by running "tpm.msc" or through scripting against the Win32_Tpm interface. See the related policy setting to configure the Group Policy list of blocked TPM commands. If you disable or do not configure this policy setting, Windows will

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				block the TPM commands in the default list, in addition to commands in the Group Policy and local lists of blocked TPM commands.
Computer	Trusted Platform Module Services	Ignore the local list of blocked TPM commands	At least Windows Vista or later	This policy setting allows you to enforce or ignore the computer's local list of blocked Trusted Platform Module (TPM) commands. If you enable this policy setting, Windows will ignore the computer's local list of blocked TPM commands and will only block those TPM commands specified by Group Policy or the default list. The local list of blocked TPM commands is configured outside of Group Policy by running "tpm.msc" or through scripting against the Win32_Tpm interface. The default list of blocked TPM commands is pre-configured by Windows. See the related policy setting to configure the Group Policy list of blocked TPM commands. If you disable or do not configure this policy setting, Windows will block the TPM commands found in the local list, in addition to commands in the Group Policy and default lists of blocked TPM commands.
Computer	Trusted Platform Module Services	Turn on TPM backup to Active Directory Domain Services	At least Windows Vista or later	This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of Trusted Platform Module (TPM) owner information. TPM owner information includes a cryptographic hash of the TPM owner password. Certain TPM commands can only be run by the TPM owner. This hash authorizes the TPM to run these commands. If you enable this policy setting, TPM owner information will be automatically and silently backed up to AD DS when you use Windows to set or change a TPM owner password. If you select the option to "Require TPM backup to AD DS", a TPM owner password cannot be set or changed unless the computer is connected to the domain and the AD DS backup succeeds. This option is selected by default to help ensure that TPM owner

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				information is available. Otherwise, AD DS backup is attempted but network or other backup failures do not impact TPM management. Backup is not automatically retried and the TPM owner information may not have been stored in AD DS during BitLocker setup. If you disable or do not configure this policy setting, TPM owner information will not be backed up to AD DS. Note: You must first set up appropriate schema extensions and access control settings on the domain before AD DS backup can succeed. Consult online documentation for more information about setting up Active Directory Domain Services for TPM. Note: The TPM cannot be used to provide enhanced security features for BitLocker Drive Encryption and other applications without first setting an owner. To take ownership of the TPM with an owner password, run "tpm.msc" and select the action to "Initialize TPM". Note: If the TPM owner information is lost or is not available, limited TPM management is possible by running "tpm.msc" on the local computer.
Computer	User Accounts	Apply the default user logon picture to all users	At least Windows Vista or later	This policy setting allows an administrator to standardize the logon pictures for all users on a system to the default user picture. One application for this policy setting is to standardize the logon pictures to a company logo. Note: The default user picture is stored at %PROGRAMDATA%\Microsoft\User Account Pictures\user.bmp. The default guest picture is stored at %PROGRAMDATA%\Microsoft\User Account Pictures\guest.bmp. If the default pictures do not exist, an empty frame is displayed. If you enable this policy setting, the default user logon picture will display for all users on the system with no customization allowed. If you disable or do not configure this policy setting,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				users will be able to customize their logon pictures.
Computer	User Profiles	Delete user profiles older than a specified number of days on system restart	At least Windows Vista or later	This policy setting allows an administrator to automatically delete user profiles on system restart that have not been used within a specified number of days. Note: One day is interpreted as 24 hours after a specific user profile was accessed. If you enable this policy setting, the User Profile Service will automatically delete on the next system restart all user profiles on the computer that have not been used within the specified number of days. If you disable or do not configure this policy setting, User Profile Service will not automatically delete any profiles on the next system restart.
Computer	User Profiles	Do not forcefully unload the users registry at user logoff	At least Windows Vista or later	Microsoft Windows will always unload the users registry, even if there are any open handles to the per-user registry keys at user logoff. Using this policy setting, an administrator can negate this behavior, preventing Windows from forcefully unloading the users registry at user logoff. Note: This policy should only be used for cases where you may be running into application compatibility issues due to this specific Windows behavior. It is not recommended to enable this policy by default as it may prevent users from getting an updated version of their roaming user profile. If you enable this policy setting, Windows will not forcefully unload the users registry at logoff, but will unload the registry when all open handles to the per-user registry keys are closed. If you disable or do not configure this policy setting, Windows will always unload the users registry at logoff, even if there are any open handles to the per-user registry keys at user logoff.
User	User Profiles	Network directories to sync at Logon/Logoff time only	At least Windows Vista or later	This policy setting allows you to specify which network directories will be synchronized only at logon and logoff via Offline Files. This policy setting is meant

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				to be used in conjunction with Folder Redirection, to help resolve issues with applications that do not work well with Offline Files while the user is online. If you enable this policy setting, the network paths specified in this policy setting will be synchronized only by Offline Files during user logon and logoff, and will be taken offline while the user is logged on. If you disable or do not configure this policy setting, the paths specified in this policy setting will behave like any other cached data via Offline Files and continue to remain online while the user is logged on, if the network paths are accessible. Note: You should not use this policy setting to suspend any of the root redirected folders such as Appdata\Roaming, Start Menu, and Documents. You should suspend only the subfolders of these parent folders.
Computer	User Profiles	Set maximum wait time for the network if a user has a roaming user profile or remote home directory	At least Windows Vista or later	If the user has a roaming user profile or remote home directory and the network is currently unavailable, Microsoft Windows waits 30 seconds for the network when the user logs on to the computer. Using this policy setting, an administrator can specify how long Windows should wait for the network to become available. If the network is unavailable after the maximum wait time, Windows will continue the log on the user without a network connection. The user's roaming profile is not synchronized with the server, and the remote home directory is not used for the logon session. This policy is useful for the cases in which a network may take typically longer to initialize, such as with a wireless network. Note: If the network becomes available before the maximum wait time, Windows will proceed immediately with the user logon. Windows will not wait on the network if the physical network connection is not available on the computer (if the media is disconnected or the network adapter is not available). If you enable this policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting, Windows will wait for the network to become available up to the maximum wait time specified in this policy setting. Setting the value to zero will cause Windows to proceed without waiting for the network. If you disable or do not configure this policy setting, Windows will wait for the network for a maximum of 30 seconds.
Computer	User Profiles	Set roaming profile path for all users logging onto this computer	At least Windows Vista or later	Specifies whether Microsoft Windows should use the specified network path as the roaming user profile path for all users logging onto this computer. To use this setting, type the path to the network share in the form \\Computername\Sharename\. It is recommended to add %USERNAME% to the path to give each user an individual profile folder. If not specified, all users logging onto this computer will use the same roaming profile folder as specified by this policy. You need to ensure that you have set the appropriate security on the folder to allow all users to access the profile. If you enable this policy setting, all users logging on this computer will use the roaming profile path specified in this policy. If you disable or do not configure this policy setting, then users logging on this computer will use their local profile or standard roaming user profile. Note: There are 4 ways to configure a roaming profile for a user. Windows reads profile configuration in the following order and uses the first configured setting it reads. 1. Terminal Services roaming profile path specified by Terminal Services policy 2. Terminal Services roaming profile path specified by the user object 3. A per-computer roaming profile path specified in this policy 4. A per-user roaming profile path specified in the user object
Computer	Video and Display	Turn Off Adaptive Display Timeout	At least Windows Vista or later	Manages how Windows controls the setting that specifies how long a computer

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Settings	(On Battery)		must be inactive before Windows turns off the computerΓÇÖs display. When this policy is enabled, Windows automatically adjusts the setting based on what users do with their keyboard or mouse to keep the display on. When this policy is disabled, Windows uses the same setting regardless of usersΓÇÖ keyboard or mouse behavior. If you donΓÇÖt configure this setting, users can see and change this setting.
Computer	Video and Display Settings	Turn Off Adaptive Display Timeout (Plugged In)	At least Windows Vista or later	Manages how Windows controls the setting that specifies how long a computer must be inactive before Windows turns off the computerΓÇÖs display. When this policy is enabled, Windows automatically adjusts the setting based on what users do with their keyboard or mouse to keep the display on. When this policy is disabled, Windows uses the same setting regardless of usersΓÇÖ keyboard or mouse behavior. If you donΓÇÖt configure this setting, users can see and change this setting.
Computer	Video and Display Settings	Turn Off the Display (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the display. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the display. If you disable this policy or do not configure it, users can see and change this setting. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Video and Display Settings	Turn Off the Display (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the display. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the display. If you disable this policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				or do not configure it, users can see and change this setting. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer/User	Window Frame Coloring	Do not allow color changes	At least Windows Vista or later	This policy setting controls the ability to change the color of window frames. If you enable this policy setting, you prevent users from changing the default window frame color. If you disable or do not configure this policy setting, you allow users to change the default window frame color. Note: This setting can be used in conjunction with the "Specify a default color for window frames" setting, to enforce a specific color for window frames that cannot be changed by users.
Computer/User	Window Frame Coloring	Specify a default color	At least Windows Vista or later	This policy setting controls the default color for window frames when the user does not specify a color. If you enable this policy setting and specify a default color, this color will be used in glass window frames, if the user has not specified a color. If you disable or do not configure this policy setting, the default internal color will be used, if the user has not specified a color. Note: This policy setting can be used in conjunction with the, "Prevent color changes of window frames" setting, to enforce a specific color for window frames that cannot be changed by users.
Computer	Windows Boot Performance Diagnostics, Windows Memory Leak Diagnosis, Windows Resource	Configure Scenario Execution Level	At least Windows Vista or later	Determines the execution level for Windows Boot Performance Diagnostics. If you enable this policy setting, you must select an execution level from the dropdown menu. If you select problem detection and troubleshooting only, the Diagnostic Policy Service (DPS) will detect Windows Boot Performance problems and attempt to determine their root causes. These root causes will be logged to the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Exhaustion Detection and Resolution, Windows Shutdown Performance Diagnostics, Windows Standby/Resume Performance Diagnostics, Windows System Responsiveness Performance Diagnostics			event log when detected, but no corrective action will be taken. If you select detection, troubleshooting and resolution, the DPS will detect Windows Boot Performance problems and indicate to the user that assisted resolution is available. If you disable this policy setting, Windows will not be able to detect, troubleshoot or resolve any Windows Boot Performance problems that are handled by the DPS. If you do not configure this policy setting, the DPS will enable Windows Boot Performance for resolution by default. This policy setting takes effect only if the diagnostics-wide scenario execution policy is not configured. No system restart or service restart is required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer/User	Windows Calendar	Turn off Windows Calendar	At least Windows Vista or later	Windows Calendar is a feature that allows users to manage appointments and tasks by creating personal calendars, publishing them, and subscribing to other users calendars. If you enable this setting, Windows Calendar will be turned off. If you disable or do not configure this setting, Windows Calendar will be turned on. The default is for Windows Calendar to be turned on.
Computer/User	Windows Color System	Prohibit installing or uninstalling color profiles	At least Windows Vista or later	This policy setting affects the ability of users to install or uninstall color profiles. If you enable this policy setting, users will not be able to install new color profiles or uninstall previously installed color profiles. If you disable or do not configure this policy setting, all users will be able to install new color profiles. Standard users will be able to uninstall color profiles that they previously installed. Administrators will

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				be able to uninstall all color profiles.
Computer	Windows Connect Now	Configuration of wireless settings using Windows Connect Now	At least Windows Vista or later	This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP), through the Windows Portable Device API (WPD), and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium. If this policy setting is enabled, additional choices are available to turn off the operations over a specific medium. If this policy setting is disabled, operations are disabled over all media. If this policy setting is not configured, operations are enabled over all media. The default for this policy setting allows operations over all media.
Computer/User	Windows Connect Now	Prohibit Access of the Windows Connect Now wizards	At least Windows Vista or later	This policy setting prohibits access to Windows Connect Now (WCN) wizards. If this policy setting is enabled, the wizards are disabled and users will have no access to any of the wizard tasks. All the configuration related tasks, including ΓÇÿSet up a wireless router or access pointΓÇÖ and ΓÇÿAdd a wireless deviceΓÇÖ, will be disabled. If this policy is disabled or not configured, users will have access to the wizard tasks; including ΓÇÿSet up a wireless router or access pointΓÇÖ and ΓÇÿAdd a wireless deviceΓÇÖ. The default for this policy setting allows users to access all WCN wizards.
Computer	Windows Customer Experience Improvement Program	Allow Corporate redirection of Customer Experience Improvement uploads	At least Windows Vista or later	If you enable this setting all Customer Experience Improvement Program uploads are redirected to Microsoft Operations Manager server. If you disable this setting uploads are not redirected to a Microsoft Operations Manager server. If you do not configure this setting uploads are not redirected to a Microsoft Operations Manager server.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Windows Customer Experience Improvement Program	Allow Windows Customer Experience Improvement Program to collect corporate information	At least Windows Vista or later	The Windows Customer Experience Improvement Program will collect information about your hardware configuration and how you use our software and services to identify trends and usage patterns. We will not collect your name, address, or any other personally identifiable information. There are no surveys to complete, no salesperson will call, and you can continue working without interruption. It is simple and user-friendly. If you enable this policy setting all users are opted into Windows Customer Experience Improvement Program. If you disable this policy setting all users are opted out of Windows Customer Experience Improvement Program. If you do not configure this policy setting, administrator can use the Problem Reports and Solutions component in Control Panel to enable Windows Customer Experience Improvement Program for all users.
Computer	Windows Customer Experience Improvement Program	Tag Windows Customer Experience Improvement data with Study Identifier	At least Windows Vista or later	This policy setting will enable tagging of Windows Customer Experience Improvement data when a study is being conducted. If you enable this setting then Windows CEIP data uploaded will be tagged. If you do not configure this setting or disable it, then CEIP data will not be tagged with the Study Identifier.
Computer	Windows Defender	Check for New Signatures Before Scheduled Scans	At least Windows Vista or later	Checks for new signatures before running scheduled scans. If you enable this policy setting, the scheduled scan checks for new signatures before it scans the computer. If you disable or do not configure this policy setting, the scheduled scan begins without downloading new signatures.
Computer	Windows Defender	Configure Microsoft SpyNet Reporting	At least Windows Vista or later	Adjusts membership in Microsoft SpyNet. Microsoft SpyNet is the online community that helps you choose how to respond to potential spyware threats. The community also helps stop the spread of new spyware infections. Here's how it works. When Windows Defender detects software or changes by software not

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				yet classified for risks, you see how other members responded to the alert. In turn, the action you apply help other members choose how to respond. Your actions also help Microsoft choose which software to investigate for potential threats. You can choose to send basic or additional information about detected software. Additional information helps improve how Windows Defender works. It can include, for example, the location of detected items on your computer if harmful software has been removed. Windows Defender will automatically collect and send the information. If you enable this policy setting and choose "No Membership" from the drop-down list, SpyNet membership will be disabled. At this setting, no information will be sent to Microsoft. You will not be alerted if Windows Defender detects unclassified software running on your computer. Local users will not be able to change their SpyNet membership. If you enable this policy setting and choose "Basic" from the drop-down list, SpyNet membership is set to "Basic". At this setting, basic information about the detected items and the actions you apply will be shared with the online community. You will not be alerted if Windows Defender detects software that has not yet been classified for risks. If you enable this policy setting and choose "Advanced" from the drop-down list, SpyNet membership is set to "Advanced". At this setting, you send your choices and additional information about detected items. You are alerted so you can take action when Windows Defender detects changes to your computer by unclassified software. Your decisions to allow or block changes help Microsoft create new definitions for Windows Defender and better detect harmful software. In some instances, personal information may be sent but no information is used to contact

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				you. If you disable or do not configure this policy setting, by default SpyNet membership is disabled. At this setting, no information will be sent to Microsoft. You will not be alerted if Windows Defender detects unclassified software running on your computer. Local users will still be able to change their SpyNet membership.
Computer	Windows Defender	Download Entire Signature Set	At least Windows Vista or later	Downloads the full signature set, rather than only the signatures that have been updated since the last signature download. Downloading the full signature set can help troubleshoot problems with signature installations, but because the file is large, it can take longer to download. If you enable this policy setting, the full signatures set is downloaded. If you disable or do not configure this policy setting, by default only updated signatures are downloaded.
Computer	Windows Defender	Enable Logging Known Good Detections	At least Windows Vista or later	Enables logging detection data during Real-time Protection when Windows Defender detects known good files. Logging detections provides you with detailed information about the programs that run on the computers you monitor. If you enable this policy setting, known good files are logged. If you disable or do not configure this policy setting, by default known good files are not logged. Enabling this policy setting can result in a greater number of events in the log.
Computer	Windows Defender	Enable Logging Unknown Detection	At least Windows Vista or later	Enables logging detections during Real-time Protection when Windows Defender detects unknown files. Logging detections provides you with detailed information about the programs that run on the computers you monitor. If you enable or do not configure this policy setting, by default unknown files are logged. If you disable this policy setting, unknown files are not logged. Enabling this policy setting can result in a greater number of events in the log.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Windows Defender	Turn off Real-Time Protection Prompts for Unknown Detection	At least Windows Vista or later	Turns off Real-Time Protection (RTP) prompts for unknown detection. If you enable this policy setting, Windows Defender does not prompt users to allow or block unknown activity. If you disable or do not configure this policy setting, by default Windows Defender prompts users to allow or block unknown activity on the computer.
Computer	Windows Defender	Turn off Windows Defender	At least Windows Vista or later	Turns off Windows Defender Real-Time Protection, and no more scans are scheduled. If you enable this policy setting, Windows Defender does not run, and computers will not be scanned for spyware or other potentially unwanted software. If you disable or do not configure this policy setting, by default Windows Defender runs and computers are scanned for spyware and other potentially unwanted software.
Computer	Windows Defender	Turn on definition updates through both WSUS and Windows Update	At least Windows Vista or later	This policy setting allows you to configure Windows Defender to check and install definition updates from Windows Update when a locally managed Windows Server Update Services (WSUS) server is not available. Windows Defender checks for definition updates using the Automatic Updates client. The Automatic Updates client can be configured to check the public Windows Update Web site or a locally managed WSUS server. When a computer is not able to connect to an internal WSUS server, such as when a portable computer is roaming outside of the corporate network, Windows Defender can be configured to also check Windows Update to ensure definition updates are delivered to these roaming machines. If you enable or do not configure this policy setting, by default Windows Defender will check for definition updates from Windows Update, if connections to a locally managed WSUS server fail. If you disable this policy setting, Windows

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Defender will check for definition updates only on a locally managed WSUS server, if the Automatic Updates client is so configured.
Computer/User	Windows Error Reporting	Disable Logging	At least Windows Vista or later	If this setting is enabled Windows Error Reporting events will not be logged to the system event log.
Computer/User	Windows Error Reporting	Disable Windows Error Reporting	At least Windows Vista or later	If this setting is enabled, Windows Error Reporting will not send any problem information to Microsoft. Additionally, solution information will not be available in the Problem Reports and Solutions control panel.
Computer/User	Windows Error Reporting	Do not send additional data	At least Windows Vista or later	If this setting is enabled any additional data requests from Microsoft in response to a Windows Error Reporting event will be automatically declined without notice to the user.
User	Windows Explorer	Display the menu bar in Windows Explorer	At least Windows Vista or later	This policy setting configures Windows Explorer to always display the menu bar. Note: By default, the menu bar is not displayed in Windows Explorer. If you enable this policy setting, the menu bar will be displayed in Windows Explorer. If you disable or do not configure this policy setting, the menu bar will not be displayed in Windows Explorer. Note: When the menu bar is not displayed, users can access the menu bar by pressing the 'ALT' key.
User	Windows Explorer	Prevent users from adding files to the root of their Users Files folder.	At least Windows Vista or later	This policy setting allows administrators to prevent users from adding new items such as files or folders to the root of their Users Files folder in Windows Explorer. If you enable this policy setting, users will no longer be able to add new items such as files or folders to the root of their Users Files folder in Windows Explorer. If you disable or do not configure this policy setting, users will be able to add new items such as files or folders to the root of their Users Files folder in Windows Explorer. Note: Enabling this policy setting does not prevent the user from being

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				able to add new items such as files and folders to their actual file system profile folder at %userprofile%.
User	Windows Explorer	Turn off common control and window animations	At least Windows Vista or later	This policy is similar to settings directly available to computer users. Disabling animations can improve usability for users with some visual disabilities as well as improving performance and battery life in some scenarios.
Computer	Windows Explorer	Turn off heap termination on corruption	At least Windows Vista or later	Disabling heap termination on corruption can allow certain legacy plug-in applications to function without terminating Explorer immediately, although Explorer may still terminate unexpectedly later.
User	Windows Explorer	Turn off the display of thumbnails and only display icons on network folders	At least Windows Vista or later	Disables the display of thumbnails on network folders in Windows Explorer. Windows Explorer displays thumbnails on network folders by default. If you enable this policy, Windows Explorer will only display icons and never display thumbnails on network folders.
User	Windows Explorer	Turn off the display of thumbnails and only display icons.	At least Windows Vista or later	Disables the display of thumbnails in Windows Explorer. Windows Explorer displays thumbnails by default. If you enable this policy setting, Windows Explorer will only display icons and never display thumbnails.
Computer/User	Windows HotStart	Turn off Windows HotStart	At least Windows Vista or later	This policy setting allows you to manage whether HotStart buttons can be used to launch applications. If you enable this policy setting, applications cannot be launched using the HotStart buttons. If you disable or do not configure this policy setting, applications can be launched using the HotStart buttons.
Computer	Windows Logon Options	Disable or enable software Secure Attention Sequence	At least Windows Vista or later	This policy setting controls whether or not software can simulate the Secure Attention Sequence (SAS). If you enable this policy setting, you have one of four options: If you set this policy setting to "None," user mode software cannot simulate the SAS. If you set this policy setting to "Services," services can simulate

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the SAS. If you set this policy setting to "Ease of Access applications," Ease of Access applications can simulate the SAS. If you set this policy setting to "Services and Ease of Access applications," both services and Ease of Access applications can simulate the SAS. If you disable or do not configure this setting, only Ease of Access applications running on the secure desktop can simulate the SAS.
Computer	Windows Logon Options	Display information about previous logons during user logon	At least Windows Vista or later	This policy setting controls whether or not the system displays information about previous logons and logon failures to the user. For local user accounts and domain user accounts in Microsoft Windows Server ΓÇ¥LonghornΓÇ¥ functional level domains, if you enable this setting, a message appears after the user logs on that displays the date and time of the last successful logon by that user, the date and time of the last unsuccessful logon attempted with that user name, and the number of unsuccessful logons since the last successful logon by that user. This message must be acknowledged by the user before the user is presented with the Microsoft Windows desktop. For domain user accounts in Windows Server 2003, Windows 2000 native, or Windows 2000 mixed functional level domains, if you enable this setting, a warning message will appear that Windows could not retrieve the information and the user will not be able to log on. Therefore, you should not enable this policy setting if the domain is not at the Windows Server ΓÇ£LonghornΓÇ¥ domain functional level. If you disable or do not configure this setting, messages about the previous logon or logon failures are not displayed.
User	Windows Logon Options	Remove logon hours expiration	At least Windows Vista or later	This policy controls whether the logged on user should be notified when his logon

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		warnings		hours are about to expire. By default, a user is notified before logon hours expire, if actions have been set to occur when the logon hours expire. If you enable this setting, warnings are not displayed to the user before the logon hours expire. If you disable or do not configure this setting, users receive warnings before the logon hours expire, if actions have been set to occur when the logon hours expire. Note: If you configure this setting, you might want to examine and appropriately configure the ΓÇ£Set action to take when logon hours expireΓÇ¥ setting. If ΓÇ£Set action to take when logon hours expireΓÇ¥ is disabled or not configured, the ΓÇ£Remove logon hours expiration warningsΓÇ¥ setting will have no effect, and users receive no warnings about logon hour expiration
Computer/User	Windows Logon Options	Report when logon server was not available during user logon	At least Windows Vista or later	This policy controls whether the logged on user should be notified if the logon server could not be contacted during logon and he has been logged on using previously stored account information. If enabled, a notification popup will be displayed to the user when the user logs on with cached credentials. If disabled or not configured, no popup will be displayed to the user.
User	Windows Logon Options	Set action to take when logon hours expire	At least Windows Vista or later	This policy controls which action will be taken when the logon hours expire for the logged on user. The actions include lock the workstation, disconnect the user, or log the user off completely. If you choose to lock or disconnect a session, the user cannot unlock the session or reconnect except during permitted logon hours. If you choose to log off a user, the user cannot log on again except during permitted logon hours. If you choose to log off a user, the user might lose unsaved data. If you enable this setting, the system will perform the action you specify when the userΓÇÖs logon hours expire. If you disable or do not configure this setting, the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				system takes no action when the userΓÇÖs logon hours expire. The user can continue the existing session, but cannot log on to a new session. Note: If you configure this setting, you might want to examine and appropriately configure the ΓÇ£Remove logon hours expiration warningsΓÇ¥ setting
Computer/User	Windows Mail	Turn off the communities features	At least Windows Vista or later	Windows Mail will not check your newsgroup servers for Communities support.
User	Windows Mail	Turn off the communities features	At least Windows Vista or later	Windows Mail will not check your newsgroup servers for Communities support.
Computer/User	Windows Mail	Turn off Windows Mail application	At least Windows Vista or later	Denies or allows access to the Windows Mail application. If you enable this setting, access to the Windows Mail application is denied. If you disable or do not configure this setting, access to the Windows Mail application is allowed.
Computer/User	Windows Media Center	Do not allow Windows Media Center to run	At least Windows Vista or later	Specifies whether Windows Media Center can run. If you enable this setting, Windows Media Center will not run. If you disable or do not configure this setting, Windows Media Center can be run.
Computer/User	Windows Meeting Space	Turn off Windows Meeting Space	At least Windows Vista or later	Windows Meeting Space is a feature that enables quick, face-to-face collaboration for sharing programs and handouts and for passing notes. If you enable this setting, Windows Meeting Space will be turned off. If you disable or do not configure this setting, Windows Meeting Space will be turned on. The default setting is for Windows Meeting Space to be turned on.
Computer/User	Windows Meeting Space	Turn on Windows Meeting Space auditing	At least Windows Vista or later	Windows Meeting Space is a feature that enables quick, face-to-face collaboration for sharing programs and handouts and for passing notes. If you enable this setting, Windows Meeting Space will audit various events that occur during a session (for example, when a user creates a session, joins a session, or starts a presentation) in the event log. If you disable or do not configure this setting, Windows Meeting Space auditing will be turned off. The default setting is

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				for Windows Meeting Space auditing to be turned off.
Computer/User	Windows Mobility Center	Turn off Windows Mobility Center	At least Windows Vista or later	This policy setting turns off Windows Mobility Center. If you enable this policy setting, the user is unable to invoke Windows Mobility Center. The Windows Mobility Center UI is removed from all shell entry points and the .exe file does not launch it. If you disable this policy setting, the user is able to invoke Windows Mobility Center and the .exe file launches it. If you do not configure this policy setting, Windows Mobility Center is on by default.
Computer/User	Windows Movie Maker	Do not allow Windows Movie Maker to run	At least Windows Vista or later	Specifies whether Windows Movie Maker can run. Windows Movie Maker is a feature of Windows Vista that can be used to edit and then publish 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	Windows Remote Shell	Allow Remote Shell Access	At least Windows Vista or later	Configures access to remote shells. If you enable this policy setting and set it to False, new remote shell connections will be rejected by the server. If you disable or do not configure this policy setting, new remote shell connections will be allowed.
Computer	Windows Remote Shell	MaxConcurrentUsers	At least Windows Vista or later	Configures the maximum number of users able to concurrently perform remote operations on the same system using remote CMD shell. The value can be any number from 1 to 100. If you enable this policy setting, the new shell connections will be rejected if they exceed the specified limit. If you disable or do not configure this policy setting, the default number will be 5 connections per user.
Computer	Windows Remote Shell	Specify idle Timeout	At least Windows Vista or later	Configures maximum time in milliseconds remote shell will stay open without any user activity until it is automatically deleted. Any value from 0 to 0x7FFFFFFF can

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				be set, where 0 indicates infinite timeout. If you enable this policy setting the server will wait for the specified amount of time since the last received message from the client before terminating the open shell. If you do not configure or disable this policy setting the default value of 900000 or 15 min will be used.
Computer	Windows Remote Shell	Specify maximum amount of memory in MB per Shell	At least Windows Vista or later	Configures maximum total amount of memory that can be allocated by any active remote shell and all its child processes. Any value from 0 to 0x7FFFFFFF can be set, where 0 equals unlimited memory, which means the ability of remote operations to allocate memory is only limited by the available virtual memory. If you enable this policy setting, the remote operation will be terminated when a new allocation exceeds the specified quota. If you disable or do not configure this policy setting, the value 0 will used by default.
Computer	Windows Remote Shell	Specify maximum number of processes per Shell	At least Windows Vista or later	Configures the maximum number of processes any shell operations are allowed to launch. Any number from 0 to 0x7FFFFFFF can be set, where 0 means unlimited number of processes. If you enable this policy setting, the remote operation will be terminated when it attempts to launch a new process and the process count exceeds the specified limit. If you disable or do not configure this policy setting, the limit will be 5 processes per shell.
Computer	Windows Remote Shell	Specify maximum number of remote shells per user	At least Windows Vista or later	Configures maximum number of concurrent shells any user can remotely open on the same system. Any number from 0 to 0x7FFFFFFF cand be set, where 0 means unlimited number of shells. If you enable this policy setting, the user will not be able to open new remote shells if the count exceeds the specified limit. If you disable or do not configure this policy setting, by default the limit will be set to 2 remote shells per user.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Windows Remote Shell	Specify Shell Timeout	At least Windows Vista or later	Configures maximum time in milliseconds that the remote command or script will be allowed to execute. Any value from 0 to 0x7FFFFFFF can be set, where 0 indicates infinite timeout. If you enable this policy setting the server will terminate the command in progress if it takes longer than the specified amount of time. If you do not configure or disable this policy setting, the default value of 2880000 or 8 hours will be used.
Computer/User	Windows Sidebar	Disable unpacking and installation of gadgets that are not digitally signed.	At least Windows Vista or later	Sidebar gadgets can be deployed as compressed files, either digitally signed or unsigned. If you enable this setting, Windows Sidebar will not extract any gadgets that have not been digitally signed. If you disable or do not configure this setting, Windows Sidebar will extract both signed and unsigned gadgets. The default is for Windows Sidebar to extract both signed and unsigned gadgets.
Computer/User	Windows Sidebar	Override the More Gadgets Link	At least Windows Vista or later	The Windows Sidebar contains a link to allow users to download more gadgets from a website. Microsoft hosts a default website where many gadget authors can post their gadgets. This link can be redirected to a website where alternate gadgets should be available. If you enable this setting, the Gadget Gallery in the Windows Sidebar will direct users to the alternate web site. If you disable or do not configure this setting, Windows Sidebar will direct users to the default web site. The default is for Windows Sidebar to direct users to the default web site.
Computer/User	Windows Sidebar	Turn Off User Installed Windows Sidebar Gadgets	At least Windows Vista or later	The Windows Sidebar will run gadgets that are located in the profile space of the user. Gadgets are small applets that are run by the Windows Sidebar on the Sidebar or on the desktop. If you enable this setting, Windows Sidebar will not run any user installed gadgets. If you disable or do not configure this setting, Windows Sidebar will run user installed gadgets. The default is for Windows

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Sidebar to run user installed gadgets.
Computer/User	Windows Sidebar	Turn off Windows Sidebar	At least Windows Vista or later	Windows Sidebar is a feature that allows the use of gadgets, which are small applets that may display information or utilities to the user. If you enable this setting, Windows Sidebar will be turned off. If you disable or do not configure this setting, Windows Sidebar will be turned on. The default is for Windows Sidebar to be turned on.
Computer/User	Windows SideShow	Delete data from devices running Microsoft firmware when a user logs off from the computer.	At least Windows Vista or later	This policy setting deletes all data stored on Windows SideShow-compatible devices (running Microsoft firmware) when a user logs off from the computer. This is a security precaution but it significantly limits the usefulness of the devices. If you enable this policy setting, all data stored on devices running Microsoft firmware will be deleted when a user logs off from the computer. Data will be re-sent to the device when the user logs on again. If you disable or do not configure this policy setting, data will not be deleted from these devices when users log off from the computer. Users can enable this setting in the Windows SideShow Control Panel. Note Devices not running Microsoft firmware will not be affected by this policy setting.
Computer/User	Windows SideShow	Require a PIN to access data on devices running Microsoft firmware	At least Windows Vista or later	This policy setting requires users to enter a default personal identification number (PIN) to unlock and access data on the device after a specified period of inactivity (time-out period). This setting applies to Windows SideShow-compatible devices running Microsoft firmware. If you enable this policy setting, users will be required to enter the default PIN to unlock and access data on the device after the specified time-out period. Note Users can change the PIN and time-out periods on the device settings page in the Windows SideShow Control Panel. If you disable

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				or do not configure this policy setting, users will not be required to enter a default PIN to unlock and access data on the device after a specified time-out period. However, users can choose to turn on PIN locking and can change the time-out period in the Windows SideShow Control Panel. Note Devices not running Microsoft firmware will not be affected by this policy setting. Note There is a fixed set of time-out periods which includes: after 1 minute, after 2 minutes, after 5 minutes, after 10 minutes, after 30 minutes, when the screen turns off, never.
Computer/User	Windows SideShow	Turn off automatic wake	At least Windows Vista or later	This policy setting turns off the option to periodically wake the computer to update information on Windows SideShow-compatible devices. If you enable this policy setting, the option to automatically wake the computer will not be available in the Windows SideShow Control Panel. If you disable or do not configure this policy setting, the option to automatically wake the computer will be available in the Windows SideShow Control Panel. However, the option will be disabled by default. Note Information on Windows SideShow-compatible devices will only be updated when the computer is on and awake.
Computer/User	Windows SideShow	Turn off Windows SideShow	At least Windows Vista or later	This policy setting turns off Windows SideShow. If you enable this policy setting, the Windows SideShow Control Panel will be disabled and data from Windows SideShow-compatible gadgets (applications) will not be sent to connected devices. If you disable or do not configure this policy setting, Windows SideShow is on by default.
Computer	Windows System Resource Manager	Set the Email IDs to which notifications are to be sent	At least Windows Vista or later	This setting assigns the email address(es) to which notifications will be sent. Use a semicolon (;) to separate multiple email addresses. If you enable this setting, Windows System Resource Manager (WSRM) will send notifications to the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				address(es) specified. If you disable this setting, no email addresses (default value) will be set. If you do not configure this setting, the user may specify e-mail addresses to receive notifications. This value can be e-mail aliases or e-mail address including domain name (for example, someone@example.com). Depending on the events selected for notification, these email addresses will be notified. Note : To receive notifications, the notifications setting on the event log must be turned ON. To view the list of events, click Error, Warning, or Information, and then click OK. If you select Error, Warning, or Information, all of the individual events in that category are included.
Computer	Windows System Resource Manager	Set the SMTP Server used to send notifications	At least Windows Vista or later	This setting assigns the address of the SMTP server that sends out notifications. If you enable this setting, Windows System Resource Manager (WSRM) will set the SMTP server to the value specified. If you disable this setting, no SMTP server (default value) will be set. If you do not configure this setting, the user may specify an SMTP server. This value can be the NetBIOS name or the fully qualified domain name (FQDN) of the Simple Mail Transfer Protocol (SMTP) server. This server contains the email addresses that are configured to receive notifications. Note : To receive email notifications, the notifications setting on the event log must be turned ON. To view the list of events, click Error, Warning, or Information, and then click OK. If you select Error, Warning, or Information, all of the individual events in that category are included.
Computer	Windows System Resource Manager	Set the Time interval in minutes for logging accounting data	At least Windows Vista or later	This setting directs the Accounting feature to log data on the accounting server at the specified time interval. If you enable this setting, Windows System Resource Manager (WSRM) will set the accounting time interval to the value specified. If

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				you disable this setting, the default value of 10 minutes will be set. If you do not configure this setting, the user may specify an accounting interval. The value is specified in minutes and can range between 2 minutes and 60000 minutes. Ten minutes is provided as the default value as this would be an optimal value if there are many servers logging data remotely. Setting an accounting record write interval value less than 10 minutes for a server on a network with more than 20 machines logging data remotely can possibly degrade performance. Note : Set the accounting record write interval to a higher value as the number of machines increases on the network to reduce network congestion.
Computer	Windows System Resource Manager	Turn on Accounting for WSRM	At least Windows Vista or later	This setting turns the Accounting feature On or Off. If you enable this setting, Windows System Resource Manager (WSRM) will start accounting various usage statistics of the processes. If you disable this setting, WSRM will stop logging usage statistics of processes. If you do not configure this setting, the user can specify whether accounting needs to be turned On or Off. The accounting processes is disabled by default. The accounting database provides an interface you can use to manage both the information in the database and the physical size of the database. Managing database information involves finding relevant information and then organizing it efficiently. Managing the physical size of the database requires regular attention because, unless it is configured to do otherwise, Windows System Resource Manager continues to store accounting information. As a result, the size of the database continues to increase. To manage the size of the database, you can archive accounting data for later use or delete it from the database. You can use accounting data can to monitor resource

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				usage, compare actual and expected performance, assess whether the computer's physical resources are sufficient for its intended tasks, and provide the basis for charge-back accounting.
Computer	Windows Update	Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates	At least Windows Vista or later	Specifies whether the Windows Update will use the Windows Power Management features to automatically wake up the system from hibernation, if there are updates scheduled for installation. Windows Update will only automatically wake up the system if Windows Update is configured to install updates automatically. If the system is in hibernation when the scheduled install time occurs and there are updates to be applied, then Windows Update will use the Windows Power management features to automatically wake the system up to install the updates. Windows update will also wake the system up and install an update if an install deadline occurs. The system will not wake unless there are updates to be installed. If the system is on battery power, when Windows Update wakes it up, it will not install updates and the system will automatically return to hibernation in 2 minutes.
Computer	Windows Update	Turn on recommended updates via Automatic Updates	At least Windows Vista or later	Specifies whether Automatic Updates will deliver both important as well as recommended updates from the Windows Update update service. When this policy is enabled, Automatic Updates will install recommended updates as well as important updates from Windows Update update service. When disabled or not configured Automatic Updates will continue to deliver important updates if it is already configured to do so.
Computer	WinRM Client	Allow Basic authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. If you enable this policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting, the WinRM client will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text. If you disable or do not configure this policy setting, then the WinRM client will not use Basic authentication.
Computer	WinRM Client	Allow unencrypted traffic	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network.
Computer	WinRM Client	Disallow Digest authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication. If you enable this policy setting, the WinRM client will not use Digest authentication. If you disable or do not configure this policy setting, the WinRM client will use Digest authentication.
Computer	WinRM Client	Disallow Kerberos authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Kerberos authentication directly. If you enable this policy setting, the Windows Remote Management (WinRM) client will not use Kerberos authentication directly. Kerberos may still be used if the WinRM client is using the Negotiate authentication and Kerberos is selected. If you disable or do not configure this policy setting, the WinRM client will use the Kerberos authentication directly.
Computer	WinRM Client	Disallow Negotiate authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Management (WinRM) client will not use Negotiate authentication. If you enable this policy setting, the WinRM client will not use Negotiate authentication. If you disable or do not configure this policy setting, the WinRM client will use Negotiate authentication.
Computer	WinRM Client	Trusted Hosts	At least Windows Vista or later	This policy setting allows you to manage whether Windows Remote Management (WinRM) client uses the list specified in TrustedHostsList to determine if the destination host is a trusted entity. If you enable this policy setting, the WinRM client uses the list specified in TrustedHostsList to determine if the destination host is a trusted entity. The WinRM client uses this list when neither HTTPS nor Kerberos are used to authenticate the identity of the host. If you disable or do not configure this policy setting and the WinRM client needs to use the list of trusted hosts, you must configure the list of trusted hosts locally on each computer.
Computer	WinRM Service	Allow automatic configuration of listeners	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port. If you enable this policy setting, the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port. If you disable or do not configure this policy setting, then the WinRM service does not automatically listen on the network and you must manually create listeners on every computer. To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting with exceptions for Port 80 (default port for HTTP) and 443 (default port for HTTPS). The service listens on the addresses specified by the IPv4 and IPv6 filters. IPv4 filter specifies one or more ranges of IPv4 addresses

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				and IPv6 filter specifies one or more ranges of IPv6addresses. If specified, the service enumerates the available IP addresses on the computer and uses only addresses that fall within one of the filter ranges. You should use asterisk (*) to indicate that the service listens on all available IP addresses on the computer. When * is used, other ranges in the filter are ignored. If the filter is left blank, the service does not listen on any addresses. For example, if you want the service to listen only on IPv4 addresses, leave the IPv6 filter empty. Ranges are specified using the syntax IP1-IP2. Multiple ranges are separated using "," (comma) as the delimiter. Example IPv4 filters: 2.0.0.1-2.0.0.20, 24.0.0.1-24.0.0.22 Example IPv6 filters: 3FFE:FFFF:7654:FEDA:1245:BA98:0000:0000-3FFE:FFFF:7654:FEDA:1245:BA98:3210:4562
Computer	WinRM Service	Allow Basic authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client. If you enable this policy setting, the WinRM service will accept Basic authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service will not accept Basic authentication from a remote client.
Computer	WinRM Service	Allow unencrypted traffic	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	WinRM Service	Disallow Kerberos authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not accept Kerberos credentials over the network. If you enable this policy setting, the WinRM service will not accept Kerberos credentials over the network. If you disable or do not configure this policy setting, then the WinRM service will accept Kerberos authentication from a remote client.
Computer	WinRM Service	Disallow Negotiate authentication	At least Windows Vista or later	
Node	Subnode	Full-policy Name	Supported On	
Computer/User	Accessories	Do not allow Inkball to run	At least Windows Vista or later	
Computer/User	Accessories	Do not allow printing to Journal Note Writer	At least Windows Vista or later	Prevents printing to Journal Note Writer. If you enable this policy, the Journal Note Writer printer driver will not allow printing to it. It will remain displayed in the list of available printers, but attempts to print to it will fail. If you disable this policy, you will be able to use this feature to print to a Journal Note. If you do not configure this policy, users will be able to use this feature to print to a Journal Note.
Computer/User	Accessories	Do not allow Snipping Tool to run	At least Windows Vista or later	Prevents the snipping tool from running. If you enable this policy setting, the Snipping Tool will not run. If you disable this policy setting, the Snipping Tool will run. If you do not configure this policy setting, the Snipping Tool will run.
Computer/User	Accessories	Do not allow Sticky Notes to be run	At least Windows Vista or later	Prevents start of Sticky Notes. If you enable this policy, the Sticky Notes accessory will not run. If you disable this policy, the Sticky Notes accessory will run. If you do not configure this policy, the Sticky Notes accessory will run.
Computer/User	Accessories	Do not allow Windows Journal to be run	At least Windows Vista or later	Prevents start of Windows Journal. If you enable this policy, the Windows Journal accessory will not run. If you disable this policy, the Windows Journal accessory

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				will run. If you do not configure this policy, the Windows Journal accessory will run.
Computer	ActiveX Installer Service	Approved Installation Sites for ActiveX Controls	At least Windows Vista or later	The ActiveX Installer Service is the solution to delegate the install of per-machine ActiveX controls to a Standard User in the enterprise. The list of Approved ActiveX Install sites contains the host URL and the policy settings for each host URL. Wild cards are not supported.
Computer	Advanced Error Reporting Settings	Configure Corporate Windows Error Reporting	At least Windows Vista or later	This setting determines the corporate server to which Windows Error Reporting will send reports (instead of sending reports to Microsoft). Server port indicates the port to use on the target server. Connect using SSL determines whether Windows will send reports to the server using a secured connection.
Computer/User	Advanced Error Reporting Settings	Configure Report Archive	At least Windows Vista or later	This setting controls the behavior of the Windows Error Reporting archive. If Archive behavior is set to "Store all", all data collected for each report will be stored in the appropriate location. If Archive behavior is set to "Store parameters only", only the minimum information required to check for an existing solution will be stored. The setting for "Maximum number of reports to store" determines how many reports can be stored before old reports are automatically deleted. If this setting is disabled, no Windows Error Reporting information will be stored.
Computer/User	Advanced Error Reporting Settings	Configure Report Queue	At least Windows Vista or later	This setting determines the behavior of the Windows Error Reporting queue. If Queuing behavior is set to "Default", Windows will decide each time a problem occurs whether the report should be queued or the user should be prompted to send it immediately. If Queuing behavior is set to "Always queue", all reports will be queued until the user is notified to send them or until the user chooses to send them using the Solutions to Problems control panel. If Queuing behavior is set to

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				"Always queue for administrator", reports will be queued until an administrator is notified to send them or chooses to send them using the Solutions to Problems control panel. The setting for "Maximum number of reports to queue" determines how many reports can be queued before old reports are automatically deleted. The setting for "Number of days between solution check reminders" determines the interval time between the display of system notifications which remind the user to check for solutions to problems. A setting of 0 will disable the reminder. If the Windows Error Reporting queue setting is disabled, no Windows Error Reporting information will be queued and users will be able to send reports only at the time a problem occurs.
Computer/User	Advanced Error Reporting Settings	List of applications to be excluded	At least Windows Vista or later	This setting determines the behavior of the error reporting exclusion list. Windows will not send reports for any process added to this list. Click "Show" to display the exclusion list. Click "Add..." and type a process name to add a process to the list. Select a process name and click "Remove" to remove a process from the list. Click "OK" to save the list.
Computer	Application, Security, Setup, System	Backup log automatically when full	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size and takes effect only if the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled. If you enable this policy setting and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, the Event Log file is automatically closed and renamed when it is full. A new file is then started. If you disable this policy setting and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, then new events are discarded and the old events are retained. When this policy setting is not configured and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, new

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				events are discarded and the old events are retained.
Computer	Application, Security, Setup, System	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer/User	Application Compatibility	Turn Off Program Compatibility Assistant	At least Windows Vista or later	This policy controls the state of the Program Compatibility Assistant in the system. The PCA monitors user initiated programs for known compatibility issues at run time. Whenever a potential issue with an application is detected, the PCA will prompt the user with pointers to recommended solutions. For more information on the various issue detection scenarios covered by PCA and the policies to configure them, refer to policies under System-&gt;Troubleshooting and Diagnostics-&gt;Application Compatibility Diagnostics. The PCA is on by default. If you enable this policy setting, the PCA will be turned off. This option is useful for system administrators who require faster performance and are aware of the compatibility of the applications they are using. Note: With the PCA turned off, the user will not be presented with solutions to known compatibility issues when running applications. If you disable or do not configure this policy setting, the PCA will be turned on. Note: The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Application Compatibility Diagnostics	Detect application failures caused by deprecated Windows DLLs or COM objects	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose DLL load or COM object creation failures in programs. If you enable this policy setting, the PCA detects programs trying load legacy Microsoft Windows DLLs or creating legacy COM objects that are removed in this version of Windows. When this failure is detected, after the program is terminated, PCA will notify the user about this problem and provide an option to check the Microsoft Web site for solutions. If you disable this policy setting, the PCA does not detect programs trying to load legacy Windows DLLs or creating legacy COM objects. If you do not configure this policy setting, the PCA detects programs trying to load legacy Windows DLLs or creating legacy COM objects. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect application install failures	At least Windows Vista or later	This policy setting configures the Program Compatibility Assistant (PCA) to diagnose failures with application installations. If you enable this policy setting, the PCA is configured to detect failures in the execution of application installers through heuristics. When potential failures are detected, the PCA will provide the user with an option to restart the installer with Microsoft Windows XP compatibility mode. If you disable this policy setting, the PCA is not configured to detect failures in execution of program installers. If you do not configure this policy setting, the PCA will enable this diagnostic scenario by default. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect application installers that need to be run as administrator	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose failures with application installers that are not detected to run as administrator. If you enable this policy setting, the PCA is configured to detect application installers which do not have privileges to run as administrator by the User Access Control (UAC). When potential failures are detected, the PCA will provide the user with an option to restart the installer as administrator. If you disable this policy setting, the PCA will not detect application installers which do not have privileges to run as administrator by the UAC. If you do not configure this policy setting, the PCA will be configured to detect application installers which do not have privileges to run as administrator by the UAC. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect applications unable to launch installers under UAC	At least Windows Vista or later	This policy setting configures the Program Compatibility Assistant (PCA) to diagnose failures with programs under User Account Control (UAC). If you enable this policy setting, the PCA detects programs that failed to launch child processes that are installers (typically updaters). When this failure is detected, the PCA will apply the ELEVATECREATEPROCESS compatibility mode, which enables the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				program to successfully launch the installer as with administrator privileges the next time the program is run. If you disable this policy setting, the PCA will not detect applications that fail to launch installers run under UAC. If you do not configure this policy setting, the PCA detects programs that failed to launch child processes that are installers (typically updaters). Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Notify blocked drivers	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose drivers blocked due to compatibility issues. If you enable this policy setting, the PCA will notify the user of blocked driver issues with an option to check the Microsoft Web site for solutions. If you disable this policy setting, the PCA will not notify the user of blocked driver issues. Note: With this policy setting in a disabled state, the user will not be presented with solutions to blocked drivers. If you do not configure this policy setting, the PCA will notify the user of blocked driver issues with an option to check the Microsoft Web site for solutions. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application, Security,	**Log Access**	At least Windows Vista or later	This policy setting specifies to use the security descriptor for the log using the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Setup, System			Security Descriptor Definition Language (SDDL) string. If this policy setting is enabled, only those users matching the security descriptor can access the log. If this policy setting is disabled or not configured, then all authenticated users and system services can write/read/clear this log.
Computer	Application, Security, Setup, System	**Log File Path**	At least Windows Vista or later	This policy setting controls the location of the log file. The location of the file must be writable by the Event Log service and should only be accessible to administrators. If you enable this policy setting, the Event Log uses the specified path provided in this policy setting. If you disable or do not configure this policy setting, the Event Log uses the system32 or system64 subdirectory.
Computer	Application, Security, Setup, System	Maximum Log Size (KB)	At least Windows Vista or later	This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file maximum size will be set to the local configuration value. This value can be changed by the local administrator using the log properties dialog and it defaults to 20 megabytes.
Computer/User	AutoPlay Policies	Default behavior for AutoRun	At least Windows Vista or later	Sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior in Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				represented as a handler in the Autoplay dialog. If you enable this policy, an Administrator can change the default Windows Vista behavior for autorun to: A) Completely disable autorun commands, or B) Revert back to Pre-Windows Vista behavior of automatically executing the autorun command. If you disable or not configure this policy, Windows Vista will prompt the user whether autorun command is to be run.
Computer/User	AutoPlay Policies	Don't set the always do this checkbox	At least Windows Vista or later	If this policy is enabled, the "Always do this..." checkbox in Autoplay dialog will not be set by default when the dialog is shown.
Computer	Background Intelligent Transfer Service (BITS)	Allow BITS Peercaching	At least Windows Vista or later	This setting determines if the BITS Peer-caching feature is enabled on a specific computer. By default, the files in a BITS job are downloaded only from the originating server specified by the jobΓÇÖs owner. Each client computer will download its own copy of the files from the origin server. If BITS Peer-caching is enabled, BITS will cache download jobs and make the content available to other BITS peers. When running a download job, BITS will first request the files for the job from one of its peers in the same IP subnet. If none of the peers in the subnet have the requested files, BITS will download the files for the job from the original server. If you enable this setting, BITS will cache jobs, respond to content requests from peers, and download job content from peers if possible. If you disable this setting or do not configure it, the peer-caching feature will be disabled and BITS will download files directly from the original server.
Computer	Background Intelligent Transfer Service (BITS)	Do not allow the computer to act as a BITS Peercaching client	At least Windows Vista or later	This setting specifies whether the computer will act as a BITS peercaching client. By default, when BITS peercaching is enabled, the computer acts as both a peercaching server (offering files to its peers) and a peercaching client

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				(downloading files from its peers). If you enable this setting, the computer will no longer use the BITS Peercaching feature to download files; files will be downloaded only from the origin server. However, the computer will still make files available to its peers. If you disable or do not configure this setting, the computer attempts to download peer enabled BITS jobs from peer computers before reverting to the origin server. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Do not allow the computer to act as a BITS Peercaching server	At least Windows Vista or later	This setting specifies whether the computer will act as a BITS peercaching server. By default, when BITS peercaching is enabled, the computer acts as both a peercaching server (offering files to its peers) and a peercaching client (downloading files from its peers). If you enable this setting, the computer will no longer cache downloaded files and offer them to its peers. However, the computer will still download files from peers. If you disable or do not configure this setting, the computer will offer downloaded and cached files to its peers. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Limit age of items in the BITS Peercache	At least Windows Vista or later	This setting specifies the maximum age of files in the Peercache. In order to make the most efficient use of disk space, by default BITS removes any files in the cache older than 14 days. If you enable this setting, you can specify the maximum age of files in the cache in days. You can enter a value between 1 and 120 Days. If you disable this setting or do not configure it, files older than 14 days will be removed from the Peercache. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Background Intelligent Transfer Service (BITS)	Limit the BITS Peercache size	At least Windows Vista or later	This setting specifies the maximum amount of disk space that can be used for the BITS Peercache, as a percentage of the total system disk size. BITS will add files to the Peercache and make those files available to peers until the cache content reaches the specified cache size. By default, BITS will use 1% of the total system disk for the peercache. If you enable this setting, you can enter the percentage of disk space to be used for the BITS peercache. You can enter a value between 1% and 80%. If you disable this setting or do not configure it, the default size of the BITS peercache is 1% of the total system disk size. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Maximum BITS job download time	At least Windows Vista or later	This setting limits the amount of time that BITS will take to download the files in a BITS job. The time limit applies only to the time that BITS is actively downloading files, not real-time. When the cumulative download time exceeds this limit, the job is placed in the error state. By default BITS uses a maximum download time of 15 days (54000 seconds). If you enable this setting, you can set the maximum job download time to the specified number of seconds. If you disable or do not configure this setting, the default value of 15 days (54000 seconds) will be used for the maximum job download time.
Computer	Background Intelligent Transfer Service (BITS)	Maximum network bandwidth used for Peercaching	At least Windows Vista or later	This setting limits the network bandwidth that BITS uses for peercache transfers (this setting does not affect transfers from the origin server). To prevent any negative impact to a computer caused by serving other peers, by default BITS will use up to 30% of the bandwidth of the slowest active network interface. For example, if a computer has both a 100Mbps network card, and a 56 Kbps modem, and both are active, BITS will use a maximum of 30% of 56Kbps. You

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				can change the default behavior of BITS, and specify a fixed maximum bandwidth that BITS will use for Peercaching. If you enable this setting, you can enter a value in bits per second (bps) between 1048576 and 4294967200 to use as the maximum network bandwidth used for peer-caching. If you disable this setting or do not configure it, the default value of 30% of the slowest active network interface will be used. Note: This setting has no effect if the ΓÇ£Allow BITS peercachingΓÇ¥ setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of BITS jobs for each user	At least Windows Vista or later	This setting specifies the maximum number of BITS jobs that can be created by a user. By default, BITS limits the total number of jobs that can be created by a user to 60 jobs. You can use this setting to raise or lower the maximum number of BITS jobs a user can create. If you enable this setting, BITS will limit the maximum number of BITS jobs a user can create to the specified number. If you disable or do not configure this setting, BITS will use the default user BITS job limit of 300 jobs. Note: This limit must be lower than the setting specified in ΓÇ£Maximum number of BITS jobs for this computerΓÇ¥, or 300 if the ΓÇ£Maximum number of BITS jobs for this computerΓÇ¥ setting is not configured. BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of BITS jobs for this computer	At least Windows Vista or later	This setting specifies the maximum number of BITS jobs that can be created for all users of the computer. By default, BITS limits the total number of jobs that can be created on the computer to 300 jobs. You can use this setting to raise or lower the maximum number of user BITS jobs. If you enable this setting, BITS will limit the maximum number of BITS jobs to the specified number. If you disable or do

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				not configure this setting, BITS will use the default BITS job limit of 300 jobs. Note: BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of files allowed in a BITS job	At least Windows Vista or later	This setting specifies the maximum number of files that a BITS job can contain. By default, a BITS job is limited to 200 files. You can use this setting to raise or lower the maximum number of files a BITS jobs can contain. If you enable this setting, BITS will limit the maximum number of files a job can contain to the specified number. If you disable or do not configure this setting, BITS will use the default value of 200 for the maximum number of files a job can contain. Note: BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of ranges that can be added to the file in a BITS job	At least Windows Vista or later	This setting specifies the maximum number of ranges that can be added to a file in a BITS job. By default, files in a BITS job are limited to 500 ranges per file. You can use this setting to raise or lower the maximum number ranges per file. If you enable this setting, BITS will limit the maximum number of ranges that can be added to a file to the specified number. If you disable or do not configure this setting, BITS will limit ranges to 500 ranges per file. Note: BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	BitLocker Drive Encryption	Configure encryption method	At least Windows Vista or later	This policy setting allows you to configure the algorithm and key size used by BitLocker Drive Encryption. This policy setting applies on a fully-decrypted disk. Changing the encryption method has no effect if the disk is already encrypted or if encryption is in progress. If you enable this policy setting, you can configure the encryption method used on an unencrypted volume. Consult online

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				documentation for more information about the available encryption methods. If you disable or do not configure this policy setting, BitLocker will use the default encryption method of AES 128 bit with Diffuser or the encryption method specified by a local administrator's setup script.
Computer	BitLocker Drive Encryption	Configure TPM platform validation profile	At least Windows Vista or later	This policy setting allows you to configure how the computer's Trusted Platform Module (TPM) security hardware secures the BitLocker encryption key. This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection. If you enable this policy setting before turning on BitLocker, you can configure the boot components that the TPM will validate before unlocking access to the BitLocker-encrypted OS volume. If any of these components change while BitLocker protection is in effect, the TPM will not release the encryption key to unlock the volume and the computer will enter into recovery mode during boot. If you disable or do not configure this policy setting, the TPM uses the default platform validation profile or the platform validation profile specified by a local administrator's setup script. The default platform validation profile secures the encryption key against changes to the Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions (PCR 0), the Option ROM Code (PCR 2), the Master Boot Record (MBR) Code (PCR 4), the NTFS Boot Sector (PCR 8), the NTFS Boot Block (PCR 9), the Boot Manager (PCR 10), and the BitLocker Access Control (PCR 11). WARNING: Changing from the default profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending upon inclusion or exclusion

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				(respectively) of the PCRs.
Computer	BitLocker Drive Encryption	Control Panel Setup: Configure recovery folder	At least Windows Vista or later	This policy setting allows you to specify the default path that is displayed when the BitLocker Drive Encryption setup wizard prompts the user to enter the location of a folder in which to save the recovery password. If you enable this policy setting, you can specify the path that will be used as the default folder location when the user chooses the option to save the recovery password in a folder. You can specify either a fully-qualified path or include the target computer's environment variables in the path. If the path is not valid, the BitLocker setup wizard will display the computer's top-level folder view. If you disable or do not configure this policy setting, the BitLocker setup wizard will display the computer's top-level folder view when the user chooses the option to save the recovery password in a folder. Note: In all cases, the user will be able to select other folders in which to save the recovery password.
Computer	BitLocker Drive Encryption	Control Panel Setup: Configure recovery options	At least Windows Vista or later	This policy setting allows you to configure whether the BitLocker Drive Encryption setup wizard will ask the user to save BitLocker recovery options. Two recovery options can unlock access to BitLocker-encrypted data. The user can type a random 48-digit numerical recovery password. The user can also insert a USB flash drive containing a random 256-bit recovery key. If you enable this policy setting, you can configure the options that the setup wizard exposes to users for recovering BitLocker. For example, disallowing the 48-digit recovery password will prevent users from being able to print or save recovery information to a folder. If you disable or do not configure this policy setting, the BitLocker setup wizard will present users with ways to store recovery options. Saving to a USB flash drive will

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				store the 48-digit recovery password as a text file, and the 256-bit recovery key as a hidden file. Saving to a folder will store the 48-digit recovery password as a text file. Printing will provide the 48-digit recovery password. Note: If TPM initialization is needed during the BitLocker setup, TPM owner information will be saved or printed with the BitLocker recovery information. Note: The 48-digit recovery password will not be available in FIPS compliance mode. IMPORTANT: To prevent data loss, you must have a way to recover BitLocker. If you disallow both recovery options below, you must enable the policy setting to "Turn on BitLocker backup to Active Directory Domain Services". Otherwise, a policy error occurs.
Computer	BitLocker Drive Encryption	Control Panel Setup: Enable advanced startup options	At least Windows Vista or later	This policy setting allows you to configure whether the BitLocker Drive Encryption setup wizard will ask the user to set up an additional authentication that is requested each time the computer starts. On a computer with a compatible Trusted Platform Module (TPM), two types of startup authentications can work to provide added protection for encrypted data. When the computer starts, it can require users to insert a USB flash drive containing a startup key. It can also require users to enter a 4 to 20 digit startup PIN. A USB flash drive containing a startup key is needed on computers without a compatible Trusted Platform Module (TPM). Without a TPM, BitLocker-encrypted data is protected solely by the key material on this USB flash drive. If you enable this policy setting, the wizard will show the page to allow the user to configure advanced startup options for BitLocker. You can further configure setting options for computers with and without a TPM. If you disable or do not configure this policy setting, the BitLocker setup wizard will display basic steps that allow users to enable BitLocker on

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				computers with a TPM. In this basic wizard, no additional startup key or startup PIN can be configured.
Computer	BitLocker Drive Encryption	Turn on BitLocker backup to Active Directory Domain Services	At least Windows Vista or later	This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of BitLocker Drive Encryption recovery information. If you enable this policy setting, BitLocker recovery information will be automatically and silently backed up to AD DS when BitLocker is turned on for a computer. BitLocker recovery information includes the recovery password and some unique identifier data. You can also include a package that contains a BitLocker-protected volume's encryption key. This key package is secured by one or more recovery passwords and may help perform specialized recovery when the disk is damaged or corrupted. If you select the option to "Require BitLocker backup to AD DS", BitLocker cannot be turned on unless the computer is connected to the domain and the AD DS backup succeeds. This option is selected by default to help ensure that BitLocker recovery is possible. Otherwise, AD DS backup is attempted but network or other backup failures do not impact BitLocker setup. Backup is not automatically retried and the recovery password may not have been stored in AD DS during BitLocker setup. If you disable or do not configure this policy setting, BitLocker recovery information will not be backed up to AD DS. IMPORTANT: To prevent data loss, you must have a way to recover BitLocker. Note: You must first set up appropriate schema extensions and access control settings on the domain before AD DS backup can succeed. Consult online documentation for more information about setting up Active Directory Domain Services for BitLocker. Note: TPM initialization may be needed during BitLocker

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setup. Enable the policy setting to "Turn on TPM backup to Active Directory Domain Services" in "System\Trusted Platform Module Services\" to ensure that TPM information is also backed up.
Computer	Button Settings	Select the Lid Switch Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user closes the lid on a mobile PC. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Lid Switch Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user closes the lid on a mobile PC. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Power Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the power button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Power Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the power button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Sleep Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the sleep button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Button Settings	Select the Sleep Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the sleep button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Start Menu Power Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the user interface sleep button. Possible actions include: -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Start Menu Power Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the user interface sleep button. Possible actions include: -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer/User	Client	Prevent backing up to local disks	At least Windows Vista or later	This setting lets you prevent users from selecting a local disk (internal or external) for storing file backups. If this setting is enabled, the user will be blocked from selecting a local disk as a file backup location. If this setting is disabled or not configured, users can select a local disk as a file backup location.
Computer/User	Client	Prevent backing up to network shared folder	At least Windows Vista or later	This setting lets you prevent users from selecting a network shared folder for storing file backups. If this setting is enabled, users will be blocked from selecting a network shared folder as a file backup location. If this setting is disabled or not configured, users can select a network shared folder as a file backup location.
Computer/User	Client	Prevent backing up to optical media (CD/DVD)	At least Windows Vista or later	This setting lets you prevent users from selecting optical media (CD/DVD) for storing file backups. If this setting is enabled, users will be blocked from selecting optical media as a file backup location. If this setting is disabled or not configured,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				users can select optical media as a file backup location.
Computer/User	Client	Prevent the user from running the Backup Status and Configuration program	At least Windows Vista or later	This setting lets you disable the Backup Status and Configuration program, which links to the file backup, file restore, and Complete PC Backup applications and shows backup status. If this setting is enabled, a user cannot start the Backup Status and Configuration program. If this setting is disabled or not configured, users can start the Backup Status and Configuration program.
Computer/User	Client	Turn off backup configuration	At least Windows Vista or later	This setting lets you disable file backup functionality. If this setting is enabled, the file backup program is disabled. If this setting is disabled or not configured, the file backup program is enabled and users can create a file backup.
Computer/User	Client	Turn off Complete PC Backup functionality	At least Windows Vista or later	This setting lets you disable Complete PC Backup functionality. If this setting is enabled, the Complete PC Backup program is disabled. If this setting is disabled or not configured, the Complete PC Backup program is enabled and users can create a Complete PC Backup image.
Computer/User	Client	Turn off restore functionality	At least Windows Vista or later	This setting lets you disable file restore functionality. If this setting is enabled, the file restore program is disabled. If this setting is disabled or not configured, the file restore program is enabled and users can restore files.
Computer/User	Consent	Configure Default consent	At least Windows Vista or later	This setting determines the consent behavior of Windows Error Reporting. If Consent level is set to "Always ask before sending data", Windows will prompt the user for consent to send reports. If Consent level is set to "Send parameters", the minimum data required to check for an existing solution will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If Consent level is set to "Send parameters and safe additional data", the minimum data required to check for an existing solution as

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				well as data which Windows has determined does not contain (within a high probability) personally identifiable data will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If Consent level is set to "Send all data", any data requested by Microsoft will be sent automatically. If this setting is disabled or not configured then consent will default to "Always ask before sending data".
Computer/User	Consent	Customize consent settings	At least Windows Vista or later	This policy setting determines the consent behavior of Windows Error Reporting for specific event types. If this policy setting is enabled and the consent level is set to "0" (Disable), Windows Error Reporting will not send any data to Microsoft for this event. If the consent level is set to "1" (Always ask before sending data), Windows will prompt the user for consent to send reports. If the consent level is set to "2" (Send parameters), the minimum data required to check for an existing solution will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If the consent level is set to "3" (Send parameters and safe additional data), the minimum data required to check for an existing solution as well as data which Windows has determined does not contain (within a high probability) personally identifiable data will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If the consent level is set to "4" (Send all data), any data requested by Microsoft will be sent automatically. If this setting is disabled or not configured then consent will default to the default consent setting.
Computer/User	Consent	Ignore custom consent settings	At least Windows Vista or later	This setting determines the behavior of the default consent setting in relation to custom consent settings. If this setting is enabled, the default Consent level

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting will always override any other consent setting. If this setting is disabled or not configured, each custom consent setting will determine the consent level for that event type and the default consent setting will determine the consent level of any other reports.
Computer	Corrupted File Recovery	Configure Corrupted File Recovery Behavior	At least Windows Vista or later	This policy setting allows you to configure the recovery behavior for corrupted files to one of three states: Regular: Detection, troubleshooting, and recovery of corrupted files will automatically start with a minimal UI display. Windows will attempt to present you with a dialog box when a system restart is required. This is the default recovery behavior for corrupted files. Silent: Detection, troubleshooting, and recovery of corrupted files will automatically start with no UI. Windows will log an administrator event when a system restart is required. This behavior is recommended for headless operation. Troubleshooting Only: Detection and troubleshooting of corrupted files will automatically start with no UI. Recovery is not attempted automatically. Windows will log an administrator event with instructions if manual recovery is possible. If you enable this setting, the recovery behavior for corrupted files will be set to either the regular (default), silent, or troubleshooting only state. If you disable this setting, the recovery behavior for corrupted files will be disabled. No troubleshooting or resolution will be attempted. If you do not configure this setting, the recovery behavior for corrupted files will be set to the regular recovery behavior. No system or service restarts are required for changes to this policy to take immediate effect after a Group Policy refresh. Note: This policy setting will take effect only when the Diagnostic Policy Service (DPS) is in the running state. When the service is

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				stopped or disabled, system file recovery will not be attempted. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Credential User Interface	Do not enumerate administrator accounts on elevation.	At least Windows Vista or later	By default all administrator accounts are displayed when attempting to elevate a running application. If you enable this policy, users will be required to always type in a username and password to elevate. If you disable this policy, all local administrator accounts on the machine will be displayed so the user can choose one and enter the correct password.
Computer	Credential User Interface	Require trusted path for credential entry.	At least Windows Vista or later	This policy setting requires the user to enter Microsoft Windows credentials using a trusted path, to prevent a Trojan horse or other types of malicious code from stealing the userΓÇÖs Windows credentials. Note: This policy affects nonlogon authentication tasks only. As a security best practice, this policy should be enabled. If you enable this policy setting, users will be required to enter Windows credentials on the Secure Desktop by means of the trusted path mechanism. If you disable or do not configure this policy setting, users will enter Windows credentials within the userΓÇÖs desktop session, potentially allowing malicious code access to the userΓÇÖs Windows credentials.
Computer	Credentials Delegation	Allow Default Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can be delegated when the authentication mechanism is NTLM (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, delegation of default credentials is not permitted to any machine. Note that "Allow Delegating Default Credentials" policy applies when

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				server authentication was achieved via a trusted X509 certificate or Kerberos. Note: The "Allow Default Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Default Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can be delegated (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, delegation of default credentials is not permitted to any machine. Note: The "Allow Delegating Default Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Fresh	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		Credentials		example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's fresh credentials can be delegated when the authentication mechanism is NTLM (fresh credentials are those that you are prompted for when executing the application). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of fresh credentials is permitted to Terminal Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note: "Allow Delegating Fresh Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow Fresh Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Saved Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can be delegated (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of saved credentials is permitted to Terminal

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note:The "Allow Delegating Saved Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Fresh Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's fresh credentials can be delegated when the authentication mechanism is NTLM (fresh credentials are those that you are prompted for when executing the application). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of fresh credentials is permitted to Terminal Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note: "Allow Delegating Fresh Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow Fresh Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Saved Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can be delegated to when the authentication mechanism is NTLM (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of saved credentials is permitted to Terminal Server running on any machine (TERMSRV/*) if the client machine is not a member of any domain. If the client is domain-joined, then by default the delegation of saved credentials is not permitted to any machine. If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note: that "Allow Delegating Saved Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow Saved Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com
Computer	Credentials Delegation	Deny Delegating Default Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can NOT be delegated to (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, this setting does not specify any server. Note: "The Deny Delegating Default Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Default Credentials" to define exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Default Credentials" server list.
Computer	Credentials Delegation	Deny Delegating Fresh Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's fresh credentials can NOT be delegated (fresh credentials are those that you are prompted for when executing the application). If you disable or do not configure (by default) this policy setting, this setting does not

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				specify any server. Note: The "Deny Delegating Fresh Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Fresh Credentials" to define exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Fresh Credentials" server list.
Computer	Credentials Delegation	Deny Delegating Saved Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can NOT be delegated (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you disable or do not configure (by default) this policy setting, this setting does not specify any server. Note: The "Deny Delegating Saved Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Saved Credentials" to define exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Saved Credentials" server list.
Computer/User	Cursors	Turn off pen feedback	At least Windows Vista or later	Disables visual pen action feedback, except for press and hold feedback. If you enable this policy, all visual pen action feedback is disabled except for press and hold feedback. Additionally, the mouse cursors are shown instead of the pen cursors. If you disable or do not configure this policy, visual feedback and pen cursors will be shown unless the user disables them in Control Panel.
Computer	DC Locator DNS Records	Domain Controller Address Type Returned	At least Windows Vista or later	The Domain Controller (DC) Locator APIs return IP address of the DC with the other part of the information. Before the support of IPv6, the returned DC IP address was IPv4. But with the support of IPv6, the DC Locator APIs can return IPv6 DC address. The returned IPv6 DC address may not be correctly handled by some of the existing applications. So this policy is provided to support such scenarios. By default, DC Locator APIs can return IPv4/IPv6 DC address. But if some applications are broken due to the returned IPv6 DC address, this policy can be used to disable the default behavior and enforce to return ONLY IPv4 DC address. Once applications are fixed, this policy can be used to enable the default behavior. If you enable this policy setting, DC Locator APIs can return IPv4/IPv6 DC address. This is the default behavior of the DC Locator. If you disable this policy setting, DC Locator APIs will ONLY return IPv4 DC address if any. So if the domain controller supports both IPv4 and IPv6 addresses, DC Locator APIs will return IPv4 address. But if the domain controller supports only IPv6 address, then

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				DC Locator APIs will fail. If you do not configure this policy setting, DC Locator APIs can return IPv4/IPv6 DC address. This is the default behavior of the DC Locator.
Computer	DC Locator DNS Records	Force Rediscovery Interval	At least Windows Vista or later	The Domain Controller Locator (DC Locator) service is used by clients to find domain controllers for their Active Directory domain. When DC Locator finds a domain controller, it caches domain controllers to improve the efficiency of the location algorithm. As long as the cached domain controller meets the requirements and is running, DC Locator will continue to return it. If a new domain controller is introduced, existing clients will only discover it when a Force Rediscovery is carried out by DC Locator. To adapt to changes in network conditions DC Locator will by default carry out a Force Rediscovery according to a specific time interval and maintain efficient load-balancing of clients across all available domain controllers in all domains or forests. The default time interval for Force Rediscovery by DC Locator is 12 hours. Force Rediscovery can also be triggered if a call to DC Locator uses the DS_FORCE_REDISCOVERY flag. Rediscovery resets the timer on the cached domain controller entries. If you enable this policy setting, DC Locator on the machine will carry out Force Rediscovery periodically according to the configured time interval. The minimum time interval is 3600 seconds (1 hour) to avoid excessive network traffic from rediscovery. The maximum allowed time interval is 4294967200 seconds, while any value greater than 4294967 seconds (~49 days) will be treated as infinity. If you disable this policy setting, Force Rediscovery will be used by default for the machine at every 12 hour interval. If you do not configure this policy setting, Force

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Rediscovery will be used by default for the machine at every 12 hour interval, unless the local machine setting in the registry is a different value.
Computer	DC Locator DNS Records	Try Next Closest Site	At least Windows Vista or later	The Domain Controller Locator (DC Locator) service is used by clients to find domain controllers for their Active Directory domain. The default behavior for DC Locator is to find a DC in the same site. If none are found in the same site, a DC in another site, which might be several site-hops away, could be returned by DC Locator. Site proximity between two sites is determined by the total site-link cost between them. A site is closer if it has a lower site link cost than another site with a higher site link cost. The Try Next Closest Site feature enables DC Locator to attempt to locate a DC in the nearest site based on the site link cost if a DC in same the site is not found. In scenarios with multiple sites, failing over to the try next closest site during DC Location streamlines network traffic more effectively. If you enable this policy setting, Try Next Closest Site DC Location will be turned on for the machine across all available but un-configured network adapters. If you disable this policy setting, Try Next Closest Site DC Location will not be used by default for the machine across all available but un-configured network adapters. However, if a DC Locator call is made using the DS_TRY_NEXTCLOSEST_SITE flag explicitly, the Try Next Closest Site behavior is honored. If you do not configure this policy setting, Try Next Closest Site DC Location will not be used by default for the machine across all available but un-configured network adapters. If the DS_TRY_NEXTCLOSEST_SITE flag is used explicitly, the Next Closest Site behavior will be used.
User	Desktop	Desktop Wallpaper	At least Windows Vista or later	Specifies the desktop background ("wallpaper") displayed on all users' desktops.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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) or JPEG (*.jpg) 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: This setting does not apply to Terminal Server sessions.
Computer/User	Desktop Window Manager	Do not allow desktop composition	At least Windows Vista or later	This policy setting controls how some graphics are rendered and facilitates other features, including Flip, Flip3D, and Taskbar Thumbnails. If you enable this setting, the desktop compositor visual experience will be turned off. If you disable or do not configure this policy setting, desktop composition will be turned on, if the required hardware is in place.
Computer/User	Desktop Window Manager	Do not allow Flip3D invocation	At least Windows Vista or later	Flip3D is a 3D window switcher. If you enable this setting, Flip3D will be inaccessible. If you disable or do not configure this policy setting, Flip3D will be accessible, if desktop composition is turned on.
Computer/User	Desktop Window	Do not allow window animations	At least Windows Vista or later	This policy setting controls the appearance of window animations such as those

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Manager			found when restoring, minimizing, and maximizing windows. If you enable this setting, window animations will be turned off. If you disable or do not configure this setting, window animations will be turned on.
Computer	Device and Resource Redirection	Do not allow supported Plug and Play device redirection	At least Windows Vista or later	This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Terminal Services session. By default, Terminal Services allows redirection of supported Plug and Play devices. Users can use the ΓÇ£MoreΓÇ¥ option on the Local Resources tab of Remote Desktop Connection to choose the supported Plug and Play devices to redirect to the remote computer. If you enable this policy setting, users cannot redirect their supported Plug and Play devices to the remote computer. If you disable this policy setting or do not configure this policy setting, users can redirect their supported Plug and Play devices to the remote computer. Note: You can also disallow redirection of supported Plug and Play devices on the Client Settings tab in the Terminal Services Configuration tool. You can disallow redirection of specific types of supported Plug and Play devices by using the ΓÇ£Computer Configuration\Administrative Templates\System\Device Installation\Device Installation RestrictionsΓÇ¥ policy settings.
Computer	Device Installation	Allow remote access to the PnP interface	At least Windows Vista or later	Specifies whether or not remote access to the Plug and Play interface is allowed. If you enable this setting, remote connections to the PnP interface will be allowed. If you disable or do not configure this setting, PnP interface will not be available remotely.
Computer	Device Installation	Configure device installation timeout	At least Windows Vista or later	Specifies the number of seconds the system will wait for a device installation task to complete. If the task is not complete within the specified number of seconds,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the system will terminate the installation. If you enable this setting, the system will wait for the number of seconds specified before forcibly terminating the installation. If you disable or do not configure this setting, the system will wait 300 seconds (5 minutes) for any device installation task to complete before terminating installation.
Computer/User	Device Installation	Do not create system restore point when new device driver installed	At least Windows Vista or later	Specifies whether or not a system restore point is created when a new device driver is installed on your machine. If you enable this setting, system restore points will not be created when a new device driver is installed or updated. If you disable or do not configure this setting, a system restore point will be created whenever a new driver is installed or an existing device driver is updated.
Computer	Device Installation	Do not send a Windows Error Report when a generic driver is installed on a device	At least Windows Vista or later	Specifies whether or not to send a Windows Error Report when a generic driver is installed on a device. If you enable this setting, a Windows Error Report will not be sent when a generic driver is installed. If you disable or do not configure this setting, a Windows Error Report will be sent when a generic driver is installed.
Computer	Device Installation	Treat all digitally signed drivers equally in the driver ranking and selection process	At least Windows Vista or later	When selecting which driver to install, do not distinguish between drivers that are signed by a Microsoft Windows Publisher certificate and drivers that are signed by others. If you enable this setting, all valid Authenticode signatures are treated equally for the purpose of selecting a device driver to install. Selection is based on other criteria (such as version number or when the driver was created) rather than whether the driver was signed by a Microsoft Windows Publisher certificate or by another Authenticode certificate. A signed driver is still preferred over a driver that is not signed at all. However, drivers that are signed by Microsoft Windows Publisher certificates are not preferred over drivers signed by other Authenticode

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				certificates. If you disable or do not configure this setting, drivers that are signed by a Microsoft Windows Publisher certificate are selected for installation over drivers that are signed by other Authenticode certificates.
Computer	Device Installation	Turn off "Found New Hardware" balloons during device installation	At least Windows Vista or later	Do not display "Found New Hardware" balloons during device installation. If you enable this setting, "Found New Hardware" balloons will not appear while a device is being installed. If you disable or do not configure this setting, "Found New Hardware" balloons will appear while a device is being installed unless the driver for the device has suppressed the balloons.
Computer	Device Installation Restrictions	Allow administrators to override Device Installation Restriction policies	At least Windows Vista or later	Allows members of the Administrators group to install and update the drivers for any device, regardless of other policy settings. If you enable this setting, administrators can use "Add Hardware Wizard" or "Update Driver Wizard" to install and update the drivers for any device. If you disable or do not configure this setting, administrators are subject to all policies that restrict device installation. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Allow installation of devices that match any of these device IDs	At least Windows Vista or later	Specifies a list of Plug and Play hardware IDs and compatible IDs that describe devices that can be installed. This setting is intended to be used only when the "Prevent installation of devices not described by other policy settings" setting is enabled and does not take precedence over any policy setting that would prevent a device from being installed. If you enable this setting, any device with a hardware ID or compatible ID that matches an ID in this list can be installed or updated, if that installation has not been specifically prevented by the "Prevent

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				installation of devices that match these device IDs," "Prevent installation of devices for these device classes," or "Prevent installation of removable devices" policy setting. If another policy setting prevents a device from being installed, the device cannot be installed even if it is also described by a value in this policy setting. If you disable or do not configure this setting and no other policy describes the device, the "Prevent installation of devices not described by other policy settings" setting determines whether the device can be installed. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Allow installation of devices using drivers that match these device setup classes	At least Windows Vista or later	Specifies a list of device setup class GUIDs describing devices that can be installed. This setting is intended to be used only when the "Prevent installation of devices not described by other policy settings" setting is enabled and does not have precedence over any setting that would prevent a device from being installed. If you enable this setting, any device with a hardware ID or compatible ID that matches one of the IDs in this list can be installed or updated, if that installation has not been specifically prevented by the "Prevent installation of devices that match these device IDs," "Prevent installation of devices for these device classes," or "Prevent installation of removable devices" policy setting. If another policy setting prevents a device from being installed, the device cannot be installed even if it is also described by a value in this setting. If you disable or do not configure this setting and no other policy describes the device, the "Prevent installation of devices not described by other policy settings" setting determines whether the device can be installed. If this computer is a Terminal Server, then

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Display a custom message when installation is prevented by policy (balloon text)	At least Windows Vista or later	Specifies a custom message that is displayed to the user in the text of the notification balloon when policy prevents the installation of a device. If you enable this setting, then this text is displayed as the main body text of the message displayed by Windows whenever device installation is prevented by policy. If you disable or do not configure this setting, then Windows displays a default message whenever device installation is prevented by policy.
Computer	Device Installation Restrictions	Display a custom message when installation is prevented by policy (balloon title)	At least Windows Vista or later	Specifies a custom message that is displayed to the user in the title of the notification balloon when policy prevents the installation of a device. If you enable this setting, then this text is displayed as the title text of the message displayed by Windows whenever device installation is prevented by policy. If you disable or do not configure this setting, then Windows displays a default title whenever device installation is prevented by policy.
Computer	Device Installation Restrictions	Prevent installation of devices not described by other policy settings	At least Windows Vista or later	This setting controls the installation policy for devices that are not specifically described by any other policy. If you enable this setting, any device that is not described by either the "Allow installation of devices that match these device IDs" or "Allow installation of devices for these device classes" cannot be installed or have its driver updated. If you disable or do not configure this setting, any device that is not described by the "Prevent installation of devices that match these device IDs," "Prevent installation of devices for these device classes," or "Deny installation of removable devices" policies can be installed and have its driver updated. If this computer is a Terminal Server, then enabling this policy also

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Prevent installation of devices that match any of these device IDs	At least Windows Vista or later	Specifies a list of Plug and Play hardware IDs and compatible IDs for devices that cannot be installed. If you enable this setting, a device cannot be installed or updated if its hardware ID or compatible ID matches one in this list. If you disable or do not configure this setting, new devices can be installed and existing devices can be updated, as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Prevent installation of devices using drivers that match these device setup classes	At least Windows Vista or later	Specifies a list of Plug and Play device setup class GUIDs for devices that cannot be installed. If you enable this setting, new devices cannot be installed and existing devices cannot be updated if they use drivers that belong to any of the listed device setup classes. If you disable or do not configure this setting, new devices can be installed and existing devices can be updated as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. If this computer is a Terminal Server, then enabling this

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Prevent installation of removable devices	At least Windows Vista or later	Prevents removable devices from being installed. If you enable this setting, removable devices may not be installed, and existing removable devices cannot have their drivers updated. If you disable or do not configure this setting, removable devices can be installed and existing removable devices can be updated as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. For this policy, a device is considered to be removable when the drivers for the device to which it is connected indicate that the device is removable. For example, a Universal Serial Bus (USB) device is reported to be removable by the drivers for the USB hub to which the device is connected. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer/User	Digital Locker	Do not allow Digital Locker to run	At least Windows Vista or later	Specifies whether Digital Locker can run. Digital Locker is a dedicated download manager associated with Windows Marketplace and a feature of Windows that can be used to manage and download products acquired and stored in the user's Windows Marketplace Digital Locker. If you enable this setting, Digital Locker will not run. If you disable or do not configure this setting, Digital Locker can be run.
Computer	Disk Diagnostic	Disk Diagnostic: Configure custom	At least Windows Vista or later	Substitutes custom alert text in the disk diagnostic message shown to users when

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		alert text		a disk reports a S.M.A.R.T. fault. If you enable this policy setting, Windows will display custom alert text in the disk diagnostic message. The custom text may not exceed 512 characters. nIf you disable or do not configure this policy setting, Windows will display the default alert text in the disk diagnostic message. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect if the Disk Diagnostic scenario policy is enabled or not configured and the Diagnostic Policy Service (DPS) is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Disk Diagnostic	Disk Diagnostic: Configure execution level	At least Windows Vista or later	Determines the execution level for S.M.A.R.T.-based disk diagnostics. Self-Monitoring And Reporting Technology (S.M.A.R.T.) is a standard mechanism for storage devices to report faults to Windows. A disk that reports a S.M.A.R.T. fault may need to be repaired or replaced. The Diagnostic Policy Service (DPS) will detect and log S.M.A.R.T. faults to the event log when they occur. If you enable this policy setting, the DPS will also warn users of S.M.A.R.T. faults and guide them through backup and recovery to minimize potential data loss. If you disable this policy, S.M.A.R.T. faults will still be detected and logged, but no corrective action will be taken. If you do not configure this policy setting, the DPS will enable S.M.A.R.T. fault resolution by default. This policy setting takes effect only if the diagnostics-wide scenario execution policy is not configured. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Service is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Disk NV Cache	Turn Off Boot and Resume Optimizations	At least Windows Vista or later	Turns off the boot and resume optimizations for the hybrid hard disks in the system. If you enable this policy setting, the system does not use the non-volatile (NV) cache to optimize boot and resume. If you disable this policy setting, the system uses the NV cache to achieve faster boot and resume. The system determines the data that will be stored in the NV cache to optimize boot and resume. The required data is stored in the NV cache during shutdown and hibernate respectively. This might cause a slight increase in the time taken for shutdown and hibernate. If you do not configure this policy, the default behavior is observed and the NV cache is used for boot and resume optimizations. NOTE: This policy is applicable only if the NV Cache Feature is on.
Computer	Disk NV Cache	Turn Off Cache Power Mode	At least Windows Vista or later	Turns off the power save mode on the hybrid hard disks in the system. If you enable this policy, the disks will not be put into NV cache power save mode and no power savings would be achieved. If you disable this policy setting, then the hard disks are put into a NV cache power saving mode. In this mode, the system tries to save power by aggressively spinning down the disk. If you do not configure this policy setting, the default behavior is to allow the hybrid hard disks to be in power save mode. NOTE: This policy is applicable only if the NV Cache feature is on.
Computer	Disk NV Cache	Turn Off Non Volatile Cache Feature	At least Windows Vista or later	Turns off all support for the non-volatile (NV) cache on all hybrid hard disks in the system. To check if you have hybrid hard disks in the system, from the device

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				manager, right click the disk drive and select Properties. The NV cache can be used to optimize boot and resume by reading data from the cache while the disks are spinning up. The NV cache can also be used to reduce the power consumption of the system by keeping the disks spun down while satisfying reads and writes from the cache. If you enable this policy setting, the system will not manage the NV cache and will not enable NV cache power saving mode. If you disable this policy setting, the system will manage the NV cache on the disks provided the other policy settings for the NV cache are appropriately configured. NOTE: This setting will take effect on next boot. If you do not configure this policy, the default behavior is to turn on support for the NV cache.
Computer	Disk NV Cache	Turn Off Solid State Mode	At least Windows Vista or later	Turns off the solid state mode for the hybrid hard disks. If you enable this policy setting, frequently written files such as the file system metadata and registry may not be stored in the NV cache. If you disable this policy setting, the system will store frequently written data into the non-volatile (NV) cache. This allows the system to exclusively run out of the NV cache and power down the disk for longer periods to save power. Note that this can cause increased wear of the NV cache. If you do not configure this policy, the default behavior of the system is observed and frequently written files will be stored in the NV cache. NOTE: This policy is applicable only if the NV Cache Feature is on.
Computer	DNS Client	Allow DNS Suffix Appending to Unqualified Multi-Label Name Queries	At least Windows Vista or later	Specifies whether the computers to which this setting is applied may attach suffixes to an unqualified multi-label name before sending subsequent DNS queries, if the original name query fails. A name containing dots, but not dot-terminated, is called an unqualified multi-label name, for example "server.corp". A

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				fully qualified name would have a terminating dot, for example "server.corp.contoso.com.". If you enable this setting, suffixes are allowed to be appended to an unqualified multi-label name, if the original name query fails. For example, an unqualified multi-label name query for "server.corp" will be queried by the DNS Client first. If the query succeeds, the response is returned to the client. If the query fails, the unqualified multi-label name is appended with DNS Suffixes configured for the computer for queries. These suffixes can be derived from a combination of the local DNS Client's primary domain suffix, a connection-specific domain suffix and/or DNS Suffix Search List. For example, if the local DNS Client receives a query for "server.corp", and a primary domain suffix is configured as "contoso.com", with this setting the DNS Client will send a query for "server.corp.contoso.com." if the original name query for "server.corp" fails. If you disable this setting, no suffixes are appended to unqualified multi-label name queries if the original name query fails. If you do not configure this setting, computers will use their local DNS Client configuration to determine the query behavior for unqualified multi-label names.
Computer	DNS Client	Turn off Multicast Name Resolution	At least Windows Vista or later	Local Link Multicast Name Resolution (LLMNR) is a secondary name resolution protocol. Queries are sent over the Local Link, a single subnet, from a client machine using Multicast to which another client on the same link, which also has LLMNR enabled, can respond. LLMNR provides name resolution in scenarios in which conventional DNS name resolution is not possible. If you enable this policy setting, Multicast name resolution or LLMNR, will be turned off for the machine across all available but un-configured network adapters. If you disable this policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting, Multicast name resolution or LLMNR, will be turned on for the machine across all available but un-configured network adapters. If you do not configure this policy setting, Multicast name resolution or LLMNR, will be turned on for the machine across all available but un-configured network adapters by default.
Computer	Driver Installation	Allow non-administrators to install drivers for these device setup classes	At least Windows Vista or later	Specifies a list of device setup class GUIDs describing device drivers that non-administrator members of the built-in Users group may install on the system. If you enable this setting, members of the Users group may install new drivers for the specified device setup classes. The drivers must be signed according to Windows Driver Signing Policy, or be signed by publishers already in the TrustedPublisher store. If you disable or do not configure this setting, only members of the Administrators group are allowed to install new device drivers on the system.
User	Explorer Frame Pane	Turn off Details Pane	At least Windows Vista or later	Hides the Details Pane in Windows Explorer. If you enable this policy setting, the Details Pane in Windows Explorer is hidden and cannot be turned on by the user. If you disable, or do not configure this setting, the Details Pane is displayed by default and can be hidden by the user.
User	Explorer Frame Pane	Turn off Preview Pane	At least Windows Vista or later	Hides the Preview Pane in Windows Explorer. If you enable this policy setting, the Preview Pane in Windows Explorer is hidden and cannot be turned on by the user. If you disable, or do not configure this setting, the Preview Pane is displayed by default and can be hidden by the user.
Computer/User	Folder Redirection	Use localized subfolder names when redirecting Start and My Documents	At least Windows Vista or later	This policy setting allows the administrator to define whether Folder Redirection should use localized names for the All Programs, Startup, My Music, My Pictures, and My Videos subfolders when redirecting the parent Start menu and legacy My

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Documents folder respectively. If you enable this policy setting, Windows Vista will use localized folder names for these subfolders when redirecting the Start Menu or legacy My Documents folder. If you disable or not configure this policy setting, Windows Vista will use the standard English names for these subfolders when redirecting the Start Menu or legacy My Documents folder. Note: This policy is valid only on Windows Vista when it processes a legacy redirection policy already deployed for these folders in your existing localized environment.
Computer	Game Explorer	Turn off downloading of game information	At least Windows Vista or later	Manages download of game box art and ratings from the Windows Metadata Services. If you enable this setting, game information including box art and ratings will not be downloaded. If you disable or do not configure this setting, game information will be downloaded from Windows Metadata Services.
Computer	Game Explorer	Turn off tracking of last play time of games in the Games folder	At least Windows Vista or later	Tracks the last play time of games in the Games folder. If you enable this setting the last played time of games will not be recorded in Games folder. This setting only affects the Games folder. If you disable or do not configure this setting, the last played time will be displayed to the user.
Computer	General iSCSI	Do not allow additional session logins	At least Windows Vista or later	If enabled then only those sessions that are established via a persistent login will be established and no new persistent logins may be created. If disabled then additional persistent and non persistent logins may be established.
Computer	General iSCSI	Do not allow changes to initiator iqn name	At least Windows Vista or later	If enabled then do not allow the initiator iqn name to be changed. If disabled then the initiator iqn name may be changed.
Computer	Group Policy	Startup policy processing wait time	At least Windows Vista or later	This policy setting specifies how long Group Policy should wait for network availability notifications during startup policy processing. If the startup policy processing is synchronous, the computer is blocked until the network is available

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				or the default wait time is reached. If the startup policy processing is asynchronous, the computer is not blocked and policy processing will occur in the background. In either case, configuring this policy setting overrides any system-computed wait times. If you enable this policy setting, Group Policy will use this administratively configured maximum wait time and override any default or system-computed wait time. If you disable or do not configure this policy setting, Group Policy will use the default wait time of 30 seconds on computers running the Microsoft Windows Vista operating system.
Computer	Group Policy	Turn off Local Group Policy objects processing	At least Windows Vista or later	This policy setting prevents Local Group Policy objects (Local GPOs) from being applied. By default, the policy settings in Local GPOs are applied before any domain-based GPO policy settings. These policy settings can apply to both users and the local computer. You can disable the processing and application of all Local GPOs to ensure that only domain-based GPOs are applied. If you enable this policy setting, the system will not process and apply any Local GPOs. If you disable or do not configure this policy setting, Local GPOs will continue to be applied. Note: For computers joined to a domain, it is strongly recommended that you only configure this policy setting in domain-based GPOs. This setting will be ignored on computers that are joined to a workgroup.
User	Group Policy snap-in extensions	Windows Firewall with Advanced Security	At least Windows Vista or later	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

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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	Group Policy snap-in extensions, mmc	**NAP Client Configuration**	At least Windows Vista or later	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	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Handwriting personalization	Turn off automatic learning	At least Windows Vista or later	Turns off the automatic learning component of handwriting recognition personalization. Automatic learning enables the collection and storage of text and/or ink written by the user in order to help adapt handwriting recognition to the vocabulary and handwriting style of the user. Text that is collected includes all outgoing messages in Windows Mail, and MAPI enabled e-mail clients, plus URLs from the Internet Explorer browser history. The information that is stored includes word frequency and new words not already known to the handwriting recognition engines (for example proper names and acronyms). Deleting e-mail content or the browser history will not delete the stored personalization data. Ink entered through Input Panel is collected and stored. Note: Automatic learning of both text and ink might not be available for all languages, even when handwriting personalization is available. See Tablet PC Help for more information. If you enable this policy, automatic learning stops and any stored data is deleted. Users will not be able to configure this setting in Control Panel. If you disable this policy, automatic learning is turned on. Users will not be able to configure this setting in Control Panel. Collected data is only used for handwriting recognition if handwriting personalization is turned on. If you do not configure this policy, users can choose to enable or disable automatic learning either from the Handwriting tab in the Tablet Settings in Control Panel or from the opt-in dialog. Related to ΓÇ£Turn off handwriting personalizationΓÇ¥ policy. Note: The amount of stored ink is limited to 50 MB and the amount of text information to about 5 MB. When these limits are reached and new data is collected, old data is deleted to make room for more recent data. Note: Handwriting personalization in Microsoft Windows VistaΓäó

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				works only for Microsoft handwriting recognizers, not with third-party recognizers.
Computer/User	Handwriting personalization	Turn off handwriting personalization	At least Windows Vista or later	Turns off handwriting recognition personalization so the handwriting recognition engine that ships with Windows VistaΓäó is used instead of the personalized handwriting recognizer. Handwriting personalization allows the handwriting recognizer to adapt to the writing style and vocabulary of a user by using automatic learning and the handwriting recognition personalization tool. Handwriting personalization is not available for all languages that have handwriting recognition. See Tablet PC Help for more information. If you enable this policy, handwriting personalization is turned off. The handwriting recognition that ships with Windows VistaΓäó is used. The information collected for handwriting personalization is not deleted, but it will not be used for handwriting recognition. Users will not be able to configure this setting in Control Panel. If you disable this policy, handwriting personalization is turned on. Users will not be able to configure this setting in Control Panel. If you do not configure this policy, handwriting personalization is turned on. Users will be able to configure this setting on the Handwriting tab of Tablet Settings, in Control Panel. Related to ΓÇ£Turn off automatic learningΓÇ¥ policy. Note: Handwriting personalization in Microsoft Windows VistaΓäó works only for Microsoft handwriting recognizers, not with third-party recognizers.
Computer	Hard Disk Settings	Turn Off the Hard Disk (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the hard disk. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the hard disk. If you disable this policy or do not configure it, users can see and change this setting.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Hard Disk Settings	Turn Off the Hard Disk (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the hard disk. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the hard disk. If you disable this policy or do not configure it, users can see and change this setting.
Computer/User	Hardware Buttons	Prevent Back-ESC mapping	At least Windows Vista or later	Removes the Back-&gt;ESC mapping that normally occurs when menus are visible, and for applications that subscribe to this behavior. If you enable this policy, a button assigned to Back will not map to ESC. If you disable this policy, Back-&gt;ESC mapping will occur. If you do not configure this policy, Back-&gt;ESC mapping will occur.
Computer/User	Hardware Buttons	Prevent launch an application	At least Windows Vista or later	Prevents the user from launching an application from a Tablet PC hardware button. If you enable this policy, applications cannot be launched from a hardware button, and "Launch an application" is removed from the drop down menu for configuring button actions (in the Tablet PC Control Panel buttons tab). If you disable this policy, applications can be launched from a hardware button. If you do not configure this policy, applications can be launched from a hardware button.
Computer/User	Hardware Buttons	Prevent press and hold	At least Windows Vista or later	Prevents press and hold actions on hardware buttons, so that only one action is available per button. If you enable this policy, press and hold actions are unavailable, and the button configuration dialog will display the following text: "Some settings are controlled by Group Policy. If a setting is unavailable, contact your system administrator." If you disable this policy, press and hold actions for buttons will be available. If you do not configure this policy, press and hold actions will be available.
Computer/User	Hardware Buttons	Turn off hardware buttons	At least Windows Vista or later	Turns off Tablet PC hardware buttons. If you enable this policy, no actions will

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				occur when the buttons are pressed, and the buttons tab in Tablet PC Control Panel will be removed. If you disable this policy, user and OEM defined button actions will occur when the buttons are pressed. If you do not configure this policy, user and OEM defined button actions will occur when the buttons are pressed.
Computer/User	Import Video	Do not allow Import Video to run	At least Windows Vista or later	Specifies whether Import Video can run. Import Video is a feature of Windows Vista that can be used to import video from a digital video device where the video is encoded and saved as a video file on your computer. If you enable this setting, Import Video will not run. If you disable or do not configure this setting, Import Video can be run.
Computer/User	Input Panel	For tablet pen input, donΓÇÖt show the Input Panel icon	At least Windows Vista or later	Prevents the Tablet PC Input Panel icon from appearing next to any text entry area in applications where this behavior is available. This policy applies only when using a tablet pen as an input device. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel will never appear next to text entry areas when using a tablet pen as an input device. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel will appear next to any text entry area in applications where this behavior is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will be able to configure this setting on the Opening tab in Input Panel Options. Caution: If you enable both the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				ΓÇ£Prevent Input Panel from appearing next to text entry areasΓÇ¥ policy and the ΓÇ£Prevent Input Panel tab from appearingΓÇ¥ policy, and disable the ΓÇ£Show Input Panel taskbar iconΓÇ¥ policy, the user will then have no way to access Input Panel.
Computer/User	Input Panel	For touch input, donΓÇÖt show the Input Panel icon	At least Windows Vista or later	Prevents the Tablet PC Input Panel icon from appearing next to any text entry area in applications where this behavior is available. This policy applies only when a user is using touch input. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel will never appear next to any text entry area when a user is using touch input. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will be able to configure this setting on the Opening tab in Input Panel Options.
Computer/User	Input Panel	Include rarely used Chinese, Kanji, or Hanja characters	At least Windows Vista or later	Includes rarely used Chinese, Kanji, and Hanja characters when handwriting is converted to typed text. This policy applies only to the use of the Microsoft recognizers for Chinese (Simplified), Chinese (Traditional), Japanese, and Korean. This setting appears in Input Panel Options only when these input languages or keyboards are installed. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				text, symbols, numbers, or keyboard shortcuts. If you enable this policy, rarely used Chinese, Kanji, and Hanja characters will be included in recognition results when handwriting is converted to typed text. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, rarely used Chinese, Kanji, and Hanja characters will not be included in recognition results when handwriting is converted to typed text. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, rarely used Chinese, Kanji, and Hanja characters will not be included in recognition results when handwriting is converted to typed text. Users will be able to configure this setting on the Advanced tab in the Input Panel Options dialog box.
Computer/User	Input Panel	Prevent Input Panel tab from appearing	At least Windows Vista or later	Prevents Input Panel tab from appearing on the edge of the Tablet PC screen. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel tab will not appear on the edge of the Tablet PC screen. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel tab will appear on the edge of the Tablet PC screen. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel tab will appear on the edge of the Tablet PC screen. Users will be able to configure this setting on the Opening tab in Input Panel Options. Caution: If you enable both the ΓÇ£Prevent Input Panel from appearing next to text entry areasΓÇ¥ policy and the ΓÇ£Prevent Input Panel tab from

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				appearingΓÇ¥ policy, and disable the ΓÇ£Show Input Panel taskbar iconΓÇ¥ policy, the user will then have no way to access Input Panel.
Computer/User	Input Panel	Switch to the Simplified Chinese (PRC) gestures	At least Windows Vista or later	Switches the gesture set used for editing from the common handheld computer gestures to the Simplified Chinese (PRC) standard gestures. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, the Simplified Chinese (PRC) editing gestures will be used. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, the common handheld editing gesture set will be used. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, the common handheld editing gesture set will be used. Users will be able to configure this setting on the Gestures tab in Input Panel Options.
Computer/User	Input Panel	Turn off AutoComplete integration with Input Panel	At least Windows Vista or later	Turns off the integration of application auto complete lists with Tablet PC Input Panel in applications where this behavior is available. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, application auto complete lists will never appear next to Input Panel. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, application auto complete lists will appear next to Input Panel in applications where the functionality is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, application auto complete lists will appear next to Input

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Panel in applications where the functionality is available. Users will be able to configure this setting on the Settings tab in Input Panel Options.
Computer/User	Input Panel	Turn off password security in Input Panel	At least Windows Vista or later	Adjusts password security settings in Tablet PC Input Panel. These settings include using the on-screen keyboard by default, preventing users from switching to another Input Panel skin (the writing pad or character pad), and not showing what keys are tapped when entering a password. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy and choose ΓÇ£LowΓÇ¥ from the drop-down box, password security is set to ΓÇ£Low.ΓÇ¥ At this setting, all password security settings are turned off. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£Medium-LowΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium-Low.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel displays the cursor and which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£MediumΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is not allowed, and Input Panel displays the cursor and which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose to ΓÇ£Medium-HighΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium-

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£HighΓÇ¥ from the drop-down box, password security is set to ΓÇ£High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is not allowed, and Input Panel does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, password security is set to ΓÇ£Medium-High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, password security is set to ΓÇ£Medium-HighΓÇ¥ by default. At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel does not display the cursor or which keys are tapped. Users will be able to configure this setting on the Advanced tab in Input Panel Options. Caution: If you lower password security settings, people who can see the userΓÇÖs screen might be able to see their passwords.
Computer/User	Input Panel	Turn off tolerant and Z-shaped scratch-out gestures	At least Windows Vista or later	Turns off both the more tolerant scratch-out gestures that were added in Windows Vista and the Z-shaped scratch-out gesture that was available in Microsoft

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Windows XP Tablet PC Edition. The tolerant gestures let users scratch out ink in Input Panel by using strikethrough and other scratch-out gesture shapes. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy and choose ΓÇ£AllΓÇ¥ from the drop-down menu, no scratch-out gestures will be available in Input Panel. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£Tolerant," users will be able to use the Z-shaped scratch-out gesture that was available in Microsoft Windows XP Tablet PC Edition. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£None,ΓÇ¥ users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will be able to configure this setting on the Gestures tab in Input Panel Options.
User	Instant Search	Custom Instant Search Internet search provider	At least Windows Vista or later	Set up the menu name and URL for the custom Internet search provider. If you enable this setting, the specified menu name and URL will be used for Internet searches. If you disable or not configure this setting, the default Internet search provider will be used.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Internet Communication settings	Turn off handwriting recognition error reporting	At least Windows Vista or later	Turns off the handwriting recognition error reporting tool. The handwriting recognition error reporting tool enables users to report errors encountered in Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows. If you enable this policy, users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft. If you disable this policy, Tablet PC users can report handwriting recognition errors to Microsoft. If you do not configure this policy Tablet PC users can report handwriting recognition errors to Microsoft.
User	Internet Communication settings	Turn off Help Experience Improvement Program	At least Windows Vista or later	Specifies whether users can participate in the Help Experience Improvement program. The Help Experience Improvement program collects information about how customers use Windows Help so that Microsoft can improve it. If this setting is enabled, this policy prevents users from participating in the Help Experience Improvement program. If this setting is disabled or not configured, users will be able to turn on the Help Experience Improvement program feature from the Help and Support settings page.
User	Internet Communication settings	Turn off Help Ratings	At least Windows Vista or later	Specifies whether users can provide ratings for Help content. If this setting is enabled, this policy setting prevents ratings controls from being added to Help content. If this setting is disabled or not configured, a rating control will be added to Help topics. Users can use the control to provide feedback on the quality and usefulness of the Help and Support content.
Computer/User	Internet Communication settings	Turn off Windows Movie Maker online Web links	At least Windows Vista or later	Specifies whether links to Web sites are available in Windows Movie Maker. These links include the "Windows Movie Maker on the Web" and "Privacy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Statement" commands that appear on the Help menu. 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. 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	Internet Communication settings	Turn off Windows Online	At least Windows Vista or later	Specifies whether users can search and view content from Windows Online in Help and Support. Windows Online provides the most up-to-date Help content for Windows. If this settings is enabled, users will be prevented from accessing online assistance content from Windows Online. If this setting is disabled or not configured, users will be able to access online assistance if they have a connection to the Internet and have not disabled Windows Online from the Help and Support Options page.
Computer	iSCSI Security	Do not allow changes to initiator CHAP secret	At least Windows Vista or later	If enabled then do not allow the initiator CHAP secret to be changed. If disabled then the initiator CHAP secret may be changed.
Computer	iSCSI Security	Do not allow connections without IPSec	At least Windows Vista or later	If enabled then only those connections that are configured for IPSec may be established. If disabled then connections that are configured for IPSec or connections not configured for IPSec may be established.
Computer	iSCSI Security	Do not allow sessions without mutual CHAP	At least Windows Vista or later	If enabled then only those sessions that are configured for mutual CHAP may be established. If disabled then sessions that are configured for mutual CHAP or sessions not configured for mutual CHAP may be established.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	iSCSI Security	Do not allow sessions without one way CHAP	At least Windows Vista or later	If enabled then only those sessions that are configured for one-way CHAP may be established. If disabled then sessions that are configured for one-way CHAP or sessions not configured for one-way CHAP may be established. Note that if the "Do not allow sessions without mutual CHAP" setting is enabled then that setting overrides this one.
Computer	iSCSI Target Discovery	Do not allow adding new targets via manual configuration	At least Windows Vista or later	If enabled then new targets may not be manually configured by entering the target name and target portal; already discovered targets may be manually configured. If disabled then new and already discovered targets may be manually configured. Note: if enabled there may be cases where this will break VDS.
Computer	iSCSI Target Discovery	Do not allow manual configuration of discovered targets	At least Windows Vista or later	If enabled then discovered targets may not be manually configured. If disabled then discovered targets may be manually configured. Note: if enabled there may be cases where this will break VDS.
Computer	iSCSI Target Discovery	Do not allow manual configuration of iSNS servers	At least Windows Vista or later	If enabled then new iSNS servers may not be added and thus new targets discovered via those iSNS servers; existing iSNS servers may not be removed. If disabled then new iSNS servers may be added and thus new targets discovered via those iSNS servers; existing iSNS servers may be removed.
Computer	iSCSI Target Discovery	Do not allow manual configuration of target portals	At least Windows Vista or later	If enabled then new target portals may not be added and thus new targets discovered on those portals; existing target portals may not be removed. If disabled then new target portals may be added and thus new targets discovered on those portals; existing target portals may be removed.
Computer	Kerberos	Define host name-to-Kerberos realm mappings	At least Windows Vista or later	This policy setting allows you to specify which DNS host names and which DNS suffixes are mapped to a Kerberos realm. If you enable this policy setting, you can view and change the list of DNS host names and DNS suffixes mapped to a

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Kerberos realm as defined by Group Policy. To view the list of mappings, enable the policy setting and then click the Show button. To add a mapping, enable the policy setting, note the syntax, click the Show button, click the Add button, and then type a realm name in the Value Name and the list of DNS host names and DNS suffixes in the Value using the syntax format. To remove a mapping, click its entry, and then click the Remove button. To edit a mapping, remove the current entry from the list and add a new one with different parameters. If you disable this policy setting, the host name-to-Kerberos realm mappings list defined by Group Policy is deleted. If you do not configure this policy setting, the system will use the host name-to-Kerberos realm mappings that are defined in the local registry, if they exist.
Computer	Kerberos	Define interoperable Kerberos V5 realm settings	At least Windows Vista or later	This policy setting configures the Kerberos client so that it can authenticate with interoperable Kerberos V5 realms, as defined by this policy setting. If you enable this policy setting, you can view and change the list of interoperable Kerberos V5 realms and their settings. To view the list of interoperable Kerberos V5 realms, enable the policy setting and then click the Show button. To add an interoperable Kerberos V5 realm, enable the policy setting, note the syntax, click the Show button, click the Add button, and then type the interoperable Kerberos V5 realm name in the Value Name field, and type the definition of settings using the syntax format in the Value field. To remove an interoperable Kerberos V5 realm, click its entry, and then click the Remove button. To edit a mapping, remove the current entry from the list and add a new one with different parameters. If you disable this policy setting, the interoperable Kerberos V5 realm settings defined by Group

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Policy are deleted. If you do not configure this policy setting, the system will use the interoperable Kerberos V5 realm settings that are defined in the local registry, if they exist.
Computer	Kerberos	Require strict KDC validation	At least Windows Vista or later	This policy setting controls the Kerberos client's behavior in validating the KDC certificate. If you enable this policy setting, the Kerberos client requires that the KDC's X.509 certificate contains the KDC key purpose object identifier in the Extended Key Usage (EKU) extensions, and that the KDC's X.509 certificate contains a dNSName subjectAltName (SAN) extension that matches the DNS name of the domain. If the computer is joined to a domain, the Kerberos client requires that the KDC's X.509 certificate must be signed by a Certificate Authority (CA) in the NTAUTH store. If the computer is not joined to a domain, the Kerberos client allows the root CA certificate on the smart card to be used in the path validation of the KDC's X.509 certificate. If you disable or do not configure this policy setting, the Kerberos client will require only that the KDC certificate contain the Server Authentication purpose object identifier in the EKU extensions.
Computer	Link-Layer Topology Discovery	Turn on Mapper I/O (LLTDIO) driver	At least Windows Vista or later	This policy setting turns on the Mapper I/O network protocol driver. LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis. If you enable this policy setting, additional options are available to fine-tune your selection. You may choose the "Allow operation while in domain" option to allow LLTDIO to operate on a network interface that's connected to a managed network. On the other hand, if a network interface is connected to an unmanaged network, you may choose the "Allow operation while

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				in public network" and "Prohibit operation while in private network" options instead. If you disable this policy setting, LLTDIO will not participate in any of the activities described above. If you do not configure this policy setting, LLTDIO will be enabled with all options turned on at all times.
Computer	Link-Layer Topology Discovery	Turn on Responder (RSPNDR) driver	At least Windows Vista or later	This policy setting turns on the Responder network protocol driver. The Responder allows a computer to participate in Link Layer Topology Discovery requests so that it can be discovered and located on the network. It also allows a computer to participate in Quality-of-Service activities such as bandwidth estimation and network health analysis. If you enable this policy setting, additional options are available to fine-tune your selection. You may choose the "Allow operation while in domain" option to allow the Responder to operate on a network interface that's connected to a managed network. On the other hand, if a network interface is connected to an unmanaged network, you may choose the "Allow operation while in public network" and "Prohibit operation while in private network" options instead. If you disable this policy setting, the Responder will not participate in any of the activities described above. If you do not configure this policy setting, the Responder will be enabled with all options turned on at all times.
Computer/User	Locale Services	Disallow changing of geographic location	At least Windows Vista or later	This policy prevents users from changing their user geographical location (GeoID). If this policy is Enabled, then the user cannot change their geographical location (GeoID) If the policy is Disabled or Not Configured, then the user may select any GeoID. If this policy is Enabled at the Machine level, then it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer/User	Locale Services	Disallow selection of Custom Locales	At least Windows Vista or later	This policy prevents a user from selecting a supplemental custom locale as their user locale. The user is restricted to the set of locales that shipped with the operating system. Note that this does not affect the selection of replacement locales. To prevent the selection of replacement locales, adjust the permissions of the %windir%\Globalization directory to prevent the installation of locales by unauthorized users. Note that "Restrict user locales" can also be enabled to disallow selection of a custom locale, even if this policy is not configured. If this policy is Enabled, then the user cannot select a custom locale as their user locale, but they may still select a replacement locale if one is installed. If the policy is Disabled or Not Configured, then the user may select a custom locale as their user locale. If this policy is Enabled at the Machine level, it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer/User	Locale Services	Disallow user override of locale settings	At least Windows Vista or later	This policy prevents the user from customizing their locale by changing their user overrides. Any existing overrides in place when this policy is enabled will be frozen. To remove existing user override, first reset the user(s) values to the defaults and then apply this policy. When this policy is enabled, users may still choose alternate locales installed on the system unless prevented by other

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				policies, however they will be unable to customize those choices. If this policy is Enabled, then the user cannot customize their user locale with user overrides. If this policy is Disabled or Not Configured, then the user can customize their user locale overrides. If this policy is Enabled at the Machine level, then it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer	Locale Services	Restrict system locales	At least Windows Vista or later	This policy restricts the permitted system locales to the specified list. If the list is empty, it locks the system locale to its current value. This policy does not change the existing system locale; however, the next time that an admin attempts to change the machine's system locale they will be restricted to the specified list. The locale list is specified using language names, separated by a semi-colon (;). For example, en-US is English (United States). Specifying "en-US;en-CA" would restrict the system locale to English (United States) and English (Canada). If this policy is Enabled, then administrators may select a system locale only from the specified system locale list. If this policy is Disabled or Not Configured, then administrators may select any system locale shipped with the operating system.
Computer/User	Locale Services	Restrict user locales	At least Windows Vista or later	This policy restricts users on a machine to the specified list of user locales. If the list is empty, it locks all user locales to their current values. This policy does not change existing user locale settings; however, the next time a user attempts to change their user locale, their choices will be restricted to locales in this list. To set this policy on a per-user basis, make sure that the per-machine policy is set to

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				not configured. The locale list is specified using language tags, separated by a semicolon (;). For example, en-US is English (United States). Specifying "en-CA;fr-CA" would restrict the system locale to English (Canada) and French (Canada). If this policy is enabled, then only locales in the enabled list may be selected by users. If this policy is disabled or not configured, then users may select any locale installed on the machine, unless restricted by the "Disallow selection of Custom Locales" policy. If this policy is enabled at the machine level, it cannot be disabled by a per-user policy. If this policy is disabled at the machine level, then the per-user policy will be ignored. If this policy is not configured at the machine level, then restrictions will be based on per-user policies. Note that if an administrator has enabled the "Disallow selection of custom locales" policy, then users will be prevented from selecting supplemental custom locales, even if they are in the acceptable locale list for this policy.
Computer	Logon	Hide entry points for Fast User Switching	At least Windows Vista or later	By enabling the policy, Administrators hide the Switch user button in the Logon UI, the Start menu and the Task Manager.
Computer	logon:Logon	Assign a default domain for logon	At least Windows Vista or later	This policy setting specifies a default logon domain which may be a different domain than the machine joined domain. Without this policy, at logon, if a user does not specify a domain for logon, the domain to which the machine belongs is assumed as the default domain. For example if the machine belongs to the Fabrikam domain, the default domain for user logon is Fabrikam. If you enable this policy setting, the a default logon domain will be set to the specified domain which may not be the machine joined domain. If you disable or do not configure this policy setting, the default logon domain will always be set to the machine

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				joined domain.
Computer	logon:Logon	Exclude credential providers	At least Windows Vista or later	This policy setting allows the administrator to exclude the specified credential providers from use during authentication. Note: credential providers are used to process and validate user credentials during logon or when authentication is required. Windows Vista provides two default credential providers: Password and Smart Card. An administrator can install additional credential providers for different sets of credentials (for example, to support biometric authentication). If you enable this policy, an administrator can specify the CLSIDs of the credential providers to exclude from the set of installed credential providers available for authentication purposes. If you disable or do not configure this policy, all installed credential providers will be available for authentication purposes.
Computer	Microsoft Peer-to-Peer Networking Services	Disable password strength validation for Peer Grouping	At least Windows Vista or later	By default, when a Peer Group is created that allows for password-authentication (or the password for such a Group is changed), Peer Grouping validates that the password meets the password complexity requirements for the local system. Thus, it will not allow any passwords to be used for a Peer Group that are weaker than what would be allowed for a login password. This setting controls this validation behavior. If set to 1, then this validation will not be performed and any password will be allowed. If set to 0, the validation will be performed.
Computer	Microsoft Support Diagnostic Tool	Microsoft Support Diagnostic Tool: Configure execution level	At least Windows Vista or later	Determines the execution level for Microsoft Support Diagnostic Tool. Microsoft Support Diagnostic Tool (MSDT) gathers diagnostic data for analysis by support professionals. If you enable this policy setting, administrators will be able to use MSDT to collect and send diagnostic data to a support professional to resolve a problem. If you disable this policy, MSDT will not be able to gather diagnostic

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				data. If you do not configure this policy setting, MSDT will be enabled by default. This policy setting takes effect only if the diagnostics-wide scenario execution policy is not configured. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service (DPS) is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Microsoft Support Diagnostic Tool	Microsoft Support Diagnostic Tool: Restrict tool download	At least Windows Vista or later	Restricts the tool download policy for Microsoft Support Diagnostic Tool. Microsoft Support Diagnostic Tool (MSDT) gathers diagnostic data for analysis by support professionals. For some problems, MSDT may prompt the user to download additional tools for troubleshooting. These tools are required to completely troubleshoot the problem. If tool download is restricted, it may not be possible to find the root cause of the problem. If you enable this policy setting for remote troubleshooting, MSDT will prompt the user to download additional tools to diagnose problems on remote computers only. If the setting is enabled for local and remote troubleshooting, MSDT will always prompt for additional tool download. If you disable this policy, MSDT will never download tools, and will be unable to diagnose problems on remote computers. If you do not configure this policy setting, MSDT will prompt the user before downloading any additional tools. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when MSDT is enabled. This policy setting will only take effect when the Diagnostic Policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Service (DPS) is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
User	mmc:MMC_RESTRICT	Failover Clusters Manager	At least Windows Vista or later	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	mmc:MMC_RESTRICT	TPM Management	At least Windows Vista or later	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

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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	mmc:MMC_RESTRICT	Windows Firewall with Advanced Security	At least Windows Vista or later	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.
Computer/User	Network Projector	Turn off Connect to a Network	At least Windows Vista or later	Disables the Connect to a Network Projector wizard so that users cannot connect

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		Projector		to a network projector. If you enable this policy, users cannot use the Connect to a Network Projector wizard to connect to a projector. If you disable this policy or do not configure it, users can run the Connect to a Network Projector wizard to connect to a projector.
User	Network Projector	Turn off Connect to a Network Projector	At least Windows Vista or later	Disables the Connect to a Network Projector wizard so that users cannot connect to a network projector. If you enable this policy, users cannot use the Connect to a Network Projector wizard to connect to a projector. If you disable this policy or do not configure it, users can run the Connect to a Network Projector wizard to connect to a projector.
User	Network Sharing	Prevent users from sharing files within their profile.	At least Windows Vista or later	By default users are allowed to share files within their profile to other users on their network once an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile. If you enable this policy, users will not be able to share files within their profile using the sharing wizard. Also, the sharing wizard will not create a share at %root%\users and can only be used to create SMB shares on folders. If you disable or donΓÇÖt configure this policy, then users will be able to share files out of their user profile once an administrator has opted in the computer.
Computer	Notification Settings	Critical Battery Notification Action	At least Windows Vista or later	Specifies the action that Windows takes when battery capacity reaches the critical battery notification level. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Critical Battery Notification Level	At least Windows Vista or later	Specifies the percentage of battery capacity remaining that triggers the critical

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				battery notification action. If you enable this policy, you must enter a numeric value (percentage) to set the battery level that triggers the critical notification. To set the action that is triggered, see the "Critical Battery Notification Action" policy setting. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Low Battery Notification Action	At least Windows Vista or later	Specifies the action that Windows takes when battery capacity reaches the low battery notification level. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Low Battery Notification Level	At least Windows Vista or later	Specifies the percentage of battery capacity remaining that triggers the low battery notification action. If you enable this policy, you must enter a numeric value (percentage) to set the battery level that triggers the low notification. To set the action that is triggered, see the "Low Battery Notification Action" policy setting. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Turn Off Low Battery User Notification	At least Windows Vista or later	Disables a user notification when the battery capacity remaining equals the low battery notification level. If you enable this policy, Windows will not show a notification when the battery capacity remaining equals the low battery notification level. To configure the low battery notification level, see the "Low Battery Notification Level" policy setting. The notification will only be shown if the "Low Battery Notification Action" policy setting is configured to "No Action". If you do not configure this policy setting, users can see and change this setting.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	NTFS Filesystem	Selectively allow the evaluation of a symbolic link.	At least Windows Vista or later	Symbolic links can introduce vulnerabilities in certain applications. To mitigate this issue, you can selectively enable or disable the evaluation of these types of symbolic links: Local Link to a Local Target Local Link to a Remote Target Remote Link to Remote Target Remote Link to Local Target For further information please refer to the Windows Help section NOTE: If this policy is Disabled or Not Configured, local administrators may select the types of symbolic links to be evaluated.
Computer	Offline Files	Configure slow-link mode	At least Windows Vista or later	This policy setting allows you to enable and configure the slow-link mode of Offline Files. When Offline Files is operating in slow-link mode, all file requests are satisfied from the Offline Files cache, just as when the user is working offline. However, the user can manually initiate synchronization on demand. Once the synchronization completes, the system continues to operate in the slow-link mode until the user transitions the share to online mode. If you enable this policy setting, Offline Files will operate in slow-link mode if the end-to-end network throughput between the client and the server is below the throughput threshold parameter, or if the network latency is above the latency threshold parameter. You can configure slow-link mode by specifying thresholds for Throughput (bits per second) and Latency (in milliseconds) for specific UNC paths. You can specify one or both threshold parameters. When a share is transitioned to slow-link mode, the user can force the share to transition to online mode. However, the system periodically checks to see if a connection to a server is slow. If the connection is slow then the share will again be transitioned to slow-link mode. Note: You can use wildcards (*) for specifying UNC paths. If you disable or do not configuring

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this policy setting, Offline Files will not transition to slow-link mode.
Computer	Offline Files	Turn on economical application of administratively assigned Offline Files	At least Windows Vista or later	This policy setting allows you to turn on economical application of administratively assigned Offline Files. If you enable this policy setting, only new files and folders in administratively assigned folders are synchronized at logon. Files and folders that are already available offline are skipped and are synchronized later. If you disable or do not configure this policy setting, all administratively assigned folders are synchronized at logon.
Computer	Online Assistance	Turn off Active Help	At least Windows Vista or later	Specifies whether active content links in trusted assistance content are rendered. By default, the Help viewer renders trusted assistance content with active elements such as ShellExecute links and Guided Help links. If you enable this policy, such links are not rendered. The text is displayed but there are no clickable links for these elements. If you Disable or do not configure this setting, the default behavior (Help viewer renders trusted assistance content with active elements) applies.
Computer	Online Assistance	Turn off Untrusted Content	At least Windows Vista or later	Specifies whether untrusted content is rendered. By default, the Help viewer renders untrusted assistance content pages with the exception of active links. Active links, such as ShellExecute and Guided Help, are rendered as text and are not clickable. If you enable this policy, untrusted content is not rendered at all, and a navigation error page is displayed to the user. If you Disable or do not configure this setting, the default behavior (untrusted content is rendered with the exception of active links, which are rendered as text only) applies.
Computer	Parental Controls	Make Parental Controls control panel visible on a Domain	At least Windows Vista or later	Configure the Parental Controls feature. If you turn on this setting, the Parental Controls control panel will be visible on a domain joined computer. If you turn off

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				or do not configure this setting, the Parental Controls control panel will not be visible on a domain joined computer.
Computer/User	Pen Flicks Learning	Prevent Flicks Learning Mode	At least Windows Vista or later	Makes pen flicks learning mode unavailable. If you enable this policy, pen flicks are still available but learning mode is not. Pen flicks are off by default and can be turned on system-wide, but cannot be restricted to learning mode applications. This means that the pen flicks training triggers in Internet Explorer are disabled and that the pen flicks notification will never be displayed. However, pen flicks, the pen flicks tray icon and pen flicks training (that can be accessed through CPL) are still available. Conceptually this policy is a subset of the Disable pen flicks policy. If you disable or do not configure this policy, all the features described above will be available.
Computer/User	Pen UX Behaviors	Prevent flicks	At least Windows Vista or later	Makes pen flicks and all related features unavailable. If you enable this policy, pen flicks and all related features are unavailable. This includes: pen flicks themselves, pen flicks training, pen flicks training triggers in Internet Explorer, the pen flicks notification and the pen flicks tray icon. If you disable or do not configure this policy, pen flicks and related features are available.
Computer/User	Performance Control Panel	Turn off access to the OEM and Microsoft branding section	At least Windows Vista or later	Removes access to the performance center control panel OEM and Microsoft branding links. If you enable this setting, the OEM and Microsoft web links within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel OEM and Microsoft branding links will be displayed to the user.
Computer/User	Performance Control	Turn off access to the performance	At least Windows Vista or later	Removes access to the performance center control panel page. If you enable this

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Panel	center core section		setting, some settings within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel core section will be displayed to the user.
Computer/User	Performance Control Panel	Turn off access to the solutions to performance problems section	At least Windows Vista or later	Removes access to the performance center control panel solutions to performance problems. If you enable this setting, the solutions and issue section within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel solutions to performance problems section will be displayed to the user.
Computer	Power Management	Select an Active Power Plan	At least Windows Vista or later	Specifies the active power plan from a list of default Windows power plans. To specify a custom power plan, use the Custom Active Power Plan setting. To enable this setting, select "Enabled" and choose a power plan from the Active Power Plan list. If you disable this policy or do not configure it, users can see and change this setting.
Computer	Power Management	Specify a Custom Active Power Plan	At least Windows Vista or later	Specifies an active power plan when you enter a power planΓÇÖs GUID. Retrieve the custom power plan GUID by using powercfg, the power configuration command line tool. Enter the GUID using the following format: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX. (For example, enter 103eea6e-9fcd-4544-a713-c282d8e50083.) To specify a plan for the list of default Windows power plans, use the Active Power Plan policy setting. If you disable this policy or do not configure it, users can see and change this setting.
Computer/User	Presentation Settings	Turn off Windows presentation	At least Windows Vista or later	This policy setting turns off Windows presentation settings. If you enable this

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		settings		policy setting, Windows presentation settings cannot be invoked. If you disable this policy setting, Windows presentation settings can be invoked. The presentation settings icon will be displayed in the notification area. This will give users a quick and easy way to configure their system settings before a presentation to block system notifications and screen blanking, adjust speaker volume, and apply a custom background image. Note: Users will be able to customize their system settings for presentations in Windows Mobility Center. If you do not configure this policy setting, Windows presentation settings can be invoked.
Computer/User	Previous Versions	Hide previous versions list for local files	At least Windows Vista or later	This policy setting lets you hide the list or restore of previous versions of files that are on local disks. The previous versions could come from the on-disk shadow copies or from backup media. If this policy setting is enabled, users will not be able to list or restore previous versions of files on local disks. If this policy setting is disabled, users will be able to list and restore previous versions of files on local disks. If this policy setting is not configured, it will default to disabled.
Computer/User	Previous Versions	Hide previous versions list for remote files	At least Windows Vista or later	This policy setting lets you hide the list or restore of previous versions of files that are on file shares. The previous versions could come from the on-disk shadow copies on the file share. If this policy setting is enabled, users will not be able to list or restore previous versions of files on file shares. If this policy setting is disabled, users will be able to list and restore previous versions of files on file shares. If this policy setting is not configured, it will default to disabled.
Computer/User	Previous Versions	Hide previous versions of files on backup location	At least Windows Vista or later	This setting lets you hide entries in the list of previous versions of a file in which the previous version is located on backup media. Previous versions can come

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				from the on-disk shadow copies or the backup media. If this setting is enabled, users will not see any previous versions corresponding to backup copies, and will only see previous versions corresponding to on-disk shadow copies. If this setting is disabled, users will be able to see previous versions corresponding to backup copies as well as previous versions corresponding to on-disk shadow copies. If this setting is not configured, it will default to disabled.
Computer/User	Previous Versions	Prevent restoring local previous versions	At least Windows Vista or later	This setting lets you suppress the Restore button in the previous versions property page when the user has selected a previous version of a local file. If this setting is enabled, then the Restore button will be disabled when the user selects a previous version corresponding to a local file. If this setting is disabled, then the Restore button will remain active for a previous version corresponding to a local file. If the user clicks the Restore button, then Windows will attempt to restore the file from the local disk. If this setting is not configured, it will default to disabled - the Restore button will be active when the previous version is of a local file.
Computer/User	Previous Versions	Prevent restoring previous versions from backups	At least Windows Vista or later	This setting lets you suppress the Restore button in the previous versions property page when the user has selected a previous version of a local file, in which the previous version is stored on a backup. If this setting is enabled, then the Restore button will be disabled when the user selects a previous version corresponding to a backup. If this setting is disabled, then the Restore button will remain active for a previous version corresponding to a backup. If the user clicks the Restore button, then Windows will attempt to restore the file from the backup media. If this setting is not configured, it will default to disabled - the Restore button will be active when the previous version is of a local file and stored on the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				backup.
Computer/User	Previous Versions	Prevent restoring remote previous versions	At least Windows Vista or later	This setting lets you suppress the Restore button in the previous versions property page when the user has selected a previous version of a file on a file share. If this setting is enabled, then the Restore button will be disabled when the user selects a previous version corresponding to a file on a file share. If this setting is disabled, then the Restore button will remain active for a previous version corresponding to a file on a file share. If the user clicks the Restore button, then Windows will attempt to restore the file from the file share. If this setting is not configured, it will default to disabled - the Restore button will be active when the previous version is of a file on a file share.
Computer	Printers	Add Printer wizard - Network scan page (Managed network)	At least Windows Vista or later	This policy sets the maximum number of printers (of each type) that the Add Printer wizard will display on a computer on a managed network (when the computer is able to reach a domain controller, e.g. a domain-joined laptop on a corporate network.) If this setting is disabled, the network scan page will not be displayed. If this setting is not configured, the Add Printer wizard will display the default number of printers of each type: Directory printers: 20 TCP/IP printers: 0 Web Services Printers: 0 Bluetooth printers: 10 If you would like to not display printers of a certain type, enable this policy and set the number of printers to display to 0.
Computer	Printers	Always render print jobs on the server	At least Windows Vista or later	When printing through a print server, determines whether the print spooler on the client will process print jobs itself, or pass them on to the server to do the work. This policy setting only effects printing to a Windows print server. If you enable this policy setting on a client machine, the client spooler will not process print jobs

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				before sending them to the print server. This decreases the workload on the client at the expense of increasing the load on the server. If you disable this policy setting on a client machine, the client itself will process print jobs into printer device commands. These commands will then be sent to the print server, and the server will simply pass the commands to the printer. This increases the workload of the client while decreasing the load on the server. If you do not enable this policy setting, the behavior is the same as disabling it. Note: This policy does not determine whether offline printing will be available to the client. The client print spooler can always queue print jobs when not connected to the print server. Upon reconnecting to the server, the client will submit any pending print jobs. Note: Some printer drivers require a custom print processor. In some cases the custom print processor may not be installed on the client machine, such as when the print server does not support transferring print processors during point-and-print. In the case of a print processor mismatch, the client spooler will always send jobs to the print server for rendering. Disabling the above policy setting does not override this behavior. Note: In cases where the client print driver does not match the server print driver (mismatched connection), the client will always process the print job, regardless of the setting of this policy.
User	Printers	Only use Package Point and print	At least Windows Vista or later	This policy restricts clients computers to use package point and print only. If this setting is enabled, users will only be able to point and print to printers that use package-aware drivers. When using package point and print, client computers will check the driver signature of all drivers that are downloaded from print servers. If this setting is disabled, or not configured, users will not be restricted to package-

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				aware point and print only.
User	Printers	Package Point and print - Approved servers	At least Windows Vista or later	Restricts package point and print to approved servers. If this setting is enabled, users will only be able to package point and print to print servers approved by the network administrator. When using package point and print, client computers will check the driver signature of all drivers that are downloaded from print servers. If this setting is disabled, or not configured, package point and print will not be restricted to specific print servers.
User	Programs	Hide "Get Programs" page	At least Windows Vista or later	Prevents users from viewing or installing published programs from the network. This setting prevents users from accessing the "Get Programs" page from the Programs Control Panel in Category View, Programs and Features in Classic View and the "Install a program from the netowrk" task. The "Get Programs" page 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 of their availability, to recommend their use, or to enable users to install them without having to search for installation files. If this setting is enabled, users cannot view the programs that have been published by the system administrator, and they cannot use the "Get Programs" page to install published programs. Enabling this feature does not prevent users from installing programs by using other methods. Users will still be able to view and installed assigned (partially installed) programs that are offered on the desktop or on the Start menu. If this setting is disabled or is not configured, the "Install a program from the network" task to the "Get Programs" page will be

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				available to all users. Note: If the "Hide Programs Control Panel" setting is enabled, this setting is ignored.
User	Programs	Hide "Installed Updates" page	At least Windows Vista or later	This setting prevents users from accessing "Installed Updates" page from the "View installed updates" task. "Installed Updates" allows users to view and uninstall updates currently installed on the computer. The updates are often downloaded directly from Windows Update or from various program publishers. If this setting is disabled or not configured, the "View installed updates" task and the "Installed Updates" page will be available to all users. This setting does not prevent users from using other tools and methods to install or uninstall programs.
User	Programs	Hide "Programs and Features" page	At least Windows Vista or later	This setting prevents users from accessing "Programs and Features" to view, uninstall, change, or repair programs that are currently installed on the computer. If this setting is disabled or not configured, "Programs and Features" will be available to all users. This setting does not prevent users from using other tools and methods to view or uninstall programs. It also does not prevent users from linking to related Programs Control Panel Features including Windows Features, Get Programs, or Windows Marketplace.
User	Programs	Hide "Set Program Access and Computer Defaults" page	At least Windows Vista or later	This setting removes the Set Program Access and Defaults page from the Programs Control Panel. As a result, users cannot view or change the associated page. The Set Program Access and Computer Defaults page allows administrators to specify default programs for certain activities, such as Web browsing or sending e-mail, as well as specify the programs that are accessible from the Start menu, desktop, and other locations. If this setting is disabled or not configured, the Set Program Access and Defaults button is available to all users.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				This setting does not prevent users from using other tools and methods to change program access or defaults. This setting does not prevent the Default Programs icon from appearing on the Start menu.
User	Programs	Hide "Windows Features"	At least Windows Vista or later	This setting prevents users from accessing the "Turn Windows features on or off" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs. As a result, users cannot view, enable, or disable various Windows features and services. If this setting is disabled or is not configured, the "Turn Windows features on or off" task will be available to all users. This setting does not prevent users from using other tools and methods to configure services or enable or disable program components.
User	Programs	Hide "Windows Marketplace"	At least Windows Vista or later	This setting prevents users from access the "Get new programs from Windows Marketplace" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs. Windows Marketplace allows users to purchase and/or download various programs to their computer for installation. Enabling this feature does not prevent users from navigating to Windows Marketplace using other methods. If this feature is disabled or is not configured, the "Get new programs from Windows Marketplace" task link will be available to all users. Note: If the "Hide Programs control Panel" setting is enabled, this setting is ignored.
User	Programs	Hide the Programs Control Panel	At least Windows Vista or later	This setting prevents users from using the Programs Control Panel in Category View and Programs and Features in Classic View. The Programs Control Panel allows users to uninstall, change, and repair programs, enable and disable Windows Features, set program defaults, view installed updates, and purchase

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				software from Windows Marketplace. Programs published or assigned to the user by the system administrator also appear in the Programs Control Panel. If this setting is disabled or not configured, the Programs Control Panel in Category View and Programs and Features in Classic View will be 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.
Computer	Regional and Language Options	Force selected machine UI language to overwrite the user UI language	At least Windows Vista or later	This is a setting for computers with more than one UI language installed. If you enable this setting, the UI language of Windows menus and dialogs language for systems with more than one language will follow the language specified by the administrator as the machine UI languages. The user UI language will be ignored.
User	Regional and Language Options	Hide Regional and Language Options administrative options	At least Windows Vista or later	This policy removes the Administrative options from the Regional and Language Options control panel. Administrative options include interfaces for setting system locale and copying settings to the default user. This policy does not, however, prevent an administrator or another application from changing these values programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not be able to see the Administrative options. If the policy is Disabled or Not Configured, then the user will see the Administrative options. Note that even if a user can see the Administrative options, other policies may prevent them from modifying the values.
User	Regional and Language Options	Hide the geographic location option	At least Windows Vista or later	This policy removes the option to change the user's geographical location (GeoID) from the Language and Regional Options control panel. This does not, however,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				prevent the user or an application from changing the GeoID programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the option to change the user geographical location (GeoID). If the policy is Disabled or Not Configured, then the user will see the option for changing the user location (GeoID). Note that even if a user can see the GeoID Option, the "Disallow changing of geographical location" option may prevent them from actually changing their current geographical location.
User	Regional and Language Options	Hide the select language group options	At least Windows Vista or later	This policy removes the option to change the user's menus and dialogs (UI) language from the Language and Regional Options control panel. This does not, however, prevent the user or an application from changing the UI language programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the option for changing the UI language. If the policy is Disabled or Not Configured, then the user will see the option for changing the UI language. Note that even if a user can see the option to change the UI language, other policies may prevent them from changing their UI language.
User	Regional and Language Options	Hide user locale selection and customization options	At least Windows Vista or later	This policy removes the regional formats interface from the Regional and Language Options control panel. This does not, however, prevent the user or an application from changing their user locale or user overrides programmatically. The policy is only used to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the regional formats options. If the policy is Disabled or Not Enabled, then the user will see the regional formats options for changing and customizing the user locale.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Regional and Language Options	Restricts the Machine UI languages Windows uses for all logged users	At least Windows Vista or later	This is a setting for computers with more than one UI language installed. If you enable this setting the UI language of Windows menus and dialogs language for systems with more than one language is restricted to the specific language. If the specified language is not installed on the target computer or the policy is disabled, the language selection defaults to the language selected by the local administrator.
Computer	Remote Assistance	Allow only Vista or later connections	At least Windows Vista or later	This policy setting enables Remote Assistance invitations to be generated with improved encryption so that only computers running this version (or later versions) of the operating system can connect. This setting does not affect Remote Assistance connections that are initiated by instant messaging contacts or the unsolicited Offer Remote Assistance. If you enable this policy setting, only computers running this version (or later versions) of the operating system can connect to this computer. If you disable this policy setting, computers running this version and a previous version of the operating system can connect to this computer. If you do not configure this setting, computers running this version and a previous version of the operating system can connect to this computer.
Computer	Remote Assistance	Customize Warning Messages	At least Windows Vista or later	The "Display warning message before sharing control" policy setting allows you to specify a custom message to display before a user shares control of his or her computer. The "Display warning message before connecting" policy setting allows you to specify a custom message to display before a user allows a connection to his or her computer. If you enable this policy setting, the warning message you specify will override the default message that is seen by the novice. If you disable this policy setting, the user will see the default warning message. If you do not

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				configure this setting, the user will see the default warning message.
Computer	Remote Assistance	Turn on bandwidth optimization	At least Windows Vista or later	This policy setting allows you to improve performance in low bandwidth scenarios. This setting is incrementally scaled from "No optimization" to "Full optimization". Each incremental setting includes the previous optimization setting. For example: "Turn off background" will include the following optimizations: No full window drag Turn off background "Full optimization (no 8-bit color)" will include the following optimizations: Use 8-bit color No full window drag Turn off background If you enable this policy setting, bandwidth optimization will occur at the level specified. If you disable this policy setting, application-based settings will be used. If you do not configure this policy setting, application-based settings will be used.
Computer	Remote Assistance	Turn on session logging	At least Windows Vista or later	This policy setting allows you to turn logging on or off. Log files are located in the user's Documents folder under Remote Assistance. If you enable this policy setting, log files will be generated. If you disable this policy setting, log files will not be generated. If you do not configure this setting, application-based settings will be used.
Computer/User	Removable Storage Access	All Removable Storage classes: Deny all access	At least Windows Vista or later	Configure access to all removable storage classes. This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class. If you enable this policy setting, no access is allowed to any removable storage class. If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.
Computer	Removable Storage Access	All Removable Storage: Allow direct access in remote sessions	At least Windows Vista or later	This policy setting grants normal users direct access to removable storage devices in remote sessions. If you enable this policy setting, remote users will be

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				able to open direct handles to removable storage devices in remote sessions. If you disable or do not configure this policy setting, remote users will not be able to open direct handles to removable storage devices in remote sessions.
Computer/User	Removable Storage Access	CD and DVD: Deny read access	At least Windows Vista or later	This policy setting denies read access to the CD and DVD removable storage class. If you enable this policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	CD and DVD: Deny write access	At least Windows Vista or later	This policy setting denies write access to the CD and DVD removable storage class. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Custom Classes: Deny read access	At least Windows Vista or later	This policy setting denies read access to custom removable storage classes. If you enable this policy setting, read access will be denied to these removable storage classes. If you disable or do not configure this policy setting, read access will be allowed to these removable storage classes.
Computer/User	Removable Storage Access	Custom Classes: Deny write access	At least Windows Vista or later	This policy setting denies write access to custom removable storage classes. If you enable this policy setting, write access will be denied to these removable storage classes. If you disable or do not configure this policy setting, write access will be allowed to these removable storage classes.
Computer/User	Removable Storage Access	Floppy Drives: Deny read access	At least Windows Vista or later	This policy setting denies read access to the Floppy Drives removable storage class, including USB Floppy Drives. If you enable this policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Removable Storage Access	Floppy Drives: Deny write access	At least Windows Vista or later	This policy setting denies write access to the Floppy Drives removable storage class, including USB Floppy Drives. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Removable Disks: Deny read access	At least Windows Vista or later	This policy setting denies read access to removable disks. If you enable this policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Removable Disks: Deny write access	At least Windows Vista or later	This policy setting denies write access to removable disks. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Tape Drives: Deny read access	At least Windows Vista or later	This policy setting denies read access to the Tape Drive removable storage class. If you enable this policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Tape Drives: Deny write access	At least Windows Vista or later	This policy setting denies write access to the Tape Drive removable storage class. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	Time (in seconds) to force reboot	At least Windows Vista or later	Set the amount of time (in seconds) that the system will wait to reboot in order to enforce a change in access rights to removable storage devices. If you enable this setting, set the amount of seconds you want the system to wait until a reboot.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				If you disable or do not configure this setting, the system will not force a reboot. NOTE: If no reboot is forced, the access right will not take effect until the system is restarted.
Computer/User	Removable Storage Access	WPD Devices: Deny read access	At least Windows Vista or later	This policy setting denies read access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices. If you enable this policy setting, read access will be denied to this removable storage class. If you disable or do not configure this policy setting, read access will be allowed to this removable storage class.
Computer/User	Removable Storage Access	WPD Devices: Deny write access	At least Windows Vista or later	This policy setting denies write access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices. If you enable this policy setting, write access will be denied to this removable storage class. If you disable or do not configure this policy setting, write access will be allowed to this removable storage class.
Computer	Scripts	Allow logon scripts when NetBIOS or WINS is disabled	At least Windows Vista or later	This policy setting allows user logon scripts to run when the logon cross-forest, DNS suffixes are not configured and NetBIOS or WINS is disabled. This policy setting affects all user accounts interactively logging on to the computer. If you enable this policy setting, user logon scripts will run if NetBIOS or WINS is disabled during cross-forest logons without the DNS suffixes being configured. If you disable or do not configure this policy setting, no user account cross-forest, interactive logging will be able to run logon scripts if NetBIOS or WINS is disabled and the DNS suffixes are not configured.
Computer	Search	Allow indexing of encrypted files	At least Windows Vista or later	This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing disregards encryption flags (access restrictions still apply

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				though) and will attempt to decrypt and index the content. If you disable this policy setting, the search service components (including the ones from 3rd parties) are expected not to index encrypted items such as emails or files, and to avoid indexing encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through the control panel, will be respected. Note: By default, the control panel setting is set to not index encrypted content. Note: Enabling this policy setting will not allow encrypted files in the local file system to be indexed.
Computer	Search	Allow using diacritics	At least Windows Vista or later	This policy setting allows words that contain diacritic characters to be treated as separate words. If you enable this policy setting, words that only differ in diacritics are treated as different words. If you disable this policy setting, words with diacritics and words without diacritics are treated as identical words. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through the control panel, will be respected. Note: By default, the control panel setting is set to treat words that differ only because of diacritics as the same word.
Computer	Search	Indexer data location	At least Windows Vista or later	Store indexer database in this directory. This directory must be located on a local fixed drive.
Computer	Search	Prevent displaying advanced indexing options in the Control Panel	At least Windows Vista or later	If enabled, Search and Indexing Options control panel applet does not allow opening the advanced options dialog. Otherwise it can be opened. This policy setting is not configured by default.
Computer	Search	Prevent indexing e-mail attachments	At least Windows Vista or later	Enable this policy setting to prevent the indexing of the content of e-mail attachments. If enabled, indexing service components (including the ones from

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				3rd parties) are expected not to index e-mail attachments. Consider enabling this policy setting if you are concerned about the security or indexing performance of 3rd party document filters (iFilters). This policy setting is disabled by default.
Computer	Search	Prevent indexing files in Offline Files cache	At least Windows Vista or later	If enabled, files on network shares made available offline are not indexed. Otherwise they are indexed. This policy setting is not configured by default.
Computer	Search	Prevent indexing Microsoft Office Outlook	At least Windows Vista or later	Enable this policy setting to prevent indexing of any Microsoft Outlook items. The default behavior is to automatically index Outlook items. This policy setting is not configured by default. If this policy setting is enabled then the user's Outlook items will not be added to the index and the user will not see them in search results.
Computer	Search	Prevent indexing public folders	At least Windows Vista or later	Enable this policy setting to prevent indexing public folders in Microsoft Office Outlook. When this policy setting is disabled or not configured, the user has the option to index cached public folders in Outlook. Public folders are only indexed when using Outlook 2003 or later. The user must be running in cached mode and the Download Public Folder Favorites option must be turned on.
Computer	Search	Prevent indexing uncached Exchange folders	At least Windows Vista or later	Enabling this policy setting prevents indexing of mail items on a Microsoft Exchange server when Microsoft Outlook is run in uncached mode. This is the default behavior and so for uncached items to be indexed this policy setting must be disabled. Note that versions of Outlook prior to 2003 do not support cached mode and so only local items such as PST files will be indexed if this policy setting is enabled or left in the not configured state.
Computer	Security	Require use of specific security layer for remote (RDP) connections	At least Windows Vista or later	Specifies whether to require the use of a specific security layer to secure communications between clients and terminal servers during Remote Desktop Protocol (RDP) connections. If you enable this setting, all communications

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				between clients and terminal servers during remote connections must use the security method specified in this setting. The following security methods are available: * Negotiate: The Negotiate method enforces the most secure method that is supported by the client. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the terminal server. If TLS is not supported, native Remote Desktop Protocol (RDP) encryption is used to secure communications, but the terminal server is not authenticated. * RDP: The RDP method uses native RDP encryption to secure communications between the client and terminal server. If you select this setting, the terminal server is not authenticated. * SSL (TLS 1.0): The SSL method requires the use of TLS 1.0 to authenticate the terminal server. If TLS is not supported, the connection fails. If you disable or do not configure this setting, the security method to be used for remote connections to terminal servers is not enforced through Group Policy. However, you can configure a required security method for these connections by using Terminal Services Configuration.
Computer	Security	Require user authentication using RDP 6.0 for remote connections	At least Windows Vista or later	Specifies whether to require user authentication using Remote Desktop Protocol (RDP) version 6.0 before allowing remote connections to terminal servers. This option enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this setting, only computers running Windows Vista or later can connect to terminal servers. If you disable this setting, RDP 6.0 is not required for user authentication before allowing remote connections to terminal servers. Instead, user authentication as implemented by earlier versions of RDP can be used. If you do not configure this setting, you can

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				specify that RDP 6.0 be required for user authentication by using Terminal Services Configuration or the Remote tab in System Properties. Disabling or not configuring this setting provides less security, because user authentication will occur later in the remote connection process.
Computer	Security	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer	Security	Server Authentication Certificate Template	At least Windows Vista or later	This policy setting allows you to specify the name of the certificate template that determines which certificate is automatically selected to authenticate a terminal server. A certificate is needed to authenticate a terminal server when SSL (TLS 1.0) is used to secure communication between a client and a terminal server during RDP connections. If you enable this policy setting, you need to specify a certificate template name. Only certificates created by using the specified certificate template will be considered when a certificate to authenticate the terminal server is automatically selected. Automatic certificate selection only occurs when a specific certificate has not been selected. If no certificate can be found that was created with the specified certificate template, the terminal server will issue a certificate enrollment request and will use the current certificate until the request is completed. If more than one certificate is found that was created with the specified certificate template, the certificate that will expire latest and that

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				matches the current name of the terminal server will be selected. If you disable or do not configure this policy setting, a self-signed certificate will be used by default to authenticate the terminal server. You can select a specific certificate to be used to authenticate the terminal server on the General tab of the Terminal Services Configuration tool. Note: If you select a specific certificate to be used to authenticate the terminal server, that certificate will take precedence over this policy setting.
Computer	Server	Allow only system backup	At least Windows Vista or later	This policy setting allows you to manage whether backups of only system volumes is allowed or both OS and data volumes can be backed up. If you enable this policy setting, machine administrator/backup operator can backup only volumes hosting OS components and no data only volumes can be backed up.If you disable or do not configure this policy setting, backups can include both system or data volumes.
Computer	Server	Disallow locally attached storage as backup target	At least Windows Vista or later	This policy setting allows you to manage whether backups of a machine can run to locally attached storage or not. If you enable this policy setting, machine administrator/backup operator cannot user Windows Server Backup to run backups to a locally attached storage or disk. If you disable or do not configure this policy setting, there is no restriction on locally attached storage or disk being backup target.
Computer	Server	Disallow network as backup target	At least Windows Vista or later	This policy setting allows you to manage whether backups of a machine can run to a network share or not. If you enable this policy setting, machine administrator/backup operator cannot user Windows Server Backup to run backups to a network share. If you disable or do not configure this policy setting,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				there is no restriction on network share being backup target.
Computer	Server	Disallow optical media as backup target	At least Windows Vista or later	This policy setting allows you to manage whether backups of a machine can run to an optical media or not. If you enable this policy setting, machine administrator/backup operator cannot user Windows Server Backup to run backups to an optical media. If you disable or do not configure this policy setting, there is no restriction on optical media being backup target.
Computer	Server	Disallow run-once backups	At least Windows Vista or later	This policy setting allows you to manage whether run-once backups of a machine can be run or not. If you enable this policy setting, machine administrator/backup operator cannot user Windows Server Backup to run non-scheduled run-once backups. If you disable or do not configure this policy setting, there is no restriction on running run-once backups.
Computer	Setup	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer	Setup	Turn on logging	At least Windows Vista or later	This policy setting turns on logging. If you enable or do not configure this policy setting, then events can be written to this log. If the policy setting is disabled, then no new events can be logged. Events can always be read from the log, regardless of this policy setting.
Computer	Shutdown Options	Turn off automatic termination of applications that block or cancel	At least Windows Vista or later	This policy setting specifies whether Windows will allow console applications and GUI applications without visible top-level windows to block or cancel shutdown.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		shutdown		By default, such applications are automatically terminated if they attempt to cancel shutdown or block it indefinitely. If you enable this setting, console applications or GUI applications without visible top-level windows that block or cancel shutdown will not be automatically terminated during shutdown. If you disable or do not configure this setting, these applications will be automatically terminated during shutdown, helping to ensure that Windows can shut down faster and more smoothly.
Computer	Sleep Settings	Allow Standby States (S1-S3) When Sleeping (On Battery)	At least Windows Vista or later	Dictates whether or not Windows is allowed to use standby states when sleeping the computer. When this policy is enabled, Windows may use standby states to sleep the computer. If this policy is disabled, the only sleep state a computer may enter is hibernate. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Sleep Settings	Allow Standby States (S1-S3) When Sleeping (Plugged In)	At least Windows Vista or later	Dictates whether or not Windows is allowed to use standby states when sleeping the computer. When this policy is enabled, Windows may use standby states to sleep the computer. If this policy is disabled, the only sleep state a computer may enter is hibernate. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Sleep Settings	Require a Password When a Computer Wakes (On Battery)	At least Windows Vista or later	Specifies whether or not the user is prompted for a password when the system resumes from sleep. If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep. If you disable this policy, the user is not prompted for a password when the system resumes from

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				sleep.
Computer	Sleep Settings	Require a Password When a Computer Wakes (Plugged In)	At least Windows Vista or later	Specifies whether or not the user is prompted for a password when the system resumes from sleep. If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep. If you disable this policy, the user is not prompted for a password when the system resumes from sleep.
Computer	Sleep Settings	Specify the System Hibernate Timeout (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows transitions the system to hibernate. If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to hibernate. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Specify the System Hibernate Timeout (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows transitions the system to hibernate. If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to hibernate. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Specify the System Sleep Timeout (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows transitions the system to sleep. If you enable this policy setting, you must provide a value, in seconds, indicating how much idle time should elapse before Windows transitions to sleep. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Specify the System Sleep Timeout (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows transitions the system to sleep. If you enable this policy setting, you must provide a value, in seconds, indicating

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				how much idle time should elapse before Windows transitions to sleep. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Turn Off Hybrid Sleep (On Battery)	At least Windows Vista or later	Disables Hybrid Sleep. If you enable this policy setting, a hiberfile is not generated when the system transitions to sleep (Stand By). If you do not configure this policy setting, users can see and change this setting. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Sleep Settings	Turn Off Hybrid Sleep (Plugged In)	At least Windows Vista or later	Disables Hybrid Sleep. If you enable this policy setting, a hiberfile is not generated when the system transitions to sleep (Stand By). If you do not configure this policy setting, users can see and change this setting. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Sleep Settings	Turn on Applications to Prevent Sleep Transitions (On Battery)	At least Windows Vista or later	Enables applications and services to prevent the system from sleeping. If you enable this policy setting, an application or service may prevent the system from sleeping (Hybrid Sleep, Stand By, or Hibernate). If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Sleep Settings	Turn on Applications to Prevent Sleep Transitions (Plugged In)	At least Windows Vista or later	Enables applications and services to prevent the system from sleeping. If you enable this policy setting, an application or service may prevent the system from sleeping (Hybrid Sleep, Stand By, or Hibernate). If you disable this policy setting or do not configure it, users can see and change this setting.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Smart Card	Allow certificates with no extended key usage certificate attribute	At least Windows Vista or later	This policy setting lets you allow certificates without an Extended Key Usage (EKU) set to be used for logon. Under previous versions of Microsoft Windows, the EKU extension was required to have the smart card logon Object Identifier (OID) present. This setting controls that restriction. If you enable this policy setting, only those smart card based certificates that contain the smart card logon OID or no EKU extension will be listed on the logon screen. If you disable or do not configure this policy setting then only those smart card based certificates that contain the smart card logon OID will be listed on the logon screen.
Computer	Smart Card	Allow Integrated Unblock screen to be displayed at the time of logon	At least Windows Vista or later	This policy setting lets you determine whether the integrated unblock feature will be available in the logon User Interface (UI). In order to use the integrated unblock feature your smart card must support this feature. Please check with your hardware manufacturer to see if your smart card supports this feature. If you enable this policy setting, the integrated unblock feature will be available. If you disable or do not configure this policy setting then the integrated unblock feature will not be available.
Computer	Smart Card	Allow signature keys valid for Logon	At least Windows Vista or later	This policy setting lets you allow signature key-based certificates to be enumerated and available for logon. If you enable this policy setting then any certificates available on the smart card with a signature only key will be listed on the logon screen. If you disable or do not configure this policy setting, any available smart card signature key-based certificates will not be listed on the logon screen.
Computer	Smart Card	Allow time invalid certificates	At least Windows Vista or later	This policy setting permits those certificates to be displayed for logon that are either expired or not yet valid. Under previous versions of Microsoft Windows,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				certificates were required to contain a valid time and not be expired. The certificate must still be accepted by the domain controller in order to be used. This setting only controls the displaying of the certificate on the client machine. If you enable this policy setting certificates will be listed on the logon screen regardless of whether they have an invalid time or their time validity has expired. If you disable or do not configure this policy setting, certificates which are expired or not yet valid will not be listed on the logon screen.
Computer	Smart Card	Allow user name hint	At least Windows Vista or later	This policy setting lets you determine whether an optional field will be displayed during logon and elevation that allows a user to enter his or her user name or user name and domain, thereby associating a certificate with that user. If you enable this policy setting then an optional field that allows a user to enter their user name or user name and domain will be displayed. If you disable or do not configure this policy setting, an optional field that allows a users to enter their user name or user name and domain will not be displayed.
Computer	Smart Card	Configure root certificate clean up	At least Windows Vista or later	This policy setting allows you to manage the clean up behavior of root certificates. If you enable this policy setting then root certificate cleanup will occur according to the option selected. If you disable or do not configure this setting then root certificate clean up will occur on log off.
Computer	Smart Card	Display string when smart card is blocked	At least Windows Vista or later	This policy setting allows you to manage the displayed message when a smart card is blocked. If you enable this policy setting, the specified message will be displayed to the user when the smart card is blocked. Note: The following policy setting must be enabled - Allow Integrated Unblock screen to be displayed at the time of logon. If you disable or do not configure this policy setting, the default

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				message will be displayed to the user when the smart card is blocked, if the integrated unblock feature is enabled.
Computer	Smart Card	Filter duplicate logon certificates	At least Windows Vista or later	This policy settings lets you configure if all your valid logon certificates are displayed. During the certificate renewal period, a user can have multiple valid logon certificates issued from the same certificate template. This can cause confusion as to which certificate to select for logon. The common case for this behavior is when a certificate is renewed and the old one has not yet expired. Two certificates are determined to be the same if they are issued from the same template with the same major version and they are for the same user (determined by their UPN). If there are two or more of the "same" certificate on a smart card and this policy is enabled then the certificate that is used for logon on Windows 2000, Windows XP, and Windows 2003 Server will be shown, otherwise the the certificate with the expiration time furthest in the future will be shown. Note: This setting will be applied after the following policy: "Allow time invalid certificates" If you enable or do not configure this policy setting, filtering will take place. If you disable this policy setting, no filtering will take place.
Computer	Smart Card	Force the reading of all certificates from the smart card	At least Windows Vista or later	This policy setting allows you to manage the reading of all certificates from the smart card for logon. During logon Windows will by default only read the default certificate from the smart card unless it supports retrieval of all certificates in a single call. This setting forces Windows to read all the certificates from the card. This can introduce a significant performance decrease in certain situations. Please contact your smart card vendor to determine if your smart card and associated CSP supports the required behavior. If you enable this setting, then

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Windows will attempt to read all certificates from the smart card regardless of the feature set of the CSP. If you disable or do not configure this setting, Windows will only attempt to read the default certificate from those cards that do not support retrieval of all certificates in a single call. Certificates other than the default will not be available for logon.
Computer	Smart Card	Reverse the subject name stored in a certificate when displaying	At least Windows Vista or later	This policy setting lets you reverse the subject name from how it is stored in the certificate when displaying it during logon. By default the user principal name (UPN) is displayed in addition to the common name to help users distinguish one certificate from another. For example, if the certificate subject was CN=User1, OU=Users, DN=example, DN=com and had an UPN of user1@example.com then "User1" will be displayed along with "user1@example.com." If the UPN is not present then the entire subject name will be displayed. This setting controls the appearance of that subject name and might need to be adjusted per organization. If you enable this policy setting or do not configure this setting, then the subject name will be reversed. If you disable , the subject name will be displayed as it appears in the certificate.
Computer	Smart Card	Turn on certificate propagation from smart card	At least Windows Vista or later	This policy setting allows you to manage the certificate propagation that occurs when a smart card is inserted. If you enable or do not configure this policy setting then certificate propagation will occur when you insert your smart card. If you disable this policy setting, certificate propagation will not occur and the certificates will not be made available to applications such as Outlook.
Computer	Smart Card	Turn on root certificate propagation from smart card	At least Windows Vista or later	This policy setting allows you to manage the root certificate propagation that occurs when a smart card is inserted. If you enable or do not configure this policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting then root certificate propagation will occur when you insert your smart card. Note: For this policy setting to work the following policy setting must also be enabled: Turn on certificate propagation from smart card. If you disable this policy setting then root certificates will not be propagated from the smart card.
Computer/User	Sound Recorder	Do not allow Sound Recorder to run	At least Windows Vista or later	Specifies whether Sound Recorder can run. Sound Recorder is a feature of Microsoft Windows Vista that can be used to record sound from an audio input device where the recorded sound is encoded and saved as an audio file. If you enable this policy setting, Sound Recorder will not run. If you disable or do not configure this poliyc setting, Sound Recorder can be run.
Computer	SSL Configuration Settings	SSL Cipher Suite Order	At least Windows Vista or later	Determines the cipher suites used by the Secure Socket Layer (SSL). If this setting is enabled, SSL cipher suites will be prioritized in the order specified. If this setting is disabled or not configured, the factory default cipher suite order will be used. All available cipher suites: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521 TLS_DHE_DSS_WITH_AES_128_CBC_SHA TLS_DHE_DSS_WITH_AES_256_CBC_SHA TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 SSL_CK_RC4_128_WITH_MD5 SSL_CK_DES_192_EDE3_CBC_WITH_MD5 TLS_RSA_WITH_NULL_MD5 TLS_RSA_WITH_NULL_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_DHE_DSS_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_SHA TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_RC4_40_MD5 SSL_CK_DES_64_CBC_WITH_MD5 SSL_CK_RC4_128_EXPORT40_WITH_MD5 How to modify this setting: 1. Open a blank notepad document. 2. Copy and paste the list of available suites into it. 3. Arrange the suites in the correct order; remove any suites you don't want to use. 4. Place a comma at the end of every suite name except the last. Make sure there are NO embedded spaces. 5. Remove all the line breaks so that the cipher suite names are on a single, long line. 6. Copy the cipher-suite line to the clipboard, then paste it into the edit box. The maximum length is 1023 characaters.
User	Start Menu and Taskbar	Add the Run command to the Start	At least Windows Vista or later	If you enable this setting, the Run command is added to the Start menu. If you

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		Menu		disable or do not configure this setting, the Run command is not visible on the Start menu by default, but it can be added from the Taskbar and Start menu properties. If the Remove Run link from Start Menu policy is set, the Add the Run command to the Start menu policy has no effect.
User	Start Menu and Taskbar	Clear the recent programs list for new users	At least Windows Vista or later	If you enable this policy setting, the recent programs list in the start menu will be blank for each new user. If you disable or do not configure this policy, the start menu recent programs list will be pre-populated with programs for each new user.
User	Start Menu and Taskbar	Do not search communications	At least Windows Vista or later	If you enable this policy the start menu search box will not search for communications. If you disable or do not configure this policy, the start menu will search for communications, unless the user chooses not to in the start menu control panel.
User	Start Menu and Taskbar	Do not search files	At least Windows Vista or later	If you enable this policy the start menu search box will not search for files. If you disable or do not configure this policy, the start menu will search for files, unless the user chooses not to in the start menu control panel.
User	Start Menu and Taskbar	Do not search Internet	At least Windows Vista or later	If you enable this policy the start menu search box will not search for internet history or favorites. If you disable or do not configure this policy, the start menu will search for for internet history or favorites, unless the user chooses not to in the start menu control panel.
User	Start Menu and Taskbar	Do not search programs	At least Windows Vista or later	If you enable this policy the start menu search box will not search for programs. If you disable or do not configure this policy, the start menu will search for programs, unless the user chooses not to in the start menu control panel.
User	Start Menu and Taskbar	Lock all taskbar settings	At least Windows Vista or later	Prevents the user from making any changes to the taskbar settings through the Taskbar Properties dialog. If you enable this setting the user cannot access the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				taskbar control panel, unlock, resize, move or rearrange items on their taskbar. If you disable or do not configure this setting the user will be able to set any taskbar setting that is not disallowed by another policy setting.
User	Start Menu and Taskbar	Prevent users from adding or removing toolbars	At least Windows Vista or later	Prevents users from adding or removing toolbars. If you enable this policy setting the user will not be allowed to add or remove any toolbars to the taskbar. Applications will not be able to add toolbars either. If you disable or do not configure this policy setting, the users and applications will be able to add toolbars to the taskbar.
User	Start Menu and Taskbar	Prevent users from moving taskbar to another screen dock location	At least Windows Vista or later	Prevents users from moving taskbar to another screen dock location. If you enable this policy setting the user will not be able to drag their taskbar to another side of the monitor(s). If you disable or do not configure this policy setting the user may be able to drag their taskbar to other sides of the monitor unless disallowed by another policy setting.
User	Start Menu and Taskbar	Prevent users from rearranging toolbars	At least Windows Vista or later	Prevents users from rearranging toolbars. If you enable this setting the user will not be able to drag or drop toolbars to the taskbar. If you disable or do not configure this policy setting, users will be able to rearrange the toolbars on the taskbar.
User	Start Menu and Taskbar	Prevent users from resizing the taskbar	At least Windows Vista or later	Prevent users from resizing the taskbar. If you enable this policy setting the user will not be able to resize their taskbar to be any other size. If you disable or do not configure this policy setting, the user will be able to resize their taskbar to be any other size unless disallowed by another setting.
User	Start Menu and Taskbar	Remove Games link from Start Menu	At least Windows Vista or later	If you enable this policy the start menu will not show a link to the Games folder. If you disable or do not configure this policy, the start menu will show a link to the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Games folder, unless the user chooses to remove it in the start menu control panel.
User	Start Menu and Taskbar	Remove Search Computer link	At least Windows Vista or later	If you enable this policy, the "See all results" link will not be shown when the user performs a search in the start menu search box. If you disable or do not configure this policy, the "See all results" link will be shown when the user performs a search in the start menu search box.
User	Start Menu and Taskbar	Remove the battery meter	At least Windows Vista or later	Prevents the battery meter in the system control area from being displayed. If you enable this setting, the battery meter will not be displayed in the system notification area. If you disable or do not configure this setting, the battery meter will be displayed in the system notification area.
User	Start Menu and Taskbar	Remove the networking icon	At least Windows Vista or later	Prevents the networking icon in the system control area from being displayed. If you enable this setting, the networking icon will not be displayed in the system notification area. If you disable or do not configure this setting, the networking icon will be displayed in the system notification area.
User	Start Menu and Taskbar	Remove the volume control icon	At least Windows Vista or later	Prevents the volume control icon in the system control area from being displayed. If you enable this setting, the volume control icon will not be displayed in the system notification area. If you disable or do not configure this setting, the volume control icon will be displayed in the system notification area.
User	Start Menu and Taskbar	Remove user folder link from Start Menu	At least Windows Vista or later	If you enable this policy the start menu will not show a link to the user's storage folder. If you disable or do not configure this policy, the start menu will display a link, unless the user chooses to remove it in the start menu control panel.
User	Start Menu and Taskbar	Show QuickLaunch on Taskbar	At least Windows Vista or later	This policy setting controls whether the QuickLaunch bar is displayed in the Taskbar. If you enable this policy setting, the QuickLaunch bar will be visible and

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				cannot be turned off. If you disable this policy setting, the QuickLaunch bar will be hidden and cannot be turned on. If you do not configure this policy setting, then users will be able to turn the QuickLaunch bar on and off.
User	Start Menu and Taskbar	Turn off all balloon notifications	At least Windows Vista or later	If you enable this setting no notification balloons will be shown to the user. If you disable or do not configure this setting balloon notifications will be displayed.
User	Start Menu and Taskbar	Turn off taskbar thumbnails	At least Windows Vista or later	If you enable this setting the taskbar thumbnails will not be shown, and the system will use standard text for the tooltips. If you disable or do not configure this setting the user will see the taskbar thumbnails.
User	Start Menu and Taskbar	Use folders instead of library	At least Windows Vista or later	User folders links launch a folder view of users files instead of a library view.
Computer	System	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer/User	Tablet PC Pen Training	Turn off Tablet PC Pen Training	At least Windows Vista or later	Turns off Tablet PC Pen Training. If you enable this policy setting, users cannot open Tablet PC Pen Training. If you disable or do not configure this policy setting, users can open Tablet PC Pen Training.
Computer/User	Touch Input	Turn off Tablet PC touch input	At least Windows Vista or later	Turn off Tablet PC touch input Turns off touch input, which allows the user to interact with their computer using their finger. If you enable this setting, the user will not be able to produce input with touch. They will not be able to use touch input or touch gestures such as tap and double tap, the touch pointer, and other touch-specific features. If you disable this setting, the user can produce input with

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				touch, by using gestures, the touch pointer, and other-touch specific features. If you do not configure this setting, touch input is on by default. Note: Changes to this setting will not take effect until the user logs off.
Computer	Troubleshooting and Diagnostics	Diagnostics: Configure scenario execution level	At least Windows Vista or later	Determines the execution level for Diagnostic Policy Service (DPS) scenarios. If you enable this policy setting, you must select an execution level from the dropdown menu. If you select problem detection and troubleshooting only, the DPS will detect problems and attempt to determine their root causes. These root causes will be logged to the event log when detected, but no corrective action will be taken. If you select detection, troubleshooting and resolution, the DPS will attempt to automatically fix problems it detects or indicate to the user that assisted resolution is available. If you disable this policy setting, Windows will not be able to detect, troubleshoot or resolve any problems that are handled by the DPS. If you do not configure this policy setting, the DPS will enable all scenarios for resolution by default, unless you configure separate scenario-specific policy settings. This policy setting takes precedence over any scenario-specific policy settings when it is enabled or disabled. Scenario-specific settings only take effect if this policy is not configured. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Troubleshooting and	Diagnostics: Configure scenario	At least Windows Vista or later	Determines the data retention limit for Diagnostic Policy Service (DPS) scenario

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Diagnostics	retention		data. If you enable this policy setting, you must enter the maximum size of scenario data that should be retained in megabytes. Detailed troubleshooting data related to scenarios will be retained until this limit is reached. If you disable this setting, or if you do not configure this policy setting, the DPS will delete scenario data once it exceeds 128 megabytes in size. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service is in the running state. When the service is stopped or disabled, diagnostic scenario data will not be deleted. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Trusted Platform Module Services	Configure the list of blocked TPM commands	At least Windows Vista or later	This policy setting allows you to manage the Group Policy list of Trusted Platform Module (TPM) commands blocked by Windows. If you enable this policy setting, Windows will block the specified commands from being sent to the TPM on the computer. TPM commands are referenced by a command number. For example, command number 129 is TPM_OwnerReadInternalPub, and command number 170 is TPM_FieldUpgrade. To find the command number associated with each TPM command, run "tpm.msc" and navigate to the "Command Management" section. If you disable or do not configure this policy setting, only those TPM commands specified through the default or local lists may be blocked by Windows. The default list of blocked TPM commands is pre-configured by Windows. You can view the default list by running "tpm.msc", navigating to the "Command Management" section, and making visible the "On Default Block List" column. The local list of blocked TPM commands is configured outside of Group

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Policy by running "tpm.msc" or through scripting against the Win32_Tpm interface. See related policy settings to enforce or ignore the default and local lists of blocked TPM commands.
Computer	Trusted Platform Module Services	Ignore the default list of blocked TPM commands	At least Windows Vista or later	This policy setting allows you to enforce or ignore the computer's default list of blocked Trusted Platform Module (TPM) commands. If you enable this policy setting, Windows will ignore the computer's default list of blocked TPM commands and will only block those TPM commands specified by Group Policy or the local list. The default list of blocked TPM commands is pre-configured by Windows. You can view the default list by running "tpm.msc", navigating to the "Command Management" section, and making visible the "On Default Block List" column. The local list of blocked TPM commands is configured outside of Group Policy by running "tpm.msc" or through scripting against the Win32_Tpm interface. See the related policy setting to configure the Group Policy list of blocked TPM commands. If you disable or do not configure this policy setting, Windows will block the TPM commands in the default list, in addition to commands in the Group Policy and local lists of blocked TPM commands.
Computer	Trusted Platform Module Services	Ignore the local list of blocked TPM commands	At least Windows Vista or later	This policy setting allows you to enforce or ignore the computer's local list of blocked Trusted Platform Module (TPM) commands. If you enable this policy setting, Windows will ignore the computer's local list of blocked TPM commands and will only block those TPM commands specified by Group Policy or the default list. The local list of blocked TPM commands is configured outside of Group Policy by running "tpm.msc" or through scripting against the Win32_Tpm interface. The default list of blocked TPM commands is pre-configured by Windows. See the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				related policy setting to configure the Group Policy list of blocked TPM commands. If you disable or do not configure this policy setting, Windows will block the TPM commands found in the local list, in addition to commands in the Group Policy and default lists of blocked TPM commands.
Computer	Trusted Platform Module Services	Turn on TPM backup to Active Directory Domain Services	At least Windows Vista or later	This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of Trusted Platform Module (TPM) owner information. TPM owner information includes a cryptographic hash of the TPM owner password. Certain TPM commands can only be run by the TPM owner. This hash authorizes the TPM to run these commands. If you enable this policy setting, TPM owner information will be automatically and silently backed up to AD DS when you use Windows to set or change a TPM owner password. If you select the option to "Require TPM backup to AD DS", a TPM owner password cannot be set or changed unless the computer is connected to the domain and the AD DS backup succeeds. This option is selected by default to help ensure that TPM owner information is available. Otherwise, AD DS backup is attempted but network or other backup failures do not impact TPM management. Backup is not automatically retried and the TPM owner information may not have been stored in AD DS during BitLocker setup. If you disable or do not configure this policy setting, TPM owner information will not be backed up to AD DS. Note: You must first set up appropriate schema extensions and access control settings on the domain before AD DS backup can succeed. Consult online documentation for more information about setting up Active Directory Domain Services for TPM. Note: The TPM cannot be used to provide enhanced security features for

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				BitLocker Drive Encryption and other applications without first setting an owner. To take ownership of the TPM with an owner password, run "tpm.msc" and select the action to "Initialize TPM". Note: If the TPM owner information is lost or is not available, limited TPM management is possible by running "tpm.msc" on the local computer.
Computer	User Accounts	Apply the default user logon picture to all users	At least Windows Vista or later	This policy setting allows an administrator to standardize the logon pictures for all users on a system to the default user picture. One application for this policy setting is to standardize the logon pictures to a company logo. Note: The default user picture is stored at %PROGRAMDATA%\Microsoft\User Account Pictures\user.bmp. The default guest picture is stored at %PROGRAMDATA%\Microsoft\User Account Pictures\guest.bmp. If the default pictures do not exist, an empty frame is displayed. If you enable this policy setting, the default user logon picture will display for all users on the system with no customization allowed. If you disable or do not configure this policy setting, users will be able to customize their logon pictures.
Computer	User Profiles	Delete user profiles older than a specified number of days on system restart	At least Windows Vista or later	This policy setting allows an administrator to automatically delete user profiles on system restart that have not been used within a specified number of days. Note: One day is interpreted as 24 hours after a specific user profile was accessed. If you enable this policy setting, the User Profile Service will automatically delete on the next system restart all user profiles on the computer that have not been used within the specified number of days. If you disable or do not configure this policy setting, User Profile Service will not automatically delete any profiles on the next system restart.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	User Profiles	Do not forcefully unload the users registry at user logoff	At least Windows Vista or later	Microsoft Windows will always unload the users registry, even if there are any open handles to the per-user registry keys at user logoff. Using this policy setting, an administrator can negate this behavior, preventing Windows from forcefully unloading the users registry at user logoff. Note: This policy should only be used for cases where you may be running into application compatibility issues due to this specific Windows behavior. It is not recommended to enable this policy by default as it may prevent users from getting an updated version of their roaming user profile. If you enable this policy setting, Windows will not forcefully unload the users registry at logoff, but will unload the registry when all open handles to the per-user registry keys are closed. If you disable or do not configure this policy setting, Windows will always unload the users registry at logoff, even if there are any open handles to the per-user registry keys at user logoff.
User	User Profiles	Network directories to sync at Logon/Logoff time only	At least Windows Vista or later	This policy setting allows you to specify which network directories will be synchronized only at logon and logoff via Offline Files. This policy setting is meant to be used in conjunction with Folder Redirection, to help resolve issues with applications that do not work well with Offline Files while the user is online. If you enable this policy setting, the network paths specified in this policy setting will be synchronized only by Offline Files during user logon and logoff, and will be taken offline while the user is logged on. If you disable or do not configure this policy setting, the paths specified in this policy setting will behave like any other cached data via Offline Files and continue to remain online while the user is logged on, if the network paths are accessible. Note: You should not use this policy setting to suspend any of the root redirected folders such as Appdata\Roaming, Start Menu,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				and Documents. You should suspend only the subfolders of these parent folders.
Computer	User Profiles	Set maximum wait time for the network if a user has a roaming user profile or remote home directory	At least Windows Vista or later	If the user has a roaming user profile or remote home directory and the network is currently unavailable, Microsoft Windows waits 30 seconds for the network when the user logs on to the computer. Using this policy setting, an administrator can specify how long Windows should wait for the network to become available. If the network is unavailable after the maximum wait time, Windows will continue the log on the user without a network connection. The user's roaming profile is not synchronized with the server, and the remote home directory is not used for the logon session. This policy is useful for the cases in which a network may take typically longer to initialize, such as with a wireless network. Note: If the network becomes available before the maximum wait time, Windows will proceed immediately with the user logon. Windows will not wait on the network if the physical network connection is not available on the computer (if the media is disconnected or the network adapter is not available). If you enable this policy setting, Windows will wait for the network to become available up to the maximum wait time specified in this policy setting. Setting the value to zero will cause Windows to proceed without waiting for the network. If you disable or do not configure this policy setting, Windows will wait for the network for a maximum of 30 seconds.
Computer	User Profiles	Set roaming profile path for all users logging onto this computer	At least Windows Vista or later	Specifies whether Microsoft Windows should use the specified network path as the roaming user profile path for all users logging onto this computer. To use this setting, type the path to the network share in the form \\Computername\Sharename\. It is recommended to add %USERNAME% to the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				path to give each user an individual profile folder. If not specified, all users logging onto this computer will use the same roaming profile folder as specified by this policy. You need to ensure that you have set the appropriate security on the folder to allow all users to access the profile. If you enable this policy setting, all users logging on this computer will use the roaming profile path specified in this policy. If you disable or do not configure this policy setting, then users logging on this computer will use their local profile or standard roaming user profile. Note: There are 4 ways to configure a roaming profile for a user. Windows reads profile configuration in the following order and uses the first configured setting it reads. 1. Terminal Services roaming profile path specified by Terminal Services policy 2. Terminal Services roaming profile path specified by the user object 3. A per-computer roaming profile path specified in this policy 4. A per-user roaming profile path specified in the user object
Computer	Video and Display Settings	Turn Off Adaptive Display Timeout (On Battery)	At least Windows Vista or later	Manages how Windows controls the setting that specifies how long a computer must be inactive before Windows turns off the computerΓÇÖs display. When this policy is enabled, Windows automatically adjusts the setting based on what users do with their keyboard or mouse to keep the display on. When this policy is disabled, Windows uses the same setting regardless of usersΓÇÖ keyboard or mouse behavior. If you donΓÇÖt configure this setting, users can see and change this setting.
Computer	Video and Display Settings	Turn Off Adaptive Display Timeout (Plugged In)	At least Windows Vista or later	Manages how Windows controls the setting that specifies how long a computer must be inactive before Windows turns off the computerΓÇÖs display. When this policy is enabled, Windows automatically adjusts the setting based on what users

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				do with their keyboard or mouse to keep the display on. When this policy is disabled, Windows uses the same setting regardless of usersΓÇÖ keyboard or mouse behavior. If you donΓÇÖt configure this setting, users can see and change this setting.
Computer	Video and Display Settings	Turn Off the Display (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the display. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the display. If you disable this policy or do not configure it, users can see and change this setting. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer	Video and Display Settings	Turn Off the Display (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the display. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the display. If you disable this policy or do not configure it, users can see and change this setting. Note: This setting exists under both "Computer Configuration" and "User Configuration" in the Group Policy Object Editor. The "Computer Configuration" policy takes precedence over "User Configuration" policy.
Computer/User	Window Frame Coloring	Do not allow color changes	At least Windows Vista or later	This policy setting controls the ability to change the color of window frames. If you enable this policy setting, you prevent users from changing the default window frame color. If you disable or do not configure this policy setting, you allow users to change the default window frame color. Note: This setting can be used in conjunction with the "Specify a default color for window frames" setting, to enforce

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				a specific color for window frames that cannot be changed by users.
Computer/User	Window Frame Coloring	Specify a default color	At least Windows Vista or later	This policy setting controls the default color for window frames when the user does not specify a color. If you enable this policy setting and specify a default color, this color will be used in glass window frames, if the user has not specified a color. If you disable or do not configure this policy setting, the default internal color will be used, if the user has not specified a color. Note: This policy setting can be used in conjunction with the, "Prevent color changes of window frames" setting, to enforce a specific color for window frames that cannot be changed by users.
Computer	Windows Boot Performance Diagnostics, Windows Memory Leak Diagnosis, Windows Resource Exhaustion Detection and Resolution, Windows Shutdown Performance Diagnostics, Windows Standby/Resume Performance Diagnostics, Windows System Responsiveness	Configure Scenario Execution Level	At least Windows Vista or later	Determines the execution level for Windows Boot Performance Diagnostics. If you enable this policy setting, you must select an execution level from the dropdown menu. If you select problem detection and troubleshooting only, the Diagnostic Policy Service (DPS) will detect Windows Boot Performance problems and attempt to determine their root causes. These root causes will be logged to the event log when detected, but no corrective action will be taken. If you select detection, troubleshooting and resolution, the DPS will detect Windows Boot Performance problems and indicate to the user that assisted resolution is available. If you disable this policy setting, Windows will not be able to detect, troubleshoot or resolve any Windows Boot Performance problems that are handled by the DPS. If you do not configure this policy setting, the DPS will enable Windows Boot Performance for resolution by default. This policy setting takes effect only if the diagnostics-wide scenario execution policy is not configured. No system restart or service restart is required for this policy to take

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Performance Diagnostics			effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer/User	Windows Calendar	Turn off Windows Calendar	At least Windows Vista or later	Windows Calendar is a feature that allows users to manage appointments and tasks by creating personal calendars, publishing them, and subscribing to other users calendars. If you enable this setting, Windows Calendar will be turned off. If you disable or do not configure this setting, Windows Calendar will be turned on. The default is for Windows Calendar to be turned on.
Computer/User	Windows Color System	Prohibit installing or uninstalling color profiles	At least Windows Vista or later	This policy setting affects the ability of users to install or uninstall color profiles. If you enable this policy setting, users will not be able to install new color profiles or uninstall previously installed color profiles. If you disable or do not configure this policy setting, all users will be able to install new color profiles. Standard users will be able to uninstall color profiles that they previously installed. Administrators will be able to uninstall all color profiles.
Computer	Windows Connect Now	Configuration of wireless settings using Windows Connect Now	At least Windows Vista or later	This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP), through the Windows Portable Device API (WPD), and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium. If this policy setting is enabled, additional choices are available to turn off the operations over a specific medium. If this policy setting is disabled, operations are disabled over all media. If this policy setting is not configured, operations are enabled over all media. The

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				default for this policy setting allows operations over all media.
Computer/User	Windows Connect Now	Prohibit Access of the Windows Connect Now wizards	At least Windows Vista or later	This policy setting prohibits access to Windows Connect Now (WCN) wizards. If this policy setting is enabled, the wizards are disabled and users will have no access to any of the wizard tasks. All the configuration related tasks, including ΓÇÿSet up a wireless router or access pointΓÇÖ and ΓÇÿAdd a wireless deviceΓÇÖ, will be disabled. If this policy is disabled or not configured, users will have access to the wizard tasks; including ΓÇÿSet up a wireless router or access pointΓÇÖ and ΓÇÿAdd a wireless deviceΓÇÖ. The default for this policy setting allows users to access all WCN wizards.
Computer	Windows Customer Experience Improvement Program	Allow Corporate redirection of Customer Experience Improvement uploads	At least Windows Vista or later	If you enable this setting all Customer Experience Improvement Program uploads are redirected to Microsoft Operations Manager server. If you disable this setting uploads are not redirected to a Microsoft Operations Manager server. If you do not configure this setting uploads are not redirected to a Microsoft Operations Manager server.
Computer	Windows Customer Experience Improvement Program	Allow Windows Customer Experience Improvement Program to collect corporate information	At least Windows Vista or later	The Windows Customer Experience Improvement Program will collect information about your hardware configuration and how you use our software and services to identify trends and usage patterns. We will not collect your name, address, or any other personally identifiable information. There are no surveys to complete, no salesperson will call, and you can continue working without interruption. It is simple and user-friendly. If you enable this policy setting all users are opted into Windows Customer Experience Improvement Program. If you disable this policy setting all users are opted out of Windows Customer Experience Improvement Program. If you do not configure this policy setting, administrator can use the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Problem Reports and Solutions component in Control Panel to enable Windows Customer Experience Improvement Program for all users.
Computer	Windows Customer Experience Improvement Program	Tag Windows Customer Experience Improvement data with Study Identifier	At least Windows Vista or later	This policy setting will enable tagging of Windows Customer Experience Improvement data when a study is being conducted. If you enable this setting then Windows CEIP data uploaded will be tagged. If you do not configure this setting or disable it, then CEIP data will not be tagged with the Study Identifier.
Computer	Windows Defender	Check for New Signatures Before Scheduled Scans	At least Windows Vista or later	Checks for new signatures before running scheduled scans. If you enable this policy setting, the scheduled scan checks for new signatures before it scans the computer. If you disable or do not configure this policy setting, the scheduled scan begins without downloading new signatures.
Computer	Windows Defender	Configure Microsoft SpyNet Reporting	At least Windows Vista or later	Adjusts membership in Microsoft SpyNet. Microsoft SpyNet is the online community that helps you choose how to respond to potential spyware threats. The community also helps stop the spread of new spyware infections. Here's how it works. When Windows Defender detects software or changes by software not yet classified for risks, you see how other members responded to the alert. In turn, the action you apply help other members choose how to respond. Your actions also help Microsoft choose which software to investigate for potential threats. You can choose to send basic or additional information about detected software. Additional information helps improve how Windows Defender works. It can include, for example, the location of detected items on your computer if harmful software has been removed. Windows Defender will automatically collect and send the information. If you enable this policy setting and choose "No Membership" from the drop-down list, SpyNet membership will be disabled. At this

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting, no information will be sent to Microsoft. You will not be alerted if Windows Defender detects unclassified software running on your computer. Local users will not be able to change their SpyNet membership. If you enable this policy setting and choose "Basic" from the drop-down list, SpyNet membership is set to "Basic". At this setting, basic information about the detected items and the actions you apply will be shared with the online community. You will not be alerted if Windows Defender detects software that has not yet been classified for risks. If you enable this policy setting and choose "Advanced" from the drop-down list, SpyNet membership is set to "Advanced". At this setting, you send your choices and additional information about detected items. You are alerted so you can take action when Windows Defender detects changes to your computer by unclassified software. Your decisions to allow or block changes help Microsoft create new definitions for Windows Defender and better detect harmful software. In some instances, personal information may be sent but no information is used to contact you. If you disable or do not configure this policy setting, by default SpyNet membership is disabled. At this setting, no information will be sent to Microsoft. You will not be alerted if Windows Defender detects unclassified software running on your computer. Local users will still be able to change their SpyNet membership.
Computer	Windows Defender	Download Entire Signature Set	At least Windows Vista or later	Downloads the full signature set, rather than only the signatures that have been updated since the last signature download. Downloading the full signature set can help troubleshoot problems with signature installations, but because the file is large, it can take longer to download. If you enable this policy setting, the full

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				signatures set is downloaded. If you disable or do not configure this policy setting, by default only updated signatures are downloaded.
Computer	Windows Defender	Enable Logging Known Good Detections	At least Windows Vista or later	Enables logging detection data during Real-time Protection when Windows Defender detects known good files. Logging detections provides you with detailed information about the programs that run on the computers you monitor. If you enable this policy setting, known good files are logged. If you disable or do not configure this policy setting, by default known good files are not logged. Enabling this policy setting can result in a greater number of events in the log.
Computer	Windows Defender	Enable Logging Unknown Detection	At least Windows Vista or later	Enables logging detections during Real-time Protection when Windows Defender detects unknown files. Logging detections provides you with detailed information about the programs that run on the computers you monitor. If you enable or do not configure this policy setting, by default unknown files are logged. If you disable this policy setting, unknown files are not logged. Enabling this policy setting can result in a greater number of events in the log.
Computer	Windows Defender	Turn off Real-Time Protection Prompts for Unknown Detection	At least Windows Vista or later	Turns off Real-Time Protection (RTP) prompts for unknown detection. If you enable this policy setting, Windows Defender does not prompt users to allow or block unknown activity. If you disable or do not configure this policy setting, by default Windows Defender prompts users to allow or block unknown activity on the computer.
Computer	Windows Defender	Turn off Windows Defender	At least Windows Vista or later	Turns off Windows Defender Real-Time Protection, and no more scans are scheduled. If you enable this policy setting, Windows Defender does not run, and computers will not be scanned for spyware or other potentially unwanted software. If you disable or do not configure this policy setting, by default Windows

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Defender runs and computers are scanned for spyware and other potentially unwanted software.
Computer	Windows Defender	Turn on definition updates through both WSUS and Windows Update	At least Windows Vista or later	This policy setting allows you to configure Windows Defender to check and install definition updates from Windows Update when a locally managed Windows Server Update Services (WSUS) server is not available. Windows Defender checks for definition updates using the Automatic Updates client. The Automatic Updates client can be configured to check the public Windows Update Web site or a locally managed WSUS server. When a computer is not able to connect to an internal WSUS server, such as when a portable computer is roaming outside of the corporate network, Windows Defender can be configured to also check Windows Update to ensure definition updates are delivered to these roaming machines. If you enable or do not configure this policy setting, by default Windows Defender will check for definition updates from Windows Update, if connections to a locally managed WSUS server fail. If you disable this policy setting, Windows Defender will check for definition updates only on a locally managed WSUS server, if the Automatic Updates client is so configured.
Computer/User	Windows Error Reporting	Disable Logging	At least Windows Vista or later	If this setting is enabled Windows Error Reporting events will not be logged to the system event log.
Computer/User	Windows Error Reporting	Disable Windows Error Reporting	At least Windows Vista or later	If this setting is enabled, Windows Error Reporting will not send any problem information to Microsoft. Additionally, solution information will not be available in the Problem Reports and Solutions control panel.
Computer/User	Windows Error Reporting	Do not send additional data	At least Windows Vista or later	If this setting is enabled any additional data requests from Microsoft in response to a Windows Error Reporting event will be automatically declined without notice

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				to the user.
User	Windows Explorer	Display the menu bar in Windows Explorer	At least Windows Vista or later	This policy setting configures Windows Explorer to always display the menu bar. Note: By default, the menu bar is not displayed in Windows Explorer. If you enable this policy setting, the menu bar will be displayed in Windows Explorer. If you disable or do not configure this policy setting, the menu bar will not be displayed in Windows Explorer. Note: When the menu bar is not displayed, users can access the menu bar by pressing the 'ALT' key.
User	Windows Explorer	Prevent users from adding files to the root of their Users Files folder.	At least Windows Vista or later	This policy setting allows administrators to prevent users from adding new items such as files or folders to the root of their Users Files folder in Windows Explorer. If you enable this policy setting, users will no longer be able to add new items such as files or folders to the root of their Users Files folder in Windows Explorer. If you disable or do not configure this policy setting, users will be able to add new items such as files or folders to the root of their Users Files folder in Windows Explorer. Note: Enabling this policy setting does not prevent the user from being able to add new items such as files and folders to their actual file system profile folder at %userprofile%.
User	Windows Explorer	Turn off common control and window animations	At least Windows Vista or later	This policy is similar to settings directly available to computer users. Disabling animations can improve usability for users with some visual disabilities as well as improving performance and battery life in some scenarios.
Computer	Windows Explorer	Turn off heap termination on corruption	At least Windows Vista or later	Disabling heap termination on corruption can allow certain legacy plug-in applications to function without terminating Explorer immediately, although Explorer may still terminate unexpectedly later.
User	Windows Explorer	Turn off the display of thumbnails	At least Windows Vista or later	Disables the display of thumbnails on network folders in Windows Explorer.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		and only display icons on network folders		Windows Explorer displays thumbnails on network folders by default. If you enable this policy, Windows Explorer will only display icons and never display thumbnails on network folders.
User	Windows Explorer	Turn off the display of thumbnails and only display icons.	At least Windows Vista or later	Disables the display of thumbnails in Windows Explorer. Windows Explorer displays thumbnails by default. If you enable this policy setting, Windows Explorer will only display icons and never display thumbnails.
Computer/User	Windows HotStart	Turn off Windows HotStart	At least Windows Vista or later	This policy setting allows you to manage whether HotStart buttons can be used to launch applications. If you enable this policy setting, applications cannot be launched using the HotStart buttons. If you disable or do not configure this policy setting, applications can be launched using the HotStart buttons.
Computer	Windows Logon Options	Disable or enable software Secure Attention Sequence	At least Windows Vista or later	This policy setting controls whether or not software can simulate the Secure Attention Sequence (SAS). If you enable this policy setting, you have one of four options: If you set this policy setting to "None," user mode software cannot simulate the SAS. If you set this policy setting to "Services," services can simulate the SAS. If you set this policy setting to "Ease of Access applications," Ease of Access applications can simulate the SAS. If you set this policy setting to "Services and Ease of Access applications," both services and Ease of Access applications can simulate the SAS. If you disable or do not configure this setting, only Ease of Access applications running on the secure desktop can simulate the SAS.
Computer	Windows Logon Options	Display information about previous logons during user logon	At least Windows Vista or later	This policy setting controls whether or not the system displays information about previous logons and logon failures to the user. For local user accounts and domain user accounts in Microsoft Windows Server ΓÇ¥LonghornΓÇ¥ functional

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				level domains, if you enable this setting, a message appears after the user logs on that displays the date and time of the last successful logon by that user, the date and time of the last unsuccessful logon attempted with that user name, and the number of unsuccessful logons since the last successful logon by that user. This message must be acknowledged by the user before the user is presented with the Microsoft Windows desktop. For domain user accounts in Windows Server 2003, Windows 2000 native, or Windows 2000 mixed functional level domains, if you enable this setting, a warning message will appear that Windows could not retrieve the information and the user will not be able to log on. Therefore, you should not enable this policy setting if the domain is not at the Windows Server ΓÇ£LonghornΓÇ¥ domain functional level. If you disable or do not configure this setting, messages about the previous logon or logon failures are not displayed.
User	Windows Logon Options	Remove logon hours expiration warnings	At least Windows Vista or later	This policy controls whether the logged on user should be notified when his logon hours are about to expire. By default, a user is notified before logon hours expire, if actions have been set to occur when the logon hours expire. If you enable this setting, warnings are not displayed to the user before the logon hours expire. If you disable or do not configure this setting, users receive warnings before the logon hours expire, if actions have been set to occur when the logon hours expire. Note: If you configure this setting, you might want to examine and appropriately configure the ΓÇ£Set action to take when logon hours expireΓÇ¥ setting. If ΓÇ£Set action to take when logon hours expireΓÇ¥ is disabled or not configured, the ΓÇ£Remove logon hours expiration warningsΓÇ¥ setting will have no effect,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				and users receive no warnings about logon hour expiration
Computer/User	Windows Logon Options	Report when logon server was not available during user logon	At least Windows Vista or later	This policy controls whether the logged on user should be notified if the logon server could not be contacted during logon and he has been logged on using previously stored account information. If enabled, a notification popup will be displayed to the user when the user logs on with cached credentials. If disabled or not configured, no popup will be displayed to the user.
User	Windows Logon Options	Set action to take when logon hours expire	At least Windows Vista or later	This policy controls which action will be taken when the logon hours expire for the logged on user. The actions include lock the workstation, disconnect the user, or log the user off completely. If you choose to lock or disconnect a session, the user cannot unlock the session or reconnect except during permitted logon hours. If you choose to log off a user, the user cannot log on again except during permitted logon hours. If you choose to log off a user, the user might lose unsaved data. If you enable this setting, the system will perform the action you specify when the userΓÇÖs logon hours expire. If you disable or do not configure this setting, the system takes no action when the userΓÇÖs logon hours expire. The user can continue the existing session, but cannot log on to a new session. Note: If you configure this setting, you might want to examine and appropriately configure the ΓÇ£Remove logon hours expiration warningsΓÇ¥ setting
Computer/User	Windows Mail	Turn off the communities features	At least Windows Vista or later	Windows Mail will not check your newsgroup servers for Communities support.
User	Windows Mail	Turn off the communities features	At least Windows Vista or later	Windows Mail will not check your newsgroup servers for Communities support.
Computer/User	Windows Mail	Turn off Windows Mail application	At least Windows Vista or later	Denies or allows access to the Windows Mail application. If you enable this setting, access to the Windows Mail application is denied. If you disable or do not configure this setting, access to the Windows Mail application is allowed.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Windows Media Center	Do not allow Windows Media Center to run	At least Windows Vista or later	Specifies whether Windows Media Center can run. If you enable this setting, Windows Media Center will not run. If you disable or do not configure this setting, Windows Media Center can be run.
Computer/User	Windows Meeting Space	Turn off Windows Meeting Space	At least Windows Vista or later	Windows Meeting Space is a feature that enables quick, face-to-face collaboration for sharing programs and handouts and for passing notes. If you enable this setting, Windows Meeting Space will be turned off. If you disable or do not configure this setting, Windows Meeting Space will be turned on. The default setting is for Windows Meeting Space to be turned on.
Computer/User	Windows Meeting Space	Turn on Windows Meeting Space auditing	At least Windows Vista or later	Windows Meeting Space is a feature that enables quick, face-to-face collaboration for sharing programs and handouts and for passing notes. If you enable this setting, Windows Meeting Space will audit various events that occur during a session (for example, when a user creates a session, joins a session, or starts a presentation) in the event log. If you disable or do not configure this setting, Windows Meeting Space auditing will be turned off. The default setting is for Windows Meeting Space auditing to be turned off.
Computer/User	Windows Mobility Center	Turn off Windows Mobility Center	At least Windows Vista or later	This policy setting turns off Windows Mobility Center. If you enable this policy setting, the user is unable to invoke Windows Mobility Center. The Windows Mobility Center UI is removed from all shell entry points and the .exe file does not launch it. If you disable this policy setting, the user is able to invoke Windows Mobility Center and the .exe file launches it. If you do not configure this policy setting, Windows Mobility Center is on by default.
Computer/User	Windows Movie Maker	Do not allow Windows Movie Maker to run	At least Windows Vista or later	Specifies whether Windows Movie Maker can run. Windows Movie Maker is a feature of Windows Vista that can be used to edit and then publish video as a

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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	Windows Remote Shell	Allow Remote Shell Access	At least Windows Vista or later	Configures access to remote shells. If you enable this policy setting and set it to False, new remote shell connections will be rejected by the server. If you disable or do not configure this policy setting, new remote shell connections will be allowed.
Computer	Windows Remote Shell	MaxConcurrentUsers	At least Windows Vista or later	Configures the maximum number of users able to concurrently perform remote operations on the same system using remote CMD shell. The value can be any number from 1 to 100. If you enable this policy setting, the new shell connections will be rejected if they exceed the specified limit. If you disable or do not configure this policy setting, the default number will be 5 connections per user.
Computer	Windows Remote Shell	Specify idle Timeout	At least Windows Vista or later	Configures maximum time in milliseconds remote shell will stay open without any user activity until it is automatically deleted. Any value from 0 to 0x7FFFFFFF can be set, where 0 indicates infinite timeout. If you enable this policy setting the server will wait for the specified amount of time since the last received message from the client before terminating the open shell. If you do not configure or disable this policy setting the default value of 900000 or 15 min will be used.
Computer	Windows Remote Shell	Specify maximum amount of memory in MB per Shell	At least Windows Vista or later	Configures maximum total amount of memory that can be allocated by any active remote shell and all its child processes. Any value from 0 to 0x7FFFFFFF can be set, where 0 equals unlimited memory, which means the ability of remote operations to allocate memory is only limited by the available virtual memory. If you enable this policy setting, the remote operation will be terminated when a new

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				allocation exceeds the specified quota. If you disable or do not configure this policy setting, the value 0 will used by default.
Computer	Windows Remote Shell	Specify maximum number of processes per Shell	At least Windows Vista or later	Configures the maximum number of processes any shell operations are allowed to launch. Any number from 0 to 0x7FFFFFFF can be set, where 0 means unlimited number of processes. If you enable this policy setting, the remote operation will be terminated when it attempts to launch a new process and the process count exceeds the specified limit. If you disable or do not configure this policy setting, the limit will be 5 processes per shell.
Computer	Windows Remote Shell	Specify maximum number of remote shells per user	At least Windows Vista or later	Configures maximum number of concurrent shells any user can remotely open on the same system. Any number from 0 to 0x7FFFFFFF cand be set, where 0 means unlimited number of shells. If you enable this policy setting, the user will not be able to open new remote shells if the count exceeds the specified limit. If you disable or do not configure this policy setting, by default the limit will be set to 2 remote shells per user.
Computer	Windows Remote Shell	Specify Shell Timeout	At least Windows Vista or later	Configures maximum time in milliseconds that the remote command or script will be allowed to execute. Any value from 0 to 0x7FFFFFFF can be set, where 0 indicates infinite timeout. If you enable this policy setting the server will terminate the command in progress if it takes longer than the specified amount of time. If you do not configure or disable this policy setting, the default value of 2880000 or 8 hours will be used.
Computer/User	Windows Sidebar	Disable unpacking and installation of gadgets that are not digitally signed.	At least Windows Vista or later	Sidebar gadgets can be deployed as compressed files, either digitally signed or unsigned. If you enable this setting, Windows Sidebar will not extract any gadgets that have not been digitally signed. If you disable or do not configure this setting,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Windows Sidebar will extract both signed and unsigned gadgets. The default is for Windows Sidebar to extract both signed and unsigned gadgets.
Computer/User	Windows Sidebar	Override the More Gadgets Link	At least Windows Vista or later	The Windows Sidebar contains a link to allow users to download more gadgets from a website. Microsoft hosts a default website where many gadget authors can post their gadgets. This link can be redirected to a website where alternate gadgets should be available. If you enable this setting, the Gadget Gallery in the Windows Sidebar will direct users to the alternate web site. If you disable or do not configure this setting, Windows Sidebar will direct users to the default web site. The default is for Windows Sidebar to direct users to the default web site.
Computer/User	Windows Sidebar	Turn Off User Installed Windows Sidebar Gadgets	At least Windows Vista or later	The Windows Sidebar will run gadgets that are located in the profile space of the user. Gadgets are small applets that are run by the Windows Sidebar on the Sidebar or on the desktop. If you enable this setting, Windows Sidebar will not run any user installed gadgets. If you disable or do not configure this setting, Windows Sidebar will run user installed gadgets. The default is for Windows Sidebar to run user installed gadgets.
Computer/User	Windows Sidebar	Turn off Windows Sidebar	At least Windows Vista or later	Windows Sidebar is a feature that allows the use of gadgets, which are small applets that may display information or utilities to the user. If you enable this setting, Windows Sidebar will be turned off. If you disable or do not configure this setting, Windows Sidebar will be turned on. The default is for Windows Sidebar to be turned on.
Computer/User	Windows SideShow	Delete data from devices running Microsoft firmware when a user logs off from the computer.	At least Windows Vista or later	This policy setting deletes all data stored on Windows SideShow-compatible devices (running Microsoft firmware) when a user logs off from the computer. This is a security precaution but it significantly limits the usefulness of the devices. If

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				you enable this policy setting, all data stored on devices running Microsoft firmware will be deleted when a user logs off from the computer. Data will be re-sent to the device when the user logs on again. If you disable or do not configure this policy setting, data will not be deleted from these devices when users log off from the computer. Users can enable this setting in the Windows SideShow Control Panel. Note Devices not running Microsoft firmware will not be affected by this policy setting.
Computer/User	Windows SideShow	Require a PIN to access data on devices running Microsoft firmware	At least Windows Vista or later	This policy setting requires users to enter a default personal identification number (PIN) to unlock and access data on the device after a specified period of inactivity (time-out period). This setting applies to Windows SideShow-compatible devices running Microsoft firmware. If you enable this policy setting, users will be required to enter the default PIN to unlock and access data on the device after the specified time-out period. Note Users can change the PIN and time-out periods on the device settings page in the Windows SideShow Control Panel. If you disable or do not configure this policy setting, users will not be required to enter a default PIN to unlock and access data on the device after a specified time-out period. However, users can choose to turn on PIN locking and can change the time-out period in the Windows SideShow Control Panel. Note Devices not running Microsoft firmware will not be affected by this policy setting. Note There is a fixed set of time-out periods which includes: after 1 minute, after 2 minutes, after 5 minutes, after 10 minutes, after 30 minutes, when the screen turns off, never.
Computer/User	Windows SideShow	Turn off automatic wake	At least Windows Vista or later	This policy setting turns off the option to periodically wake the computer to update information on Windows SideShow-compatible devices. If you enable this policy

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				setting, the option to automatically wake the computer will not be available in the Windows SideShow Control Panel. If you disable or do not configure this policy setting, the option to automatically wake the computer will be available in the Windows SideShow Control Panel. However, the option will be disabled by default. Note Information on Windows SideShow-compatible devices will only be updated when the computer is on and awake.
Computer/User	Windows SideShow	Turn off Windows SideShow	At least Windows Vista or later	This policy setting turns off Windows SideShow. If you enable this policy setting, the Windows SideShow Control Panel will be disabled and data from Windows SideShow-compatible gadgets (applications) will not be sent to connected devices. If you disable or do not configure this policy setting, Windows SideShow is on by default.
Computer	Windows System Resource Manager	Set the Email IDs to which notifications are to be sent	At least Windows Vista or later	This setting assigns the email address(es) to which notifications will be sent. Use a semicolon (;) to separate multiple email addresses. If you enable this setting, Windows System Resource Manager (WSRM) will send notifications to the address(es) specified. If you disable this setting, no email addresses (default value) will be set. If you do not configure this setting, the user may specify e-mail addresses to receive notifications. This value can be e-mail aliases or e-mail address including domain name (for example, someone@example.com). Depending on the events selected for notification, these email addresses will be notified. Note : To receive notifications, the notifications setting on the event log must be turned ON. To view the list of events, click Error, Warning, or Information, and then click OK. If you select Error, Warning, or Information, all of the individual events in that category are included.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Windows System Resource Manager	Set the SMTP Server used to send notifications	At least Windows Vista or later	This setting assigns the address of the SMTP server that sends out notifications. If you enable this setting, Windows System Resource Manager (WSRM) will set the SMTP server to the value specified. If you disable this setting, no SMTP server (default value) will be set. If you do not configure this setting, the user may specify an SMTP server. This value can be the NetBIOS name or the fully qualified domain name (FQDN) of the Simple Mail Transfer Protocol (SMTP) server. This server contains the email addresses that are configured to receive notifications. Note : To receive email notifications, the notifications setting on the event log must be turned ON. To view the list of events, click Error, Warning, or Information, and then click OK. If you select Error, Warning, or Information, all of the individual events in that category are included.
Computer	Windows System Resource Manager	Set the Time interval in minutes for logging accounting data	At least Windows Vista or later	This setting directs the Accounting feature to log data on the accounting server at the specified time interval. If you enable this setting, Windows System Resource Manager (WSRM) will set the accounting time interval to the value specified. If you disable this setting, the default value of 10 minutes will be set. If you do not configure this setting, the user may specify an accounting interval. The value is specified in minutes and can range between 2 minutes and 60000 minutes. Ten minutes is provided as the default value as this would be an optimal value if there are many servers logging data remotely. Setting an accounting record write interval value less than 10 minutes for a server on a network with more than 20 machines logging data remotely can possibly degrade performance. Note : Set the accounting record write interval to a higher value as the number of machines increases on the network to reduce network congestion.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Windows System Resource Manager	Turn on Accounting for WSRM	At least Windows Vista or later	This setting turns the Accounting feature On or Off. If you enable this setting, Windows System Resource Manager (WSRM) will start accounting various usage statistics of the processes. If you disable this setting, WSRM will stop logging usage statistics of processes. If you do not configure this setting, the user can specify whether accounting needs to be turned On or Off. The accounting processes is disabled by default. The accounting database provides an interface you can use to manage both the information in the database and the physical size of the database. Managing database information involves finding relevant information and then organizing it efficiently. Managing the physical size of the database requires regular attention because, unless it is configured to do otherwise, Windows System Resource Manager continues to store accounting information. As a result, the size of the database continues to increase. To manage the size of the database, you can archive accounting data for later use or delete it from the database. You can use accounting data can to monitor resource usage, compare actual and expected performance, assess whether the computer's physical resources are sufficient for its intended tasks, and provide the basis for charge-back accounting.
Computer	Windows Update	Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates	At least Windows Vista or later	Specifies whether the Windows Update will use the Windows Power Management features to automatically wake up the system from hibernation, if there are updates scheduled for installation. Windows Update will only automatically wake up the system if Windows Update is configured to install updates automatically. If the system is in hibernation when the scheduled install time occurs and there are updates to be applied, then Windows Update will use the Windows Power

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				management features to automatically wake the system up to install the updates. Windows update will also wake the system up and install an update if an install deadline occurs. The system will not wake unless there are updates to be installed. If the system is on battery power, when Windows Update wakes it up, it will not install updates and the system will automatically return to hibernation in 2 minutes.
Computer	Windows Update	Turn on recommended updates via Automatic Updates	At least Windows Vista or later	Specifies whether Automatic Updates will deliver both important as well as recommended updates from the Windows Update update service. When this policy is enabled, Automatic Updates will install recommended updates as well as important updates from Windows Update update service. When disabled or not configured Automatic Updates will continue to deliver important updates if it is already configured to do so.
Computer	WinRM Client	Allow Basic authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. If you enable this policy setting, the WinRM client will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text. If you disable or do not configure this policy setting, then the WinRM client will not use Basic authentication.
Computer	WinRM Client	Allow unencrypted traffic	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the network.
Computer	WinRM Client	Disallow Digest authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication. If you enable this policy setting, the WinRM client will not use Digest authentication. If you disable or do not configure this policy setting, the WinRM client will use Digest authentication.
Computer	WinRM Client	Disallow Kerberos authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Kerberos authentication directly. If you enable this policy setting, the Windows Remote Management (WinRM) client will not use Kerberos authentication directly. Kerberos may still be used if the WinRM client is using the Negotiate authentication and Kerberos is selected. If you disable or do not configure this policy setting, the WinRM client will use the Kerberos authentication directly.
Computer	WinRM Client	Disallow Negotiate authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Negotiate authentication. If you enable this policy setting, the WinRM client will not use Negotiate authentication. If you disable or do not configure this policy setting, the WinRM client will use Negotiate authentication.
Computer	WinRM Client	Trusted Hosts	At least Windows Vista or later	This policy setting allows you to manage whether Windows Remote Management (WinRM) client uses the list specified in TrustedHostsList to determine if the destination host is a trusted entity. If you enable this policy setting, the WinRM client uses the list specified in TrustedHostsList to determine if the destination host is a trusted entity. The WinRM client uses this list when neither HTTPS nor

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Kerberos are used to authenticate the identity of the host. If you disable or do not configure this policy setting and the WinRM client needs to use the list of trusted hosts, you must configure the list of trusted hosts locally on each computer.
Computer	WinRM Service	Allow automatic configuration of listeners	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port. If you enable this policy setting, the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port. If you disable or do not configure this policy setting, then the WinRM service does not automatically listen on the network and you must manually create listeners on every computer. To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting with exceptions for Port 80 (default port for HTTP) and 443 (default port for HTTPS). The service listens on the addresses specified by the IPv4 and IPv6 filters. IPv4 filter specifies one or more ranges of IPv4 addresses and IPv6 filter specifies one or more ranges of IPv6addresses. If specified, the service enumerates the available IP addresses on the computer and uses only addresses that fall within one of the filter ranges. You should use asterisk (*) to indicate that the service listens on all available IP addresses on the computer. When * is used, other ranges in the filter are ignored. If the filter is left blank, the service does not listen on any addresses. For example, if you want the service to listen only on IPv4 addresses, leave the IPv6 filter empty. Ranges are specified using the syntax IP1-IP2. Multiple ranges are separated using "," (comma) as the delimiter. Example IPv4 filters: 2.0.0.1-2.0.0.20, 24.0.0.1-24.0.0.22 Example IPv6

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				filters: 3FFE:FFFF:7654:FEDA:1245:BA98:0000:0000-3FFE:FFFF:7654:FEDA:1245:BA98:3210:4562
Computer	WinRM Service	Allow Basic authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client. If you enable this policy setting, the WinRM service will accept Basic authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service will not accept Basic authentication from a remote client.
Computer	WinRM Service	Allow unencrypted traffic	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network.
Computer	WinRM Service	Disallow Kerberos authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not accept Kerberos credentials over the network. If you enable this policy setting, the WinRM service will not accept Kerberos credentials over the network. If you disable or do not configure this policy setting, then the WinRM service will accept Kerberos authentication from a remote client.
Computer	WinRM Service	Disallow Negotiate authentication	At least Windows Vista or later	This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not accept Negotiate authentication from a remote client. If you enable this policy setting, the WinRM service will not accept

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Negotiate authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service will accept Negotiate authentication from a remote client.
Node	Subnode	Full-policy Name	Supported On	Help/Explain Text
Computer/User	Accessories	Do not allow Inkball to run	At least Windows Vista or later	Prevents start of InkBall game. If you enable this policy, the InkBall game will not run. If you disable this policy, the InkBall game will run. If you do not configure this policy, the InkBall game will run.
Computer/User	Accessories	Do not allow printing to Journal Note Writer	At least Windows Vista or later	Prevents printing to Journal Note Writer. If you enable this policy, the Journal Note Writer printer driver will not allow printing to it. It will remain displayed in the list of available printers, but attempts to print to it will fail. If you disable this policy, you will be able to use this feature to print to a Journal Note. If you do not configure this policy, users will be able to use this feature to print to a Journal Note.
Computer/User	Accessories	Do not allow Snipping Tool to run	At least Windows Vista or later	Prevents the snipping tool from running. If you enable this policy setting, the Snipping Tool will not run. If you disable this policy setting, the Snipping Tool will run. If you do not configure this policy setting, the Snipping Tool will run.
Computer/User	Accessories	Do not allow Sticky Notes to be run	At least Windows Vista or later	Prevents start of Sticky Notes. If you enable this policy, the Sticky Notes accessory will not run. If you disable this policy, the Sticky Notes accessory will run. If you do not configure this policy, the Sticky Notes accessory will run.
Computer/User	Accessories	Do not allow Windows Journal to be run	At least Windows Vista or later	Prevents start of Windows Journal. If you enable this policy, the Windows Journal accessory will not run. If you disable this policy, the Windows Journal accessory will run. If you do not configure this policy, the Windows Journal accessory will run.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	ActiveX Installer Service	Approved Installation Sites for ActiveX Controls	At least Windows Vista or later	The ActiveX Installer Service is the solution to delegate the install of per-machine ActiveX controls to a Standard User in the enterprise. The list of Approved ActiveX Install sites contains the host URL and the policy settings for each host URL. Wild cards are not supported.
Computer	Advanced Error Reporting Settings	Configure Corporate Windows Error Reporting	At least Windows Vista or later	This setting determines the corporate server to which Windows Error Reporting will send reports (instead of sending reports to Microsoft). Server port indicates the port to use on the target server. Connect using SSL determines whether Windows will send reports to the server using a secured connection.
Computer/User	Advanced Error Reporting Settings	Configure Report Archive	At least Windows Vista or later	This setting controls the behavior of the Windows Error Reporting archive. If Archive behavior is set to "Store all", all data collected for each report will be stored in the appropriate location. If Archive behavior is set to "Store parameters only", only the minimum information required to check for an existing solution will be stored. The setting for "Maximum number of reports to store" determines how many reports can be stored before old reports are automatically deleted. If this setting is disabled, no Windows Error Reporting information will be stored.
Computer/User	Advanced Error Reporting Settings	Configure Report Queue	At least Windows Vista or later	This setting determines the behavior of the Windows Error Reporting queue. If Queuing behavior is set to "Default", Windows will decide each time a problem occurs whether the report should be queued or the user should be prompted to send it immediately. If Queuing behavior is set to "Always queue", all reports will be queued until the user is notified to send them or until the user chooses to send them using the Solutions to Problems control panel. If Queuing behavior is set to "Always queue for administrator", reports will be queued until an administrator is notified to send them or chooses to send them using the Solutions to Problems

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				control panel. The setting for "Maximum number of reports to queue" determines how many reports can be queued before old reports are automatically deleted. The setting for "Number of days between solution check reminders" determines the interval time between the display of system notifications which remind the user to check for solutions to problems. A setting of 0 will disable the reminder. If the Windows Error Reporting queue setting is disabled, no Windows Error Reporting information will be queued and users will be able to send reports only at the time a problem occurs.
Computer/User	Advanced Error Reporting Settings	List of applications to be excluded	At least Windows Vista or later	This setting determines the behavior of the error reporting exclusion list. Windows will not send reports for any process added to this list. Click "Show" to display the exclusion list. Click "Add..." and type a process name to add a process to the list. Select a process name and click "Remove" to remove a process from the list. Click "OK" to save the list.
Computer	Application, Security, Setup, System	Backup log automatically when full	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its maximum size and takes effect only if the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled. If you enable this policy setting and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, the Event Log file is automatically closed and renamed when it is full. A new file is then started. If you disable this policy setting and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, then new events are discarded and the old events are retained. When this policy setting is not configured and the ΓÇ£Retain old eventsΓÇ¥ policy setting is enabled, new events are discarded and the old events are retained.
Computer	Application, Security,	Retain old events	At least Windows Vista or later	This policy setting controls Event Log behavior when the log file reaches its

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Setup, System			maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events. Note: Old events may or may not be retained according to the ΓÇ£Backup log automatically when fullΓÇ¥ policy setting.
Computer/User	Application Compatibility	Turn Off Program Compatibility Assistant	At least Windows Vista or later	This policy controls the state of the Program Compatibility Assistant in the system. The PCA monitors user initiated programs for known compatibility issues at run time. Whenever a potential issue with an application is detected, the PCA will prompt the user with pointers to recommended solutions. For more information on the various issue detection scenarios covered by PCA and the policies to configure them, refer to policies under System-&gt;Troubleshooting and Diagnostics-&gt;Application Compatibility Diagnostics. The PCA is on by default. If you enable this policy setting, the PCA will be turned off. This option is useful for system administrators who require faster performance and are aware of the compatibility of the applications they are using. Note: With the PCA turned off, the user will not be presented with solutions to known compatibility issues when running applications. If you disable or do not configure this policy setting, the PCA will be turned on. Note: The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect application failures caused by deprecated Windows DLLs or	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose DLL load or COM object creation failures in programs. If you enable

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		COM objects		this policy setting, the PCA detects programs trying load legacy Microsoft Windows DLLs or creating legacy COM objects that are removed in this version of Windows. When this failure is detected, after the program is terminated, PCA will notify the user about this problem and provide an option to check the Microsoft Web site for solutions. If you disable this policy setting, the PCA does not detect programs trying to load legacy Windows DLLs or creating legacy COM objects. If you do not configure this policy setting, the PCA detects programs trying to load legacy Windows DLLs or creating legacy COM objects. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect application install failures	At least Windows Vista or later	This policy setting configures the Program Compatibility Assistant (PCA) to diagnose failures with application installations. If you enable this policy setting, the PCA is configured to detect failures in the execution of application installers through heuristics. When potential failures are detected, the PCA will provide the user with an option to restart the installer with Microsoft Windows XP compatibility mode. If you disable this policy setting, the PCA is not configured to detect failures in execution of program installers. If you do not configure this policy setting, the PCA will enable this diagnostic scenario by default. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect application installers that need to be run as administrator	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose failures with application installers that are not detected to run as administrator. If you enable this policy setting, the PCA is configured to detect application installers which do not have privileges to run as administrator by the User Access Control (UAC). When potential failures are detected, the PCA will provide the user with an option to restart the installer as administrator. If you disable this policy setting, the PCA will not detect application installers which do not have privileges to run as administrator by the UAC. If you do not configure this policy setting, the PCA will be configured to detect application installers which do not have privileges to run as administrator by the UAC. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Detect applications unable to launch installers under UAC	At least Windows Vista or later	This policy setting configures the Program Compatibility Assistant (PCA) to diagnose failures with programs under User Account Control (UAC). If you enable this policy setting, the PCA detects programs that failed to launch child processes that are installers (typically updaters). When this failure is detected, the PCA will apply the ELEVATECREATEPROCESS compatibility mode, which enables the program to successfully launch the installer as with administrator privileges the next time the program is run. If you disable this policy setting, the PCA will not

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				detect applications that fail to launch installers run under UAC. If you do not configure this policy setting, the PCA detects programs that failed to launch child processes that are installers (typically updaters). Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application Compatibility Diagnostics	Notify blocked drivers	At least Windows Vista or later	This policy setting determines whether the Program Compatibility Assistant (PCA) will diagnose drivers blocked due to compatibility issues. If you enable this policy setting, the PCA will notify the user of blocked driver issues with an option to check the Microsoft Web site for solutions. If you disable this policy setting, the PCA will not notify the user of blocked driver issues. Note: With this policy setting in a disabled state, the user will not be presented with solutions to blocked drivers. If you do not configure this policy setting, the PCA will notify the user of blocked driver issues with an option to check the Microsoft Web site for solutions. Note: Disabling the "Turn off Program Compatibility Assistant" policy setting will cause this policy setting to have no effect. The Diagnostic Policy Service (DPS) and Program Compatibility Assistant Service must be running for the PCA to execute. These services can be configured using the Services snap-in to the Microsoft Management Console.
Computer	Application, Security, Setup, System	**Log Access**	At least Windows Vista or later	This policy setting specifies to use the security descriptor for the log using the Security Descriptor Definition Language (SDDL) string. If this policy setting is enabled, only those users matching the security descriptor can access the log. If

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this policy setting is disabled or not configured, then all authenticated users and system services can write/read/clear this log.
Computer	Application, Security, Setup, System	**Log File Path**	At least Windows Vista or later	This policy setting controls the location of the log file. The location of the file must be writable by the Event Log service and should only be accessible to administrators. If you enable this policy setting, the Event Log uses the specified path provided in this policy setting. If you disable or do not configure this policy setting, the Event Log uses the system32 or system64 subdirectory.
Computer	Application, Security, Setup, System	Maximum Log Size (KB)	At least Windows Vista or later	This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file maximum size will be set to the local configuration value. This value can be changed by the local administrator using the log properties dialog and it defaults to 20 megabytes.
Computer/User	AutoPlay Policies	Default behavior for AutoRun	At least Windows Vista or later	Sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior in Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog. If you enable this policy, an Administrator can change the default Windows Vista behavior for autorun to: A)

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Completely disable autorun commands, or B) Revert back to Pre-Windows Vista behavior of automatically executing the autorun command. If you disable or not configure this policy, Windows Vista will prompt the user whether autorun command is to be run.
Computer/User	AutoPlay Policies	Don't set the always do this checkbox	At least Windows Vista or later	If this policy is enabled, the "Always do this..." checkbox in Autoplay dialog will not be set by default when the dialog is shown.
Computer	Background Intelligent Transfer Service (BITS)	Allow BITS Peercaching	At least Windows Vista or later	This setting determines if the BITS Peer-caching feature is enabled on a specific computer. By default, the files in a BITS job are downloaded only from the originating server specified by the jobΓÇÖs owner. Each client computer will download its own copy of the files from the origin server. If BITS Peer-caching is enabled, BITS will cache download jobs and make the content available to other BITS peers. When running a download job, BITS will first request the files for the job from one of its peers in the same IP subnet. If none of the peers in the subnet have the requested files, BITS will download the files for the job from the original server. If you enable this setting, BITS will cache jobs, respond to content requests from peers, and download job content from peers if possible. If you disable this setting or do not configure it, the peer-caching feature will be disabled and BITS will download files directly from the original server.
Computer	Background Intelligent Transfer Service (BITS)	Do not allow the computer to act as a BITS Peercaching client	At least Windows Vista or later	This setting specifies whether the computer will act as a BITS peercaching client. By default, when BITS peercaching is enabled, the computer acts as both a peercaching server (offering files to its peers) and a peercaching client (downloading files from its peers). If you enable this setting, the computer will no longer use the BITS Peercaching feature to download files; files will be

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				downloaded only from the origin server. However, the computer will still make files available to its peers. If you disable or do not configure this setting, the computer attempts to download peer enabled BITS jobs from peer computers before reverting to the origin server. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Do not allow the computer to act as a BITS Peercaching server	At least Windows Vista or later	This setting specifies whether the computer will act as a BITS peercaching server. By default, when BITS peercaching is enabled, the computer acts as both a peercaching server (offering files to its peers) and a peercaching client (downloading files from its peers). If you enable this setting, the computer will no longer cache downloaded files and offer them to its peers. However, the computer will still download files from peers. If you disable or do not configure this setting, the computer will offer downloaded and cached files to its peers. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Limit age of items in the BITS Peercache	At least Windows Vista or later	This setting specifies the maximum age of files in the Peercache. In order to make the most efficient use of disk space, by default BITS removes any files in the cache older than 14 days. If you enable this setting, you can specify the maximum age of files in the cache in days. You can enter a value between 1 and 120 Days. If you disable this setting or do not configure it, files older than 14 days will be removed from the Peercache. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Limit the BITS Peercache size	At least Windows Vista or later	This setting specifies the maximum amount of disk space that can be used for the BITS Peercache, as a percentage of the total system disk size. BITS will add files

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				to the Peercache and make those files available to peers until the cache content reaches the specified cache size. By default, BITS will use 1% of the total system disk for the peercache. If you enable this setting, you can enter the percentage of disk space to be used for the BITS peercache. You can enter a value between 1% and 80%. If you disable this setting or do not configure it, the default size of the BITS peercache is 1% of the total system disk size. Note: This setting has no effect if the "Allow BITS Peercaching"setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Maximum BITS job download time	At least Windows Vista or later	This setting limits the amount of time that BITS will take to download the files in a BITS job. The time limit applies only to the time that BITS is actively downloading files, not real-time. When the cumulative download time exceeds this limit, the job is placed in the error state. By default BITS uses a maximum download time of 15 days (54000 seconds). If you enable this setting, you can set the maximum job download time to the specified number of seconds. If you disable or do not configure this setting, the default value of 15 days (54000 seconds) will be used for the maximum job download time.
Computer	Background Intelligent Transfer Service (BITS)	Maximum network bandwidth used for Peercaching	At least Windows Vista or later	This setting limits the network bandwidth that BITS uses for peercache transfers (this setting does not affect transfers from the origin server). To prevent any negative impact to a computer caused by serving other peers, by default BITS will use up to 30% of the bandwidth of the slowest active network interface. For example, if a computer has both a 100Mbps network card, and a 56 Kbps modem, and both are active, BITS will use a maximum of 30% of 56Kbps. You can change the default behavior of BITS, and specify a fixed maximum bandwidth that BITS will use for Peercaching. If you enable this setting, you can enter a

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				value in bits per second (bps) between 1048576 and 4294967200 to use as the maximum network bandwidth used for peer-caching. If you disable this setting or do not configure it, the default value of 30% of the slowest active network interface will be used. Note: This setting has no effect if the ΓÇ£Allow BITS peercachingΓÇ¥ setting is disabled or not configured.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of BITS jobs for each user	At least Windows Vista or later	This setting specifies the maximum number of BITS jobs that can be created by a user. By default, BITS limits the total number of jobs that can be created by a user to 60 jobs. You can use this setting to raise or lower the maximum number of BITS jobs a user can create. If you enable this setting, BITS will limit the maximum number of BITS jobs a user can create to the specified number. If you disable or do not configure this setting, BITS will use the default user BITS job limit of 300 jobs. Note: This limit must be lower than the setting specified in ΓÇ£Maximum number of BITS jobs for this computerΓÇ¥, or 300 if the ΓÇ£Maximum number of BITS jobs for this computerΓÇ¥ setting is not configured. BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of BITS jobs for this computer	At least Windows Vista or later	This setting specifies the maximum number of BITS jobs that can be created for all users of the computer. By default, BITS limits the total number of jobs that can be created on the computer to 300 jobs. You can use this setting to raise or lower the maximum number of user BITS jobs. If you enable this setting, BITS will limit the maximum number of BITS jobs to the specified number. If you disable or do not configure this setting, BITS will use the default BITS job limit of 300 jobs. Note: BITS Jobs created by services and the local administrator account do not

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of files allowed in a BITS job	At least Windows Vista or later	This setting specifies the maximum number of files that a BITS job can contain. By default, a BITS job is limited to 200 files. You can use this setting to raise or lower the maximum number of files a BITS jobs can contain. If you enable this setting, BITS will limit the maximum number of files a job can contain to the specified number. If you disable or do not configure this setting, BITS will use the default value of 200 for the maximum number of files a job can contain. Note: BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	Background Intelligent Transfer Service (BITS)	Maximum number of ranges that can be added to the file in a BITS job	At least Windows Vista or later	This setting specifies the maximum number of ranges that can be added to a file in a BITS job. By default, files in a BITS job are limited to 500 ranges per file. You can use this setting to raise or lower the maximum number ranges per file. If you enable this setting, BITS will limit the maximum number of ranges that can be added to a file to the specified number. If you disable or do not configure this setting, BITS will limit ranges to 500 ranges per file. Note: BITS Jobs created by services and the local administrator account do not count towards this limit.
Computer	BitLocker Drive Encryption	Configure encryption method	At least Windows Vista or later	This policy setting allows you to configure the algorithm and key size used by BitLocker Drive Encryption. This policy setting applies on a fully-decrypted disk. Changing the encryption method has no effect if the disk is already encrypted or if encryption is in progress. If you enable this policy setting, you can configure the encryption method used on an unencrypted volume. Consult online documentation for more information about the available encryption methods. If you disable or do not configure this policy setting, BitLocker will use the default

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				encryption method of AES 128 bit with Diffuser or the encryption method specified by a local administrator's setup script.
Computer	BitLocker Drive Encryption	Configure TPM platform validation profile	At least Windows Vista or later	This policy setting allows you to configure how the computer's Trusted Platform Module (TPM) security hardware secures the BitLocker encryption key. This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection. If you enable this policy setting before turning on BitLocker, you can configure the boot components that the TPM will validate before unlocking access to the BitLocker-encrypted OS volume. If any of these components change while BitLocker protection is in effect, the TPM will not release the encryption key to unlock the volume and the computer will enter into recovery mode during boot. If you disable or do not configure this policy setting, the TPM uses the default platform validation profile or the platform validation profile specified by a local administrator's setup script. The default platform validation profile secures the encryption key against changes to the Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions (PCR 0), the Option ROM Code (PCR 2), the Master Boot Record (MBR) Code (PCR 4), the NTFS Boot Sector (PCR 8), the NTFS Boot Block (PCR 9), the Boot Manager (PCR 10), and the BitLocker Access Control (PCR 11). WARNING: Changing from the default profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending upon inclusion or exclusion (respectively) of the PCRs.
Computer	BitLocker Drive	Control Panel Setup: Configure	At least Windows Vista or later	This policy setting allows you to specify the default path that is displayed when

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	Encryption	recovery folder		the BitLocker Drive Encryption setup wizard prompts the user to enter the location of a folder in which to save the recovery password. If you enable this policy setting, you can specify the path that will be used as the default folder location when the user chooses the option to save the recovery password in a folder. You can specify either a fully-qualified path or include the target computer's environment variables in the path. If the path is not valid, the BitLocker setup wizard will display the computer's top-level folder view. If you disable or do not configure this policy setting, the BitLocker setup wizard will display the computer's top-level folder view when the user chooses the option to save the recovery password in a folder. Note: In all cases, the user will be able to select other folders in which to save the recovery password.
Computer	BitLocker Drive Encryption	Control Panel Setup: Configure recovery options	At least Windows Vista or later	This policy setting allows you to configure whether the BitLocker Drive Encryption setup wizard will ask the user to save BitLocker recovery options. Two recovery options can unlock access to BitLocker-encrypted data. The user can type a random 48-digit numerical recovery password. The user can also insert a USB flash drive containing a random 256-bit recovery key. If you enable this policy setting, you can configure the options that the setup wizard exposes to users for recovering BitLocker. For example, disallowing the 48-digit recovery password will prevent users from being able to print or save recovery information to a folder. If you disable or do not configure this policy setting, the BitLocker setup wizard will present users with ways to store recovery options. Saving to a USB flash drive will store the 48-digit recovery password as a text file, and the 256-bit recovery key as a hidden file. Saving to a folder will store the 48-digit recovery password as a text

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				file. Printing will provide the 48-digit recovery password. Note: If TPM initialization is needed during the BitLocker setup, TPM owner information will be saved or printed with the BitLocker recovery information. Note: The 48-digit recovery password will not be available in FIPS compliance mode. IMPORTANT: To prevent data loss, you must have a way to recover BitLocker. If you disallow both recovery options below, you must enable the policy setting to "Turn on BitLocker backup to Active Directory Domain Services". Otherwise, a policy error occurs.
Computer	BitLocker Drive Encryption	Control Panel Setup: Enable advanced startup options	At least Windows Vista or later	This policy setting allows you to configure whether the BitLocker Drive Encryption setup wizard will ask the user to set up an additional authentication that is requested each time the computer starts. On a computer with a compatible Trusted Platform Module (TPM), two types of startup authentications can work to provide added protection for encrypted data. When the computer starts, it can require users to insert a USB flash drive containing a startup key. It can also require users to enter a 4 to 20 digit startup PIN. A USB flash drive containing a startup key is needed on computers without a compatible Trusted Platform Module (TPM). Without a TPM, BitLocker-encrypted data is protected solely by the key material on this USB flash drive. If you enable this policy setting, the wizard will show the page to allow the user to configure advanced startup options for BitLocker. You can further configure setting options for computers with and without a TPM. If you disable or do not configure this policy setting, the BitLocker setup wizard will display basic steps that allow users to enable BitLocker on computers with a TPM. In this basic wizard, no additional startup key or startup PIN can be configured.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	BitLocker Drive Encryption	Turn on BitLocker backup to Active Directory Domain Services	At least Windows Vista or later	This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of BitLocker Drive Encryption recovery information. If you enable this policy setting, BitLocker recovery information will be automatically and silently backed up to AD DS when BitLocker is turned on for a computer. BitLocker recovery information includes the recovery password and some unique identifier data. You can also include a package that contains a BitLocker-protected volume's encryption key. This key package is secured by one or more recovery passwords and may help perform specialized recovery when the disk is damaged or corrupted. If you select the option to "Require BitLocker backup to AD DS", BitLocker cannot be turned on unless the computer is connected to the domain and the AD DS backup succeeds. This option is selected by default to help ensure that BitLocker recovery is possible. Otherwise, AD DS backup is attempted but network or other backup failures do not impact BitLocker setup. Backup is not automatically retried and the recovery password may not have been stored in AD DS during BitLocker setup. If you disable or do not configure this policy setting, BitLocker recovery information will not be backed up to AD DS. IMPORTANT: To prevent data loss, you must have a way to recover BitLocker. Note: You must first set up appropriate schema extensions and access control settings on the domain before AD DS backup can succeed. Consult online documentation for more information about setting up Active Directory Domain Services for BitLocker. Note: TPM initialization may be needed during BitLocker setup. Enable the policy setting to "Turn on TPM backup to Active Directory Domain Services" in "System\Trusted Platform Module Services\" to ensure that

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				TPM information is also backed up.
Computer	Button Settings	Select the Lid Switch Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user closes the lid on a mobile PC. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Lid Switch Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user closes the lid on a mobile PC. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Power Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the power button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Power Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the power button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Sleep Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the sleep button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Sleep Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the sleep button. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Start Menu Power Button Action (On Battery)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the user interface sleep button. Possible actions include: -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Button Settings	Select the Start Menu Power Button Action (Plugged In)	At least Windows Vista or later	Specifies the action that Windows takes when a user presses the user interface sleep button. Possible actions include: -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer/User	Client	Prevent backing up to local disks	At least Windows Vista or later	This setting lets you prevent users from selecting a local disk (internal or external) for storing file backups. If this setting is enabled, the user will be blocked from selecting a local disk as a file backup location. If this setting is disabled or not configured, users can select a local disk as a file backup location.
Computer/User	Client	Prevent backing up to network shared folder	At least Windows Vista or later	This setting lets you prevent users from selecting a network shared folder for storing file backups. If this setting is enabled, users will be blocked from selecting a network shared folder as a file backup location. If this setting is disabled or not configured, users can select a network shared folder as a file backup location.
Computer/User	Client	Prevent backing up to optical media (CD/DVD)	At least Windows Vista or later	This setting lets you prevent users from selecting optical media (CD/DVD) for storing file backups. If this setting is enabled, users will be blocked from selecting optical media as a file backup location. If this setting is disabled or not configured, users can select optical media as a file backup location.
Computer/User	Client	Prevent the user from running the	At least Windows Vista or later	This setting lets you disable the Backup Status and Configuration program, which

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
		Backup Status and Configuration program		links to the file backup, file restore, and Complete PC Backup applications and shows backup status. If this setting is enabled, a user cannot start the Backup Status and Configuration program. If this setting is disabled or not configured, users can start the Backup Status and Configuration program.
Computer/User	Client	Turn off backup configuration	At least Windows Vista or later	This setting lets you disable file backup functionality. If this setting is enabled, the file backup program is disabled. If this setting is disabled or not configured, the file backup program is enabled and users can create a file backup.
Computer/User	Client	Turn off Complete PC Backup functionality	At least Windows Vista or later	This setting lets you disable Complete PC Backup functionality. If this setting is enabled, the Complete PC Backup program is disabled. If this setting is disabled or not configured, the Complete PC Backup program is enabled and users can create a Complete PC Backup image.
Computer/User	Client	Turn off restore functionality	At least Windows Vista or later	This setting lets you disable file restore functionality. If this setting is enabled, the file restore program is disabled. If this setting is disabled or not configured, the file restore program is enabled and users can restore files.
Computer/User	Consent	Configure Default consent	At least Windows Vista or later	This setting determines the consent behavior of Windows Error Reporting. If Consent level is set to "Always ask before sending data", Windows will prompt the user for consent to send reports. If Consent level is set to "Send parameters", the minimum data required to check for an existing solution will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If Consent level is set to "Send parameters and safe additional data", the minimum data required to check for an existing solution as well as data which Windows has determined does not contain (within a high probability) personally identifiable data will be sent automatically, and Windows

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				will prompt the user for consent to send any additional data requested by Microsoft. If Consent level is set to "Send all data", any data requested by Microsoft will be sent automatically. If this setting is disabled or not configured then consent will default to "Always ask before sending data".
Computer/User	Consent	Customize consent settings	At least Windows Vista or later	This policy setting determines the consent behavior of Windows Error Reporting for specific event types. If this policy setting is enabled and the consent level is set to "0" (Disable), Windows Error Reporting will not send any data to Microsoft for this event. If the consent level is set to "1" (Always ask before sending data), Windows will prompt the user for consent to send reports. If the consent level is set to "2" (Send parameters), the minimum data required to check for an existing solution will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If the consent level is set to "3" (Send parameters and safe additional data), the minimum data required to check for an existing solution as well as data which Windows has determined does not contain (within a high probability) personally identifiable data will be sent automatically, and Windows will prompt the user for consent to send any additional data requested by Microsoft. If the consent level is set to "4" (Send all data), any data requested by Microsoft will be sent automatically. If this setting is disabled or not configured then consent will default to the default consent setting.
Computer/User	Consent	Ignore custom consent settings	At least Windows Vista or later	This setting determines the behavior of the default consent setting in relation to custom consent settings. If this setting is enabled, the default Consent level setting will always override any other consent setting. If this setting is disabled or not configured, each custom consent setting will determine the consent level for

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				that event type and the default consent setting will determine the consent level of any other reports.
Computer	Corrupted File Recovery	Configure Corrupted File Recovery Behavior	At least Windows Vista or later	This policy setting allows you to configure the recovery behavior for corrupted files to one of three states: Regular: Detection, troubleshooting, and recovery of corrupted files will automatically start with a minimal UI display. Windows will attempt to present you with a dialog box when a system restart is required. This is the default recovery behavior for corrupted files. Silent: Detection, troubleshooting, and recovery of corrupted files will automatically start with no UI. Windows will log an administrator event when a system restart is required. This behavior is recommended for headless operation. Troubleshooting Only: Detection and troubleshooting of corrupted files will automatically start with no UI. Recovery is not attempted automatically. Windows will log an administrator event with instructions if manual recovery is possible. If you enable this setting, the recovery behavior for corrupted files will be set to either the regular (default), silent, or troubleshooting only state. If you disable this setting, the recovery behavior for corrupted files will be disabled. No troubleshooting or resolution will be attempted. If you do not configure this setting, the recovery behavior for corrupted files will be set to the regular recovery behavior. No system or service restarts are required for changes to this policy to take immediate effect after a Group Policy refresh. Note: This policy setting will take effect only when the Diagnostic Policy Service (DPS) is in the running state. When the service is stopped or disabled, system file recovery will not be attempted. The DPS can be configured with the Services snap-in to the Microsoft Management Console.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Credential User Interface	Do not enumerate administrator accounts on elevation.	At least Windows Vista or later	By default all administrator accounts are displayed when attempting to elevate a running application. If you enable this policy, users will be required to always type in a username and password to elevate. If you disable this policy, all local administrator accounts on the machine will be displayed so the user can choose one and enter the correct password.
Computer	Credential User Interface	Require trusted path for credential entry.	At least Windows Vista or later	This policy setting requires the user to enter Microsoft Windows credentials using a trusted path, to prevent a Trojan horse or other types of malicious code from stealing the userΓÇÖs Windows credentials. Note: This policy affects nonlogon authentication tasks only. As a security best practice, this policy should be enabled. If you enable this policy setting, users will be required to enter Windows credentials on the Secure Desktop by means of the trusted path mechanism. If you disable or do not configure this policy setting, users will enter Windows credentials within the userΓÇÖs desktop session, potentially allowing malicious code access to the userΓÇÖs Windows credentials.
Computer	Credentials Delegation	Allow Default Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can be delegated when the authentication mechanism is NTLM (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, delegation of default credentials is not permitted to any machine. Note that "Allow Delegating Default Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. Note: The "Allow Default Credentials with NTLM-only Server Authentication" can

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Default Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can be delegated (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, delegation of default credentials is not permitted to any machine. Note: The "Allow Delegating Default Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Fresh Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's fresh credentials can be delegated when the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				authentication mechanism is NTLM (fresh credentials are those that you are prompted for when executing the application). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of fresh credentials is permitted to Terminal Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note: "Allow Delegating Fresh Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow Fresh Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Delegating Saved Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can be delegated (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of saved credentials is permitted to Terminal Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note:The "Allow

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Delegating Saved Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Fresh Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's fresh credentials can be delegated when the authentication mechanism is NTLM (fresh credentials are those that you are prompted for when executing the application). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of fresh credentials is permitted to Terminal Server running on any machine (TERMSRV/*). If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note: "Allow Delegating Fresh Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow Fresh Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com
Computer	Credentials Delegation	Allow Saved Credentials with NTLM-only Server Authentication	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can be delegated to when the authentication mechanism is NTLM (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you do not configure (by default) this policy setting, after proper mutual authentication, delegation of saved credentials is permitted to Terminal Server running on any machine (TERMSRV/*) if the client machine is not a member of any domain. If the client is domain-joined, then by default the delegation of saved credentials is not permitted to any machine. If you disable this policy setting delegation of fresh credentials is not permitted to any machine. Note: that "Allow Delegating Saved Credentials" policy applies when server authentication was achieved via a trusted X509 certificate or Kerberos. The "Allow Saved Credentials with NTLM-only Server Authentication" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Credentials Delegation	Deny Delegating Default Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's default credentials can NOT be delegated to (default credentials are those that you use when first logging on to Windows). If you disable or do not configure (by default) this policy setting, this setting does not specify any server. Note: "The Deny Delegating Default Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Default Credentials" to define exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Default Credentials" server list.
Computer	Credentials Delegation	Deny Delegating Fresh Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's fresh credentials can NOT be delegated (fresh credentials are those that you are prompted for when executing the application). If you disable or do not configure (by default) this policy setting, this setting does not specify any server. Note: The "Deny Delegating Fresh Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Fresh Credentials" to define exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Fresh Credentials" server list.
Computer	Credentials Delegation	Deny Delegating Saved Credentials	At least Windows Vista or later	This policy setting applies to applications using the Cred SSP component (for example: Terminal Server). If you enable this policy setting you can specify the servers to which the user's saved credentials can NOT be delegated (saved credentials are those that you elect to save/remember using the Windows credentials manager). If you disable or do not configure (by default) this policy setting, this setting does not specify any server. Note: The "Deny Delegating Saved Credentials" can be set to one or more Service Principal Names (SPNs). The SPN represents the target server to which the user credentials can be delegated. The use of a single wildcard is permitted when specifying the SPN. For Example: TERMSRV/star.humanresources.fabrikam.com Terminal server running on star.humanresources.fabrikam.com machine TERMSRV/* Terminal servers running on all machines. TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in .humanresources.fabrikam.com This setting can be used in combination with "Allow Delegating Saved Credentials" to define

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				exceptions for specific servers that are otherwise permitted when using wildcards in the "Allow Delegating Saved Credentials" server list.
Computer/User	Cursors	Turn off pen feedback	At least Windows Vista or later	Disables visual pen action feedback, except for press and hold feedback. If you enable this policy, all visual pen action feedback is disabled except for press and hold feedback. Additionally, the mouse cursors are shown instead of the pen cursors. If you disable or do not configure this policy, visual feedback and pen cursors will be shown unless the user disables them in Control Panel.
Computer	DC Locator DNS Records	Domain Controller Address Type Returned	At least Windows Vista or later	The Domain Controller (DC) Locator APIs return IP address of the DC with the other part of the information. Before the support of IPv6, the returned DC IP address was IPv4. But with the support of IPv6, the DC Locator APIs can return IPv6 DC address. The returned IPv6 DC address may not be correctly handled by some of the existing applications. So this policy is provided to support such scenarios. By default, DC Locator APIs can return IPv4/IPv6 DC address. But if some applications are broken due to the returned IPv6 DC address, this policy can be used to disable the default behavior and enforce to return ONLY IPv4 DC address. Once applications are fixed, this policy can be used to enable the default behavior. If you enable this policy setting, DC Locator APIs can return IPv4/IPv6 DC address. This is the default behavior of the DC Locator. If you disable this policy setting, DC Locator APIs will ONLY return IPv4 DC address if any. So if the domain controller supports both IPv4 and IPv6 addresses, DC Locator APIs will return IPv4 address. But if the domain controller supports only IPv6 address, then DC Locator APIs will fail. If you do not configure this policy setting, DC Locator APIs can return IPv4/IPv6 DC address. This is the default behavior of the DC

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Locator.
Computer	DC Locator DNS Records	Force Rediscovery Interval	At least Windows Vista or later	The Domain Controller Locator (DC Locator) service is used by clients to find domain controllers for their Active Directory domain. When DC Locator finds a domain controller, it caches domain controllers to improve the efficiency of the location algorithm. As long as the cached domain controller meets the requirements and is running, DC Locator will continue to return it. If a new domain controller is introduced, existing clients will only discover it when a Force Rediscovery is carried out by DC Locator. To adapt to changes in network conditions DC Locator will by default carry out a Force Rediscovery according to a specific time interval and maintain efficient load-balancing of clients across all available domain controllers in all domains or forests. The default time interval for Force Rediscovery by DC Locator is 12 hours. Force Rediscovery can also be triggered if a call to DC Locator uses the DS_FORCE_REDISCOVERY flag. Rediscovery resets the timer on the cached domain controller entries. If you enable this policy setting, DC Locator on the machine will carry out Force Rediscovery periodically according to the configured time interval. The minimum time interval is 3600 seconds (1 hour) to avoid excessive network traffic from rediscovery. The maximum allowed time interval is 4294967200 seconds, while any value greater than 4294967 seconds (~49 days) will be treated as infinity. If you disable this policy setting, Force Rediscovery will be used by default for the machine at every 12 hour interval. If you do not configure this policy setting, Force Rediscovery will be used by default for the machine at every 12 hour interval, unless the local machine setting in the registry is a different value.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	DC Locator DNS Records	Try Next Closest Site	At least Windows Vista or later	The Domain Controller Locator (DC Locator) service is used by clients to find domain controllers for their Active Directory domain. The default behavior for DC Locator is to find a DC in the same site. If none are found in the same site, a DC in another site, which might be several site-hops away, could be returned by DC Locator. Site proximity between two sites is determined by the total site-link cost between them. A site is closer if it has a lower site link cost than another site with a higher site link cost. The Try Next Closest Site feature enables DC Locator to attempt to locate a DC in the nearest site based on the site link cost if a DC in same the site is not found. In scenarios with multiple sites, failing over to the try next closest site during DC Location streamlines network traffic more effectively. If you enable this policy setting, Try Next Closest Site DC Location will be turned on for the machine across all available but un-configured network adapters. If you disable this policy setting, Try Next Closest Site DC Location will not be used by default for the machine across all available but un-configured network adapters. However, if a DC Locator call is made using the DS_TRY_NEXTCLOSEST_SITE flag explicitly, the Try Next Closest Site behavior is honored. If you do not configure this policy setting, Try Next Closest Site DC Location will not be used by default for the machine across all available but un-configured network adapters. If the DS_TRY_NEXTCLOSEST_SITE flag is used explicitly, the Next Closest Site behavior will be used.
User	Desktop	Desktop Wallpaper	At least Windows Vista or later	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

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				stored in a bitmap (*.bmp) or JPEG (*.jpg) 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: This setting does not apply to Terminal Server sessions.
Computer/User	Desktop Window Manager	Do not allow desktop composition	At least Windows Vista or later	This policy setting controls how some graphics are rendered and facilitates other features, including Flip, Flip3D, and Taskbar Thumbnails. If you enable this setting, the desktop compositor visual experience will be turned off. If you disable or do not configure this policy setting, desktop composition will be turned on, if the required hardware is in place.
Computer/User	Desktop Window Manager	Do not allow Flip3D invocation	At least Windows Vista or later	Flip3D is a 3D window switcher. If you enable this setting, Flip3D will be inaccessible. If you disable or do not configure this policy setting, Flip3D will be accessible, if desktop composition is turned on.
Computer/User	Desktop Window Manager	Do not allow window animations	At least Windows Vista or later	This policy setting controls the appearance of window animations such as those found when restoring, minimizing, and maximizing windows. If you enable this setting, window animations will be turned off. If you disable or do not configure

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this setting, window animations will be turned on.
Computer	Device and Resource Redirection	Do not allow supported Plug and Play device redirection	At least Windows Vista or later	This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Terminal Services session. By default, Terminal Services allows redirection of supported Plug and Play devices. Users can use the ΓÇ£MoreΓÇ¥ option on the Local Resources tab of Remote Desktop Connection to choose the supported Plug and Play devices to redirect to the remote computer. If you enable this policy setting, users cannot redirect their supported Plug and Play devices to the remote computer. If you disable this policy setting or do not configure this policy setting, users can redirect their supported Plug and Play devices to the remote computer. Note: You can also disallow redirection of supported Plug and Play devices on the Client Settings tab in the Terminal Services Configuration tool. You can disallow redirection of specific types of supported Plug and Play devices by using the ΓÇ£Computer Configuration\Administrative Templates\System\Device Installation\Device Installation RestrictionsΓÇ¥ policy settings.
Computer	Device Installation	Allow remote access to the PnP interface	At least Windows Vista or later	Specifies whether or not remote access to the Plug and Play interface is allowed. If you enable this setting, remote connections to the PnP interface will be allowed. If you disable or do not configure this setting, PnP interface will not be available remotely.
Computer	Device Installation	Configure device installation timeout	At least Windows Vista or later	Specifies the number of seconds the system will wait for a device installation task to complete. If the task is not complete within the specified number of seconds, the system will terminate the installation. If you enable this setting, the system will wait for the number of seconds specified before forcibly terminating the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				installation. If you disable or do not configure this setting, the system will wait 300 seconds (5 minutes) for any device installation task to complete before terminating installation.
Computer/User	Device Installation	Do not create system restore point when new device driver installed	At least Windows Vista or later	Specifies whether or not a system restore point is created when a new device driver is installed on your machine. If you enable this setting, system restore points will not be created when a new device driver is installed or updated. If you disable or do not configure this setting, a system restore point will be created whenever a new driver is installed or an existing device driver is updated.
Computer	Device Installation	Do not send a Windows Error Report when a generic driver is installed on a device	At least Windows Vista or later	Specifies whether or not to send a Windows Error Report when a generic driver is installed on a device. If you enable this setting, a Windows Error Report will not be sent when a generic driver is installed. If you disable or do not configure this setting, a Windows Error Report will be sent when a generic driver is installed.
Computer	Device Installation	Treat all digitally signed drivers equally in the driver ranking and selection process	At least Windows Vista or later	When selecting which driver to install, do not distinguish between drivers that are signed by a Microsoft Windows Publisher certificate and drivers that are signed by others. If you enable this setting, all valid Authenticode signatures are treated equally for the purpose of selecting a device driver to install. Selection is based on other criteria (such as version number or when the driver was created) rather than whether the driver was signed by a Microsoft Windows Publisher certificate or by another Authenticode certificate. A signed driver is still preferred over a driver that is not signed at all. However, drivers that are signed by Microsoft Windows Publisher certificates are not preferred over drivers signed by other Authenticode certificates. If you disable or do not configure this setting, drivers that are signed by a Microsoft Windows Publisher certificate are selected for installation over

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				drivers that are signed by other Authenticode certificates.
Computer	Device Installation	Turn off "Found New Hardware" balloons during device installation	At least Windows Vista or later	Do not display "Found New Hardware" balloons during device installation. If you enable this setting, "Found New Hardware" balloons will not appear while a device is being installed. If you disable or do not configure this setting, "Found New Hardware" balloons will appear while a device is being installed unless the driver for the device has suppressed the balloons.
Computer	Device Installation Restrictions	Allow administrators to override Device Installation Restriction policies	At least Windows Vista or later	Allows members of the Administrators group to install and update the drivers for any device, regardless of other policy settings. If you enable this setting, administrators can use "Add Hardware Wizard" or "Update Driver Wizard" to install and update the drivers for any device. If you disable or do not configure this setting, administrators are subject to all policies that restrict device installation. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Allow installation of devices that match any of these device IDs	At least Windows Vista or later	Specifies a list of Plug and Play hardware IDs and compatible IDs that describe devices that can be installed. This setting is intended to be used only when the "Prevent installation of devices not described by other policy settings" setting is enabled and does not take precedence over any policy setting that would prevent a device from being installed. If you enable this setting, any device with a hardware ID or compatible ID that matches an ID in this list can be installed or updated, if that installation has not been specifically prevented by the "Prevent installation of devices that match these device IDs," "Prevent installation of devices for these device classes," or "Prevent installation of removable devices"

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				policy setting. If another policy setting prevents a device from being installed, the device cannot be installed even if it is also described by a value in this policy setting. If you disable or do not configure this setting and no other policy describes the device, the "Prevent installation of devices not described by other policy settings" setting determines whether the device can be installed. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Allow installation of devices using drivers that match these device setup classes	At least Windows Vista or later	Specifies a list of device setup class GUIDs describing devices that can be installed. This setting is intended to be used only when the "Prevent installation of devices not described by other policy settings" setting is enabled and does not have precedence over any setting that would prevent a device from being installed. If you enable this setting, any device with a hardware ID or compatible ID that matches one of the IDs in this list can be installed or updated, if that installation has not been specifically prevented by the "Prevent installation of devices that match these device IDs," "Prevent installation of devices for these device classes," or "Prevent installation of removable devices" policy setting. If another policy setting prevents a device from being installed, the device cannot be installed even if it is also described by a value in this setting. If you disable or do not configure this setting and no other policy describes the device, the "Prevent installation of devices not described by other policy settings" setting determines whether the device can be installed. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Device Installation Restrictions	Display a custom message when installation is prevented by policy (balloon text)	At least Windows Vista or later	Specifies a custom message that is displayed to the user in the text of the notification balloon when policy prevents the installation of a device. If you enable this setting, then this text is displayed as the main body text of the message displayed by Windows whenever device installation is prevented by policy. If you disable or do not configure this setting, then Windows displays a default message whenever device installation is prevented by policy.
Computer	Device Installation Restrictions	Display a custom message when installation is prevented by policy (balloon title)	At least Windows Vista or later	Specifies a custom message that is displayed to the user in the title of the notification balloon when policy prevents the installation of a device. If you enable this setting, then this text is displayed as the title text of the message displayed by Windows whenever device installation is prevented by policy. If you disable or do not configure this setting, then Windows displays a default title whenever device installation is prevented by policy.
Computer	Device Installation Restrictions	Prevent installation of devices not described by other policy settings	At least Windows Vista or later	This setting controls the installation policy for devices that are not specifically described by any other policy. If you enable this setting, any device that is not described by either the "Allow installation of devices that match these device IDs" or "Allow installation of devices for these device classes" cannot be installed or have its driver updated. If you disable or do not configure this setting, any device that is not described by the "Prevent installation of devices that match these device IDs," "Prevent installation of devices for these device classes," or "Deny installation of removable devices" policies can be installed and have its driver updated. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Device Installation Restrictions	Prevent installation of devices that match any of these device IDs	At least Windows Vista or later	Specifies a list of Plug and Play hardware IDs and compatible IDs for devices that cannot be installed. If you enable this setting, a device cannot be installed or updated if its hardware ID or compatible ID matches one in this list. If you disable or do not configure this setting, new devices can be installed and existing devices can be updated, as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer	Device Installation Restrictions	Prevent installation of devices using drivers that match these device setup classes	At least Windows Vista or later	Specifies a list of Plug and Play device setup class GUIDs for devices that cannot be installed. If you enable this setting, new devices cannot be installed and existing devices cannot be updated if they use drivers that belong to any of the listed device setup classes. If you disable or do not configure this setting, new devices can be installed and existing devices can be updated as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer	Device Installation Restrictions	Prevent installation of removable devices	At least Windows Vista or later	Prevents removable devices from being installed. If you enable this setting, removable devices may not be installed, and existing removable devices cannot have their drivers updated. If you disable or do not configure this setting, removable devices can be installed and existing removable devices can be updated as permitted by other policy settings for device installation. NOTE: This policy setting takes precedence over any other policy settings that allow a device to be installed. If this policy setting prevents a device from being installed, the device cannot be installed or updated, even if it matches another policy setting that would allow installation of that device. For this policy, a device is considered to be removable when the drivers for the device to which it is connected indicate that the device is removable. For example, a Universal Serial Bus (USB) device is reported to be removable by the drivers for the USB hub to which the device is connected. If this computer is a Terminal Server, then enabling this policy also affects redirection of the specified devices from a Terminal Services Client to this computer.
Computer/User	Digital Locker	Do not allow Digital Locker to run	At least Windows Vista or later	Specifies whether Digital Locker can run. Digital Locker is a dedicated download manager associated with Windows Marketplace and a feature of Windows that can be used to manage and download products acquired and stored in the user's Windows Marketplace Digital Locker. If you enable this setting, Digital Locker will not run. If you disable or do not configure this setting, Digital Locker can be run.
Computer	Disk Diagnostic	Disk Diagnostic: Configure custom alert text	At least Windows Vista or later	Substitutes custom alert text in the disk diagnostic message shown to users when a disk reports a S.M.A.R.T. fault. If you enable this policy setting, Windows will display custom alert text in the disk diagnostic message. The custom text may not

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				exceed 512 characters. nIf you disable or do not configure this policy setting, Windows will display the default alert text in the disk diagnostic message. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect if the Disk Diagnostic scenario policy is enabled or not configured and the Diagnostic Policy Service (DPS) is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Disk Diagnostic	Disk Diagnostic: Configure execution level	At least Windows Vista or later	Determines the execution level for S.M.A.R.T.-based disk diagnostics. Self-Monitoring And Reporting Technology (S.M.A.R.T.) is a standard mechanism for storage devices to report faults to Windows. A disk that reports a S.M.A.R.T. fault may need to be repaired or replaced. The Diagnostic Policy Service (DPS) will detect and log S.M.A.R.T. faults to the event log when they occur. If you enable this policy setting, the DPS will also warn users of S.M.A.R.T. faults and guide them through backup and recovery to minimize potential data loss. If you disable this policy, S.M.A.R.T. faults will still be detected and logged, but no corrective action will be taken. If you do not configure this policy setting, the DPS will enable S.M.A.R.T. fault resolution by default. This policy setting takes effect only if the diagnostics-wide scenario execution policy is not configured. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Services snap-in to the Microsoft Management Console.
Computer	Disk NV Cache	Turn Off Boot and Resume Optimizations	At least Windows Vista or later	Turns off the boot and resume optimizations for the hybrid hard disks in the system. If you enable this policy setting, the system does not use the non-volatile (NV) cache to optimize boot and resume. If you disable this policy setting, the system uses the NV cache to achieve faster boot and resume. The system determines the data that will be stored in the NV cache to optimize boot and resume. The required data is stored in the NV cache during shutdown and hibernate respectively. This might cause a slight increase in the time taken for shutdown and hibernate. If you do not configure this policy, the default behavior is observed and the NV cache is used for boot and resume optimizations. NOTE: This policy is applicable only if the NV Cache Feature is on.
Computer	Disk NV Cache	Turn Off Cache Power Mode	At least Windows Vista or later	Turns off the power save mode on the hybrid hard disks in the system. If you enable this policy, the disks will not be put into NV cache power save mode and no power savings would be achieved. If you disable this policy setting, then the hard disks are put into a NV cache power saving mode. In this mode, the system tries to save power by aggressively spinning down the disk. If you do not configure this policy setting, the default behavior is to allow the hybrid hard disks to be in power save mode. NOTE: This policy is applicable only if the NV Cache feature is on.
Computer	Disk NV Cache	Turn Off Non Volatile Cache Feature	At least Windows Vista or later	Turns off all support for the non-volatile (NV) cache on all hybrid hard disks in the system. To check if you have hybrid hard disks in the system, from the device manager, right click the disk drive and select Properties. The NV cache can be used to optimize boot and resume by reading data from the cache while the disks

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				are spinning up. The NV cache can also be used to reduce the power consumption of the system by keeping the disks spun down while satisfying reads and writes from the cache. If you enable this policy setting, the system will not manage the NV cache and will not enable NV cache power saving mode. If you disable this policy setting, the system will manage the NV cache on the disks provided the other policy settings for the NV cache are appropriately configured. NOTE: This setting will take effect on next boot. If you do not configure this policy, the default behavior is to turn on support for the NV cache.
Computer	Disk NV Cache	Turn Off Solid State Mode	At least Windows Vista or later	Turns off the solid state mode for the hybrid hard disks. If you enable this policy setting, frequently written files such as the file system metadata and registry may not be stored in the NV cache. If you disable this policy setting, the system will store frequently written data into the non-volatile (NV) cache. This allows the system to exclusively run out of the NV cache and power down the disk for longer periods to save power. Note that this can cause increased wear of the NV cache. If you do not configure this policy, the default behavior of the system is observed and frequently written files will be stored in the NV cache. NOTE: This policy is applicable only if the NV Cache Feature is on.
Computer	DNS Client	Allow DNS Suffix Appending to Unqualified Multi-Label Name Queries	At least Windows Vista or later	Specifies whether the computers to which this setting is applied may attach suffixes to an unqualified multi-label name before sending subsequent DNS queries, if the original name query fails. A name containing dots, but not dot-terminated, is called an unqualified multi-label name, for example "server.corp". A fully qualified name would have a terminating dot, for example "server.corp.contoso.com.". If you enable this setting, suffixes are allowed to be

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				appended to an unqualified multi-label name, if the original name query fails. For example, an unqualified multi-label name query for "server.corp" will be queried by the DNS Client first. If the query succeeds, the response is returned to the client. If the query fails, the unqualified multi-label name is appended with DNS Suffixes configured for the computer for queries. These suffixes can be derived from a combination of the local DNS Client's primary domain suffix, a connection-specific domain suffix and/or DNS Suffix Search List. For example, if the local DNS Client receives a query for "server.corp", and a primary domain suffix is configured as "contoso.com", with this setting the DNS Client will send a query for "server.corp.contoso.com." if the original name query for "server.corp" fails. If you disable this setting, no suffixes are appended to unqualified multi-label name queries if the original name query fails. If you do not configure this setting, computers will use their local DNS Client configuration to determine the query behavior for unqualified multi-label names.
Computer	DNS Client	Turn off Multicast Name Resolution	At least Windows Vista or later	Local Link Multicast Name Resolution (LLMNR) is a secondary name resolution protocol. Queries are sent over the Local Link, a single subnet, from a client machine using Multicast to which another client on the same link, which also has LLMNR enabled, can respond. LLMNR provides name resolution in scenarios in which conventional DNS name resolution is not possible. If you enable this policy setting, Multicast name resolution or LLMNR, will be turned off for the machine across all available but un-configured network adapters. If you disable this policy setting, Multicast name resolution or LLMNR, will be turned on for the machine across all available but un-configured network adapters. If you do not configure

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this policy setting, Multicast name resolution or LLMNR, will be turned on for the machine across all available but un-configured network adapters by default.
Computer	Driver Installation	Allow non-administrators to install drivers for these device setup classes	At least Windows Vista or later	Specifies a list of device setup class GUIDs describing device drivers that non-administrator members of the built-in Users group may install on the system. If you enable this setting, members of the Users group may install new drivers for the specified device setup classes. The drivers must be signed according to Windows Driver Signing Policy, or be signed by publishers already in the TrustedPublisher store. If you disable or do not configure this setting, only members of the Administrators group are allowed to install new device drivers on the system.
User	Explorer Frame Pane	Turn off Details Pane	At least Windows Vista or later	Hides the Details Pane in Windows Explorer. If you enable this policy setting, the Details Pane in Windows Explorer is hidden and cannot be turned on by the user. If you disable, or do not configure this setting, the Details Pane is displayed by default and can be hidden by the user.
User	Explorer Frame Pane	Turn off Preview Pane	At least Windows Vista or later	Hides the Preview Pane in Windows Explorer. If you enable this policy setting, the Preview Pane in Windows Explorer is hidden and cannot be turned on by the user. If you disable, or do not configure this setting, the Preview Pane is displayed by default and can be hidden by the user.
Computer/User	Folder Redirection	Use localized subfolder names when redirecting Start and My Documents	At least Windows Vista or later	This policy setting allows the administrator to define whether Folder Redirection should use localized names for the All Programs, Startup, My Music, My Pictures, and My Videos subfolders when redirecting the parent Start menu and legacy My Documents folder respectively. If you enable this policy setting, Windows Vista will use localized folder names for these subfolders when redirecting the Start

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Menu or legacy My Documents folder. If you disable or not configure this policy setting, Windows Vista will use the standard English names for these subfolders when redirecting the Start Menu or legacy My Documents folder. Note: This policy is valid only on Windows Vista when it processes a legacy redirection policy already deployed for these folders in your existing localized environment.
Computer	Game Explorer	Turn off downloading of game information	At least Windows Vista or later	Manages download of game box art and ratings from the Windows Metadata Services. If you enable this setting, game information including box art and ratings will not be downloaded. If you disable or do not configure this setting, game information will be downloaded from Windows Metadata Services.
Computer	Game Explorer	Turn off tracking of last play time of games in the Games folder	At least Windows Vista or later	Tracks the last play time of games in the Games folder. If you enable this setting the last played time of games will not be recorded in Games folder. This setting only affects the Games folder. If you disable or do not configure this setting, the last played time will be displayed to the user.
Computer	General iSCSI	Do not allow additional session logins	At least Windows Vista or later	If enabled then only those sessions that are established via a persistent login will be established and no new persistent logins may be created. If disabled then additional persistent and non persistent logins may be established.
Computer	General iSCSI	Do not allow changes to initiator iqn name	At least Windows Vista or later	If enabled then do not allow the initiator iqn name to be changed. If disabled then the initiator iqn name may be changed.
Computer	Group Policy	Startup policy processing wait time	At least Windows Vista or later	This policy setting specifies how long Group Policy should wait for network availability notifications during startup policy processing. If the startup policy processing is synchronous, the computer is blocked until the network is available or the default wait time is reached. If the startup policy processing is asynchronous, the computer is not blocked and policy processing will occur in the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				background. In either case, configuring this policy setting overrides any system-computed wait times. If you enable this policy setting, Group Policy will use this administratively configured maximum wait time and override any default or system-computed wait time. If you disable or do not configure this policy setting, Group Policy will use the default wait time of 30 seconds on computers running the Microsoft Windows Vista operating system.
Computer	Group Policy	Turn off Local Group Policy objects processing	At least Windows Vista or later	This policy setting prevents Local Group Policy objects (Local GPOs) from being applied. By default, the policy settings in Local GPOs are applied before any domain-based GPO policy settings. These policy settings can apply to both users and the local computer. You can disable the processing and application of all Local GPOs to ensure that only domain-based GPOs are applied. If you enable this policy setting, the system will not process and apply any Local GPOs. If you disable or do not configure this policy setting, Local GPOs will continue to be applied. Note: For computers joined to a domain, it is strongly recommended that you only configure this policy setting in domain-based GPOs. This setting will be ignored on computers that are joined to a workgroup.
User	Group Policy snap-in extensions	Windows Firewall with Advanced Security	At least Windows Vista or later	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	Final Subnode	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	Group Policy snap-in extensions, mmc	**NAP Client Configuration**	At least Windows Vista or later	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.
Computer/User	Handwriting personalization	Turn off automatic learning	At least Windows Vista or later	Turns off the automatic learning component of handwriting recognition personalization. Automatic learning enables the collection and storage of text

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				and/or ink written by the user in order to help adapt handwriting recognition to the vocabulary and handwriting style of the user. Text that is collected includes all outgoing messages in Windows Mail, and MAPI enabled e-mail clients, plus URLs from the Internet Explorer browser history. The information that is stored includes word frequency and new words not already known to the handwriting recognition engines (for example proper names and acronyms). Deleting e-mail content or the browser history will not delete the stored personalization data. Ink entered through Input Panel is collected and stored. Note: Automatic learning of both text and ink might not be available for all languages, even when handwriting personalization is available. See Tablet PC Help for more information. If you enable this policy, automatic learning stops and any stored data is deleted. Users will not be able to configure this setting in Control Panel. If you disable this policy, automatic learning is turned on. Users will not be able to configure this setting in Control Panel. Collected data is only used for handwriting recognition if handwriting personalization is turned on. If you do not configure this policy, users can choose to enable or disable automatic learning either from the Handwriting tab in the Tablet Settings in Control Panel or from the opt-in dialog. Related to ΓÇ£Turn off handwriting personalizationΓÇ¥ policy. Note: The amount of stored ink is limited to 50 MB and the amount of text information to about 5 MB. When these limits are reached and new data is collected, old data is deleted to make room for more recent data. Note: Handwriting personalization in Microsoft Windows VistaΓäó works only for Microsoft handwriting recognizers, not with third-party recognizers.
Computer/User	Handwriting	Turn off handwriting	At least Windows Vista or later	Turns off handwriting recognition personalization so the handwriting recognition

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
	personalization	personalization		engine that ships with Windows VistaΓäó is used instead of the personalized handwriting recognizer. Handwriting personalization allows the handwriting recognizer to adapt to the writing style and vocabulary of a user by using automatic learning and the handwriting recognition personalization tool. Handwriting personalization is not available for all languages that have handwriting recognition. See Tablet PC Help for more information. If you enable this policy, handwriting personalization is turned off. The handwriting recognition that ships with Windows VistaΓäó is used. The information collected for handwriting personalization is not deleted, but it will not be used for handwriting recognition. Users will not be able to configure this setting in Control Panel. If you disable this policy, handwriting personalization is turned on. Users will not be able to configure this setting in Control Panel. If you do not configure this policy, handwriting personalization is turned on. Users will be able to configure this setting on the Handwriting tab of Tablet Settings, in Control Panel. Related to ΓÇ£Turn off automatic learningΓÇ¥ policy. Note: Handwriting personalization in Microsoft Windows VistaΓäó works only for Microsoft handwriting recognizers, not with third-party recognizers.
Computer	Hard Disk Settings	Turn Off the Hard Disk (On Battery)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the hard disk. If you enable this policy, you must provide a value, in seconds, indicating how much idle time should elapse before Windows turns off the hard disk. If you disable this policy or do not configure it, users can see and change this setting.
Computer	Hard Disk Settings	Turn Off the Hard Disk (Plugged In)	At least Windows Vista or later	Specifies the period of inactivity before Windows turns off the hard disk. If you enable this policy, you must provide a value, in seconds, indicating how much idle

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				time should elapse before Windows turns off the hard disk. If you disable this policy or do not configure it, users can see and change this setting.
Computer/User	Hardware Buttons	Prevent Back-ESC mapping	At least Windows Vista or later	Removes the Back-&gt;ESC mapping that normally occurs when menus are visible, and for applications that subscribe to this behavior. If you enable this policy, a button assigned to Back will not map to ESC. If you disable this policy, Back-&gt;ESC mapping will occur. If you do not configure this policy, Back-&gt;ESC mapping will occur.
Computer/User	Hardware Buttons	Prevent launch an application	At least Windows Vista or later	Prevents the user from launching an application from a Tablet PC hardware button. If you enable this policy, applications cannot be launched from a hardware button, and "Launch an application" is removed from the drop down menu for configuring button actions (in the Tablet PC Control Panel buttons tab). If you disable this policy, applications can be launched from a hardware button. If you do not configure this policy, applications can be launched from a hardware button.
Computer/User	Hardware Buttons	Prevent press and hold	At least Windows Vista or later	Prevents press and hold actions on hardware buttons, so that only one action is available per button. If you enable this policy, press and hold actions are unavailable, and the button configuration dialog will display the following text: "Some settings are controlled by Group Policy. If a setting is unavailable, contact your system administrator." If you disable this policy, press and hold actions for buttons will be available. If you do not configure this policy, press and hold actions will be available.
Computer/User	Hardware Buttons	Turn off hardware buttons	At least Windows Vista or later	Turns off Tablet PC hardware buttons. If you enable this policy, no actions will occur when the buttons are pressed, and the buttons tab in Tablet PC Control Panel will be removed. If you disable this policy, user and OEM defined button

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				actions will occur when the buttons are pressed. If you do not configure this policy, user and OEM defined button actions will occur when the buttons are pressed.
Computer/User	Import Video	Do not allow Import Video to run	At least Windows Vista or later	Specifies whether Import Video can run. Import Video is a feature of Windows Vista that can be used to import video from a digital video device where the video is encoded and saved as a video file on your computer. If you enable this setting, Import Video will not run. If you disable or do not configure this setting, Import Video can be run.
Computer/User	Input Panel	For tablet pen input, donΓÇÖt show the Input Panel icon	At least Windows Vista or later	Prevents the Tablet PC Input Panel icon from appearing next to any text entry area in applications where this behavior is available. This policy applies only when using a tablet pen as an input device. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel will never appear next to text entry areas when using a tablet pen as an input device. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel will appear next to any text entry area in applications where this behavior is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will be able to configure this setting on the Opening tab in Input Panel Options. Caution: If you enable both the ΓÇ£Prevent Input Panel from appearing next to text entry areasΓÇ¥ policy and the ΓÇ£Prevent Input Panel tab from appearingΓÇ¥ policy, and disable the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				ΓÇ£Show Input Panel taskbar iconΓÇ¥ policy, the user will then have no way to access Input Panel.
Computer/User	Input Panel	For touch input, donΓÇÖt show the Input Panel icon	At least Windows Vista or later	Prevents the Tablet PC Input Panel icon from appearing next to any text entry area in applications where this behavior is available. This policy applies only when a user is using touch input. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel will never appear next to any text entry area when a user is using touch input. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel will appear next to text entry areas in applications where this behavior is available. Users will be able to configure this setting on the Opening tab in Input Panel Options.
Computer/User	Input Panel	Include rarely used Chinese, Kanji, or Hanja characters	At least Windows Vista or later	Includes rarely used Chinese, Kanji, and Hanja characters when handwriting is converted to typed text. This policy applies only to the use of the Microsoft recognizers for Chinese (Simplified), Chinese (Traditional), Japanese, and Korean. This setting appears in Input Panel Options only when these input languages or keyboards are installed. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, rarely used Chinese, Kanji, and Hanja characters will be included in recognition results

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				when handwriting is converted to typed text. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, rarely used Chinese, Kanji, and Hanja characters will not be included in recognition results when handwriting is converted to typed text. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, rarely used Chinese, Kanji, and Hanja characters will not be included in recognition results when handwriting is converted to typed text. Users will be able to configure this setting on the Advanced tab in the Input Panel Options dialog box.
Computer/User	Input Panel	Prevent Input Panel tab from appearing	At least Windows Vista or later	Prevents Input Panel tab from appearing on the edge of the Tablet PC screen. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, Input Panel tab will not appear on the edge of the Tablet PC screen. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, Input Panel tab will appear on the edge of the Tablet PC screen. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, Input Panel tab will appear on the edge of the Tablet PC screen. Users will be able to configure this setting on the Opening tab in Input Panel Options. Caution: If you enable both the ΓÇ£Prevent Input Panel from appearing next to text entry areasΓÇ¥ policy and the ΓÇ£Prevent Input Panel tab from appearingΓÇ¥ policy, and disable the ΓÇ£Show Input Panel taskbar iconΓÇ¥ policy, the user will then have no way to access Input Panel.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Input Panel	Switch to the Simplified Chinese (PRC) gestures	At least Windows Vista or later	Switches the gesture set used for editing from the common handheld computer gestures to the Simplified Chinese (PRC) standard gestures. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, the Simplified Chinese (PRC) editing gestures will be used. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, the common handheld editing gesture set will be used. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, the common handheld editing gesture set will be used. Users will be able to configure this setting on the Gestures tab in Input Panel Options.
Computer/User	Input Panel	Turn off AutoComplete integration with Input Panel	At least Windows Vista or later	Turns off the integration of application auto complete lists with Tablet PC Input Panel in applications where this behavior is available. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy, application auto complete lists will never appear next to Input Panel. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, application auto complete lists will appear next to Input Panel in applications where the functionality is available. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, application auto complete lists will appear next to Input Panel in applications where the functionality is available. Users will be able to configure this setting on the Settings tab in Input Panel Options.

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
Computer/User	Input Panel	Turn off password security in Input Panel	At least Windows Vista or later	Adjusts password security settings in Tablet PC Input Panel. These settings include using the on-screen keyboard by default, preventing users from switching to another Input Panel skin (the writing pad or character pad), and not showing what keys are tapped when entering a password. Tablet PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy and choose ΓÇ£LowΓÇ¥ from the drop-down box, password security is set to ΓÇ£Low.ΓÇ¥ At this setting, all password security settings are turned off. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£Medium-LowΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium-Low.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel displays the cursor and which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£MediumΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is not allowed, and Input Panel displays the cursor and which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose to ΓÇ£Medium-HighΓÇ¥ from the drop-down box, password security is set to ΓÇ£Medium-High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£HighΓÇ¥ from the drop-down box, password security is set to ΓÇ£High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is not allowed, and Input Panel does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, password security is set to ΓÇ£Medium-High.ΓÇ¥ At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel does not display the cursor or which keys are tapped. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, password security is set to ΓÇ£Medium-HighΓÇ¥ by default. At this setting, when users enter passwords from Input Panel they use the on-screen keyboard by default, skin switching is allowed, and Input Panel does not display the cursor or which keys are tapped. Users will be able to configure this setting on the Advanced tab in Input Panel Options. Caution: If you lower password security settings, people who can see the userΓÇÖs screen might be able to see their passwords.
Computer/User	Input Panel	Turn off tolerant and Z-shaped scratch-out gestures	At least Windows Vista or later	Turns off both the more tolerant scratch-out gestures that were added in Windows Vista and the Z-shaped scratch-out gesture that was available in Microsoft Windows XP Tablet PC Edition. The tolerant gestures let users scratch out ink in Input Panel by using strikethrough and other scratch-out gesture shapes. Tablet

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				PC Input Panel is a Tablet PC accessory that enables you to use handwriting or an on-screen keyboard to enter text, symbols, numbers, or keyboard shortcuts. If you enable this policy and choose ΓÇ£AllΓÇ¥ from the drop-down menu, no scratch-out gestures will be available in Input Panel. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£Tolerant," users will be able to use the Z-shaped scratch-out gesture that was available in Microsoft Windows XP Tablet PC Edition. Users will not be able to configure this setting in the Input Panel Options dialog box. If you enable this policy and choose ΓÇ£None,ΓÇ¥ users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will not be able to configure this setting in the Input Panel Options dialog box. If you disable this policy, users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will not be able to configure this setting in the Input Panel Options dialog box. If you do not configure this policy, users will be able to use both the tolerant scratch-out gestures and the Z-shaped scratch-out gesture. Users will be able to configure this setting on the Gestures tab in Input Panel Options.
User	Instant Search	Custom Instant Search Internet search provider	At least Windows Vista or later	Set up the menu name and URL for the custom Internet search provider. If you enable this setting, the specified menu name and URL will be used for Internet searches. If you disable or not configure this setting, the default Internet search provider will be used.
Computer/User	Internet Communication settings	Turn off handwriting recognition error reporting	At least Windows Vista or later	Turns off the handwriting recognition error reporting tool. The handwriting recognition error reporting tool enables users to report errors encountered in

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows. If you enable this policy, users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft. If you disable this policy, Tablet PC users can report handwriting recognition errors to Microsoft. If you do not configure this policy Tablet PC users can report handwriting recognition errors to Microsoft.
User	Internet Communication settings	Turn off Help Experience Improvement Program	At least Windows Vista or later	Specifies whether users can participate in the Help Experience Improvement program. The Help Experience Improvement program collects information about how customers use Windows Help so that Microsoft can improve it. If this setting is enabled, this policy prevents users from participating in the Help Experience Improvement program. If this setting is disabled or not configured, users will be able to turn on the Help Experience Improvement program feature from the Help and Support settings page.
User	Internet Communication settings	Turn off Help Ratings	At least Windows Vista or later	Specifies whether users can provide ratings for Help content. If this setting is enabled, this policy setting prevents ratings controls from being added to Help content. If this setting is disabled or not configured, a rating control will be added to Help topics. Users can use the control to provide feedback on the quality and usefulness of the Help and Support content.
Computer/User	Internet Communication settings	Turn off Windows Movie Maker online Web links	At least Windows Vista or later	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. The "Windows Movie Maker on the Web" command lets users go directly to the Windows Movie Maker

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				Web site to get more information, and the "Privacy Statement" command lets users view information about privacy issues in respect to Windows Movie Maker. 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	Internet Communication settings	Turn off Windows Online	At least Windows Vista or later	Specifies whether users can search and view content from Windows Online in Help and Support. Windows Online provides the most up-to-date Help content for Windows. If this settings is enabled, users will be prevented from accessing online assistance content from Windows Online. If this setting is disabled or not configured, users will be able to access online assistance if they have a connection to the Internet and have not disabled Windows Online from the Help and Support Options page.
Computer	iSCSI Security	Do not allow changes to initiator CHAP secret	At least Windows Vista or later	If enabled then do not allow the initiator CHAP secret to be changed. If disabled then the initiator CHAP secret may be changed.
Computer	iSCSI Security	Do not allow connections without IPSec	At least Windows Vista or later	If enabled then only those connections that are configured for IPSec may be established. If disabled then connections that are configured for IPSec or connections not configured for IPSec may be established.
Computer	iSCSI Security	Do not allow sessions without mutual CHAP	At least Windows Vista or later	If enabled then only those sessions that are configured for mutual CHAP may be established. If disabled then sessions that are configured for mutual CHAP or sessions not configured for mutual CHAP may be established.
Computer	iSCSI Security	Do not allow sessions without one way CHAP	At least Windows Vista or later	If enabled then only those sessions that are configured for one-way CHAP may be established. If disabled then sessions that are configured for one-way CHAP or

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				sessions not configured for one-way CHAP may be established. Note that if the "Do not allow sessions without mutual CHAP" setting is enabled then that setting overrides this one.
Computer	iSCSI Target Discovery	Do not allow adding new targets via manual configuration	At least Windows Vista or later	If enabled then new targets may not be manually configured by entering the target name and target portal; already discovered targets may be manually configured. If disabled then new and already discovered targets may be manually configured. Note: if enabled there may be cases where this will break VDS.
Computer	iSCSI Target Discovery	Do not allow manual configuration of discovered targets	At least Windows Vista or later	If enabled then discovered targets may not be manually configured. If disabled then discovered targets may be manually configured. Note: if enabled there may be cases where this will break VDS.
Computer	iSCSI Target Discovery	Do not allow manual configuration of iSNS servers	At least Windows Vista or later	If enabled then new iSNS servers may not be added and thus new targets discovered via those iSNS servers; existing iSNS servers may not be removed. If disabled then new iSNS servers may be added and thus new targets discovered via those iSNS servers; existing iSNS servers may be removed.
Computer	iSCSI Target Discovery	Do not allow manual configuration of target portals	At least Windows Vista or later	If enabled then new target portals may not be added and thus new targets discovered on those portals; existing target portals may not be removed. If disabled then new target portals may be added and thus new targets discovered on those portals; existing target portals may be removed.
Computer	Kerberos	Define host name-to-Kerberos realm mappings	At least Windows Vista or later	This policy setting allows you to specify which DNS host names and which DNS suffixes are mapped to a Kerberos realm. If you enable this policy setting, you can view and change the list of DNS host names and DNS suffixes mapped to a Kerberos realm as defined by Group Policy. To view the list of mappings, enable the policy setting and then click the Show button. To add a mapping, enable the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				policy setting, note the syntax, click the Show button, click the Add button, and then type a realm name in the Value Name and the list of DNS host names and DNS suffixes in the Value using the syntax format. To remove a mapping, click its entry, and then click the Remove button. To edit a mapping, remove the current entry from the list and add a new one with different parameters. If you disable this policy setting, the host name-to-Kerberos realm mappings list defined by Group Policy is deleted. If you do not configure this policy setting, the system will use the host name-to-Kerberos realm mappings that are defined in the local registry, if they exist.
Computer	Kerberos	Define interoperable Kerberos V5 realm settings	At least Windows Vista or later	This policy setting configures the Kerberos client so that it can authenticate with interoperable Kerberos V5 realms, as defined by this policy setting. If you enable this policy setting, you can view and change the list of interoperable Kerberos V5 realms and their settings. To view the list of interoperable Kerberos V5 realms, enable the policy setting and then click the Show button. To add an interoperable Kerberos V5 realm, enable the policy setting, note the syntax, click the Show button, click the Add button, and then type the interoperable Kerberos V5 realm name in the Value Name field, and type the definition of settings using the syntax format in the Value field. To remove an interoperable Kerberos V5 realm, click its entry, and then click the Remove button. To edit a mapping, remove the current entry from the list and add a new one with different parameters. If you disable this policy setting, the interoperable Kerberos V5 realm settings defined by Group Policy are deleted. If you do not configure this policy setting, the system will use the interoperable Kerberos V5 realm settings that are defined in the local registry,

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				if they exist.
Computer	Kerberos	Require strict KDC validation	At least Windows Vista or later	This policy setting controls the Kerberos client's behavior in validating the KDC certificate. If you enable this policy setting, the Kerberos client requires that the KDC's X.509 certificate contains the KDC key purpose object identifier in the Extended Key Usage (EKU) extensions, and that the KDC's X.509 certificate contains a dNSName subjectAltName (SAN) extension that matches the DNS name of the domain. If the computer is joined to a domain, the Kerberos client requires that the KDC's X.509 certificate must be signed by a Certificate Authority (CA) in the NTAUTH store. If the computer is not joined to a domain, the Kerberos client allows the root CA certificate on the smart card to be used in the path validation of the KDC's X.509 certificate. If you disable or do not configure this policy setting, the Kerberos client will require only that the KDC certificate contain the Server Authentication purpose object identifier in the EKU extensions.
Computer	Link-Layer Topology Discovery	Turn on Mapper I/O (LLTDIO) driver	At least Windows Vista or later	This policy setting turns on the Mapper I/O network protocol driver. LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis. If you enable this policy setting, additional options are available to fine-tune your selection. You may choose the "Allow operation while in domain" option to allow LLTDIO to operate on a network interface that's connected to a managed network. On the other hand, if a network interface is connected to an unmanaged network, you may choose the "Allow operation while in public network" and "Prohibit operation while in private network" options instead. If you disable this policy setting, LLTDIO will not participate in any of the

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				activities described above. If you do not configure this policy setting, LLTDIO will be enabled with all options turned on at all times.
Computer	Link-Layer Topology Discovery	Turn on Responder (RSPNDR) driver	At least Windows Vista or later	This policy setting turns on the Responder network protocol driver. The Responder allows a computer to participate in Link Layer Topology Discovery requests so that it can be discovered and located on the network. It also allows a computer to participate in Quality-of-Service activities such as bandwidth estimation and network health analysis. If you enable this policy setting, additional options are available to fine-tune your selection. You may choose the "Allow operation while in domain" option to allow the Responder to operate on a network interface that's connected to a managed network. On the other hand, if a network interface is connected to an unmanaged network, you may choose the "Allow operation while in public network" and "Prohibit operation while in private network" options instead. If you disable this policy setting, the Responder will not participate in any of the activities described above. If you do not configure this policy setting, the Responder will be enabled with all options turned on at all times.
Computer/User	Locale Services	Disallow changing of geographic location	At least Windows Vista or later	This policy prevents users from changing their user geographical location (GeoID). If this policy is Enabled, then the user cannot change their geographical location (GeoID) If the policy is Disabled or Not Configured, then the user may select any GeoID. If this policy is Enabled at the Machine level, then it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer/User	Locale Services	Disallow selection of Custom Locales	At least Windows Vista or later	This policy prevents a user from selecting a supplemental custom locale as their user locale. The user is restricted to the set of locales that shipped with the operating system. Note that this does not affect the selection of replacement locales. To prevent the selection of replacement locales, adjust the permissions of the %windir%\Globalization directory to prevent the installation of locales by unauthorized users. Note that "Restrict user locales" can also be enabled to disallow selection of a custom locale, even if this policy is not configured. If this policy is Enabled, then the user cannot select a custom locale as their user locale, but they may still select a replacement locale if one is installed. If the policy is Disabled or Not Configured, then the user may select a custom locale as their user locale. If this policy is Enabled at the Machine level, it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer/User	Locale Services	Disallow user override of locale settings	At least Windows Vista or later	This policy prevents the user from customizing their locale by changing their user overrides. Any existing overrides in place when this policy is enabled will be frozen. To remove existing user override, first reset the user(s) values to the defaults and then apply this policy. When this policy is enabled, users may still choose alternate locales installed on the system unless prevented by other policies, however they will be unable to customize those choices. If this policy is Enabled, then the user cannot customize their user locale with user overrides. If

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				this policy is Disabled or Not Configured, then the user can customize their user locale overrides. If this policy is Enabled at the Machine level, then it cannot be disabled by a per-User policy. If this policy is Disabled at the Machine level, then the per-User policy will be ignored. If this policy is Not Configured at the machine level, then restrictions will be based on per-User policies. To set this policy on a per-user basis, make sure that the per-machine policy is set to Not Configured.
Computer	Locale Services	Restrict system locales	At least Windows Vista or later	This policy restricts the permitted system locales to the specified list. If the list is empty, it locks the system locale to its current value. This policy does not change the existing system locale; however, the next time that an admin attempts to change the machine's system locale they will be restricted to the specified list. The locale list is specified using language names, separated by a semi-colon (;). For example, en-US is English (United States). Specifying "en-US;en-CA" would restrict the system locale to English (United States) and English (Canada). If this policy is Enabled, then administrators may select a system locale only from the specified system locale list. If this policy is Disabled or Not Configured, then administrators may select any system locale shipped with the operating system.
Computer/User	Locale Services	Restrict user locales	At least Windows Vista or later	This policy restricts users on a machine to the specified list of user locales. If the list is empty, it locks all user locales to their current values. This policy does not change existing user locale settings; however, the next time a user attempts to change their user locale, their choices will be restricted to locales in this list. To set this policy on a per-user basis, make sure that the per-machine policy is set to not configured. The locale list is specified using language tags, separated by a semicolon (;). For example, en-US is English (United States). Specifying "en-

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				CA;fr-CA" would restrict the system locale to English (Canada) and French (Canada). If this policy is enabled, then only locales in the enabled list may be selected by users. If this policy is disabled or not configured, then users may select any locale installed on the machine, unless restricted by the "Disallow selection of Custom Locales" policy. If this policy is enabled at the machine level, it cannot be disabled by a per-user policy. If this policy is disabled at the machine level, then the per-user policy will be ignored. If this policy is not configured at the machine level, then restrictions will be based on per-user policies. Note that if an administrator has enabled the "Disallow selection of custom locales" policy, then users will be prevented from selecting supplemental custom locales, even if they are in the acceptable locale list for this policy.
Computer	Logon	Hide entry points for Fast User Switching	At least Windows Vista or later	By enabling the policy, Administrators hide the Switch user button in the Logon UI, the Start menu and the Task Manager.
Computer	logon:Logon	Assign a default domain for logon	At least Windows Vista or later	This policy setting specifies a default logon domain which may be a different domain than the machine joined domain. Without this policy, at logon, if a user does not specify a domain for logon, the domain to which the machine belongs is assumed as the default domain. For example if the machine belongs to the Fabrikam domain, the default domain for user logon is Fabrikam. If you enable this policy setting, the a default logon domain will be set to the specified domain which may not be the machine joined domain. If you disable or do not configure this policy setting, the default logon domain will always be set to the machine joined domain.
Computer	logon:Logon	Exclude credential providers	At least Windows Vista or later	This policy setting allows the administrator to exclude the specified credential

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				providers from use during authentication. Note: credential providers are used to process and validate user credentials during logon or when authentication is required. Windows Vista provides two default credential providers: Password and Smart Card. An administrator can install additional credential providers for different sets of credentials (for example, to support biometric authentication). If you enable this policy, an administrator can specify the CLSIDs of the credential providers to exclude from the set of installed credential providers available for authentication purposes. If you disable or do not configure this policy, all installed credential providers will be available for authentication purposes.
Computer	Microsoft Peer-to-Peer Networking Services	Disable password strength validation for Peer Grouping	At least Windows Vista or later	By default, when a Peer Group is created that allows for password-authentication (or the password for such a Group is changed), Peer Grouping validates that the password meets the password complexity requirements for the local system. Thus, it will not allow any passwords to be used for a Peer Group that are weaker than what would be allowed for a login password. This setting controls this validation behavior. If set to 1, then this validation will not be performed and any password will be allowed. If set to 0, the validation will be performed.
Computer	Microsoft Support Diagnostic Tool	Microsoft Support Diagnostic Tool: Configure execution level	At least Windows Vista or later	Determines the execution level for Microsoft Support Diagnostic Tool. Microsoft Support Diagnostic Tool (MSDT) gathers diagnostic data for analysis by support professionals. If you enable this policy setting, administrators will be able to use MSDT to collect and send diagnostic data to a support professional to resolve a problem. If you disable this policy, MSDT will not be able to gather diagnostic data. If you do not configure this policy setting, MSDT will be enabled by default. This policy setting takes effect only if the diagnostics-wide scenario execution

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				policy is not configured. No reboots or service restarts are required for this policy to take effect: changes take effect immediately. This policy setting will only take effect when the Diagnostic Policy Service (DPS) is in the running state. When the service is stopped or disabled, diagnostic scenarios will not be executed. The DPS can be configured with the Services snap-in to the Microsoft Management Console.
Computer	Microsoft Support Diagnostic Tool	Microsoft Support Diagnostic Tool: Restrict tool download		
User	mmc:MMC_RESTRICT	Failover Clusters Manager	At least Windows Vista or later	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	mmc:MMC_RESTRICT	TPM Management	At least Windows Vista or later	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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	mmc:MMC_RESTRICT	Windows Firewall with Advanced Security	At least Windows Vista or later	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

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				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.
Computer/User	Network Projector	Turn off Connect to a Network Projector	At least Windows Vista or later	Disables the Connect to a Network Projector wizard so that users cannot connect to a network projector. If you enable this policy, users cannot use the Connect to a Network Projector wizard to connect to a projector. If you disable this policy or do not configure it, users can run the Connect to a Network Projector wizard to connect to a projector.
User	Network Projector	Turn off Connect to a Network Projector	At least Windows Vista or later	Disables the Connect to a Network Projector wizard so that users cannot connect to a network projector. If you enable this policy, users cannot use the Connect to a Network Projector wizard to connect to a projector. If you disable this policy or do not configure it, users can run the Connect to a Network Projector wizard to connect to a projector.
User	Network Sharing	Prevent users from sharing files within their profile.	At least Windows Vista or later	By default users are allowed to share files within their profile to other users on their network once an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile. If you enable this policy, users will not be able to share files within their profile using the sharing wizard. Also, the sharing wizard will not create a share at %root%\users and can only be used to create SMB shares on folders. If you disable or donΓÇÖt configure this policy, then users will be able to share files out of their user profile once an administrator has opted in the computer.
Computer	Notification Settings	Critical Battery Notification Action	At least Windows Vista or later	Specifies the action that Windows takes when battery capacity reaches the critical

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				battery notification level. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Critical Battery Notification Level	At least Windows Vista or later	Specifies the percentage of battery capacity remaining that triggers the critical battery notification action. If you enable this policy, you must enter a numeric value (percentage) to set the battery level that triggers the critical notification. To set the action that is triggered, see the "Critical Battery Notification Action" policy setting. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Low Battery Notification Action	At least Windows Vista or later	Specifies the action that Windows takes when battery capacity reaches the low battery notification level. Possible actions include: -Take no action -Sleep -Hibernate -Shut down If you enable this policy setting, you must select the desired action. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Low Battery Notification Level	At least Windows Vista or later	Specifies the percentage of battery capacity remaining that triggers the low battery notification action. If you enable this policy, you must enter a numeric value (percentage) to set the battery level that triggers the low notification. To set the action that is triggered, see the "Low Battery Notification Action" policy setting. If you disable this policy setting or do not configure it, users can see and change this setting.
Computer	Notification Settings	Turn Off Low Battery User Notification	At least Windows Vista or later	Disables a user notification when the battery capacity remaining equals the low battery notification level. If you enable this policy, Windows will not show a

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				notification when the battery capacity remaining equals the low battery notification level. To configure the low battery notification level, see the "Low Battery Notification Level" policy setting. The notification will only be shown if the "Low Battery Notification Action" policy setting is configured to "No Action". If you do not configure this policy setting, users can see and change this setting.
Computer	NTFS Filesystem	Selectively allow the evaluation of a symbolic link.	At least Windows Vista or later	Symbolic links can introduce vulnerabilities in certain applications. To mitigate this issue, you can selectively enable or disable the evaluation of these types of symbolic links: Local Link to a Local Target Local Link to a Remote Target Remote Link to Remote Target Remote Link to Local Target For further information please refer to the Windows Help section NOTE: If this policy is Disabled or Not Configured, local administrators may select the types of symbolic links to be evaluated.
Computer	Offline Files	Configure slow-link mode	At least Windows Vista or later	This policy setting allows you to enable and configure the slow-link mode of Offline Files. When Offline Files is operating in slow-link mode, all file requests are satisfied from the Offline Files cache, just as when the user is working offline. However, the user can manually initiate synchronization on demand. Once the synchronization completes, the system continues to operate in the slow-link mode until the user transitions the share to online mode. If you enable this policy setting, Offline Files will operate in slow-link mode if the end-to-end network throughput between the client and the server is below the throughput threshold parameter, or if the network latency is above the latency threshold parameter. You can configure slow-link mode by specifying thresholds for Throughput (bits per second) and Latency (in milliseconds) for specific UNC paths. You can specify

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				one or both threshold parameters. When a share is transitioned to slow-link mode, the user can force the share to transition to online mode. However, the system periodically checks to see if a connection to a server is slow. If the connection is slow then the share will again be transitioned to slow-link mode. Note: You can use wildcards (*) for specifying UNC paths. If you disable or do not configuring this policy setting, Offline Files will not transition to slow-link mode.
Computer	Offline Files	Turn on economical application of administratively assigned Offline Files	At least Windows Vista or later	This policy setting allows you to turn on economical application of administratively assigned Offline Files. If you enable this policy setting, only new files and folders in administratively assigned folders are synchronized at logon. Files and folders that are already available offline are skipped and are synchronized later. If you disable or do not configure this policy setting, all administratively assigned folders are synchronized at logon.
Computer	Online Assistance	Turn off Active Help	At least Windows Vista or later	Specifies whether active content links in trusted assistance content are rendered. By default, the Help viewer renders trusted assistance content with active elements such as ShellExecute links and Guided Help links. If you enable this policy, such links are not rendered. The text is displayed but there are no clickable links for these elements. If you Disable or do not configure this setting, the default behavior (Help viewer renders trusted assistance content with active elements) applies.
Computer	Online Assistance	Turn off Untrusted Content	At least Windows Vista or later	Specifies whether untrusted content is rendered. By default, the Help viewer renders untrusted assistance content pages with the exception of active links. Active links, such as ShellExecute and Guided Help, are rendered as text and are not clickable. If you enable this policy, untrusted content is not rendered at all, and

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				a navigation error page is displayed to the user. If you Disable or do not configure this setting, the default behavior (untrusted content is rendered with the exception of active links, which are rendered as text only) applies.
Computer	Parental Controls	Make Parental Controls control panel visible on a Domain	At least Windows Vista or later	Configure the Parental Controls feature. If you turn on this setting, the Parental Controls control panel will be visible on a domain joined computer. If you turn off or do not configure this setting, the Parental Controls control panel will not be visible on a domain joined computer.
Computer/User	Pen Flicks Learning	Prevent Flicks Learning Mode	At least Windows Vista or later	Makes pen flicks learning mode unavailable. If you enable this policy, pen flicks are still available but learning mode is not. Pen flicks are off by default and can be turned on system-wide, but cannot be restricted to learning mode applications. This means that the pen flicks training triggers in Internet Explorer are disabled and that the pen flicks notification will never be displayed. However, pen flicks, the pen flicks tray icon and pen flicks training (that can be accessed through CPL) are still available. Conceptually this policy is a subset of the Disable pen flicks policy. If you disable or do not configure this policy, all the features described above will be available.
Computer/User	Pen UX Behaviors	Prevent flicks	At least Windows Vista or later	Makes pen flicks and all related features unavailable. If you enable this policy, pen flicks and all related features are unavailable. This includes: pen flicks themselves, pen flicks training, pen flicks training triggers in Internet Explorer, the pen flicks notification and the pen flicks tray icon. If you disable or do not configure this policy, pen flicks and related features are available.
Computer/User	Performance Control Panel	Turn off access to the OEM and Microsoft branding section	At least Windows Vista or later	Removes access to the performance center control panel OEM and Microsoft branding links. If you enable this setting, the OEM and Microsoft web links within

Node	Final Subnode	Full Policy Name	Supported on	Help/Explain Text
				the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel OEM and Microsoft branding links will be displayed to the user.