Report Number: C4-053R-00

# Group Policy Reference

## Systems and Network Attack Center (SNAC)

Author:
David C. Rice

Updated: March 2, 2001
Version 1.0.8

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

W2KGuides@nsa.gov

This Page Intentionally Left Blank

## Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

All other names are registered trademarks or trademarks of their respective companies.

# Table of Contents

**Trademark Information** ..... **iii**

**Table of Contents** ..... **iv**

**Introduction** ..... **1**

*About the Group Policy Reference* ..... *1*

**Chapter 1** ..... **2**

**Computer Configuration** ..... **2**

*Software Settings* ..... *2*

*Windows Settings* ..... *3*

Account Policies ..... 3
Local Policies ..... 5
Event Log ..... 15
Restricted Groups ..... 17
System Services ..... 17
Registry ..... 18
File System ..... 18
Public Key Policies ..... 19
IP Security Policies on Active Directory ..... 22

*Administrative Templates* ..... *26*

NetMeeting ..... 26
Internet Explorer ..... 26
Task Scheduler ..... 29
Windows Installer ..... 31
Logon ..... 40
Disk Quotas ..... 45
DNS Client ..... 48
Group Policy ..... 48
Windows File Protection ..... 57
Offline Files ..... 58
Network and Dial-up Connections ..... 65

**Chapter 2** ..... **73**

**User Configuration** ..... **73**

*Software Settings* ..... *73*

*Windows Settings* ..... *74*

Browser User Interface ..... 74
Connection ..... 75
URLS ..... 76
Security ..... 76
Programs ..... 77

*Administrative Templates* ..... *79*

NetMeeting ..... 79
Internet Explorer ..... 84
Windows Explorer ..... 112
Microsoft Management Console ..... 120

Task Scheduler....152
Windows Installer....154
Active Desktop....166
Active Directory....169
Add/Remove Programs....172
Display....175
Printers....177
Regional Options....179
Offline Files....179
Network and Dial-up Connections....184
Logon/Logoff....196
Group Policy....200

**Index....205**

This Page Intentionally Left Blank

# Introduction

The purpose of this guide is to inform the reader about the available settings Group Policy in an Active Directory-enabled domain updated with Service Pack 1. Local Group Policies, while very similar in function and structure, are not addressed in this reference.

This manual is not a *how-to* guide for using Group Policy in a secure configuration, but more a map to help the reader locate specific policies within the Group Policy Snap-in for a given Active Directory container. It is hoped that this map will alleviate *some* of the complexity in managing and understanding Group Policy.

The manual is organized in the identical hierarchical structure of that of the Group Policy snap-in. The Table of Contents mirrors the Group Policy snap-in with top-level nodes fully expanded. The Index in the back of this manual should help the reader search for specific policies based on certain keywords. For instance, by looking up "Audit" in the index, the reader should be able to find all instances of policies that contain the word "audit."

The organization of each Policy Explanation is as follows:

- The Policy Title as it appears in the Microsoft Management Console Group Policy snap-in.
- Next, the default configuration, or default settings of the policy are listed, followed by all possible settings available to the administrator.
- Finally, an explanation of the policy is provided. In many instances this is taken directly from the Explanation Tab for the policy itself. Additional comments have been provided for policies where the MMC explanation was determined lacking.

A concerted effort has been made to make this reference as robust as possible before general release; however, as with any large document, perfection is an iterative process. Please inform us of any corrections or omissions.

Hopefully, the Group Policy Reference will save the reader from wildly left-clicking through the Group Policy snap-in in search of a particular policy.

## About the Group Policy Reference

This document consists of the following chapters:

**Chapter 1, "Computer Configuration,"** delineates policy settings available for computers within an Active Directory-enabled domain, including Software Settings, Windows Settings, Administrative Templates and all respective sub-nodes.

**Chapter 2, "User Configuration,"** delineates policy settings available for users within an Active Directory-enabled domain, including Software Settings, Windows Settings, Administrative Templates and all respective sub-nodes.

**Index,** a collection of the most useful/common keywords in the Group Policy snap-in.

Chapter

1



# Computer Configuration

This includes all computer-related policies that specify operating system behavior, desktop behavior, application settings, security settings, computer assigned options, and computer startup and shutdown scripts. Computer-related Group Policy is applied when the operating system initializes and during periodic refresh cycle.

## Software Settings

The Software Settings node only contains the Software Installation object. Software Installation permits the administrator to create and modify unique sets of software packages to push out to the network users.

### Software Installation

Software Installation helps you specify how applications are installed and maintained within your organization.

You manage an application within a Group Policy object, which is in turn associated with a particular Active Directory container – either a site, domain, or organizational unit. Applications can be managed in one of two modes: assigned or published.

You assign an application when you want everyone to have the application on his or her computer. For example, suppose you want all users in a marketing department to have Microsoft Excel on their computers. A Group Policy object manages every user in marketing. When you assign Microsoft excel within the marketing Group Policy object, Microsoft Excel is advertised on every marketing user's computer. When an assigned application is advertised, it is not actually installed on the computer. In the case, the application advertisement installs only enough information about Microsoft Excel to make the Microsoft Excel shortcuts appear on the Start menu and the necessary file associations (.xls) appear in the registry.

When these users log on to their computers, Microsoft Excel appears on their Start menu. When they select Microsoft Excel from the Start menu for the first time, Microsoft Excel is installed. A user can also install an advertised application by opening a document associated with the application (either by file name extension or by COM-based activation). If a user who has not yet activated Microsoft Excel from the Start menu clicks a Microsoft Excel spreadsheet to open it, then Microsoft Excel is installed and the spreadsheet opens.

A user can delete an assigned application, but the assigned application is advertised again the next time the user logs on. It will be installed the next time a user selects it from the Start menu.

You publish an application when you want the application to be available to people managed by the Group Policy object, should a user want the application. With published

applications, it is up to each person to decide whether or not to install the published application.

For example, if you publish Microsoft Image Composer to users managed by the marketing Group Policy object and a marketing user wants to install Image Composer, the user can use Add/Remove Programs in Control Panel, click Image Composer from the list of published applications, and then install it. If users do not install Image Composer using Add/Remove Programs in Control Panel, and if the .jpg file name extension for the image document is associated with Image Composer, then Image Composer can be installed for users when they first open any .jpg document.

## Windows Settings

### Scripts (Startup/Shutdown)

Place startup and shutdown scripts for computers in this folder. You use this extension to specify scripts that are to run at computer startup or shutdown. These scripts run as Local System.

Windows 2000 includes Windows Script Host, a language-independent scripting host for 32-bit Windows platforms that includes both Visual Basic Scripting Edition (VBScript) and JScript scripting engines. You can use Windows Script Host to run .vbs and .js scripts directly on the Windows desktop or command console, without the need to embed those scripts in an HTML document.

### Security Settings

#### Account Policies

*Password Policy*

For domain or local user accounts, determines settings for passwords such as enforcement lifetimes.

- Enforce password history

  > *Default settings: 1 passwords remembered*
  >
  > *Minimum setting is: 0 passwords, do not keep password history*
  >
  > *Maximum setting is: 24 passwords*

- Maximum password age

  > *Default Setting: 0 days*
  >
  > *Minimum setting is: 0 days*
  >
  > *Maximum setting is: 998 days*

- Minimum password age

  > *Default Setting: 0 days*
  >
  > *Minimum setting is: 0 days*
  >
  > *Maximum setting is: 998 days*

- Minimum password length

  > *Default Setting: 0 characters*
  >
  > *Minimum setting is: 0 characters*
  >
  > *Maximum setting is: 14 characters*

- Passwords must meet complexity requirements

  > *Default Setting: Disabled*
  >
  > *Administrator may choose from among the following: Enabled, Disabled.*

- Store password using reversible encryption for all users in the domain

  > *Default Setting: Disabled*
  >
  > *Administrator may choose from among the following: Enabled, Disabled.*

*Account Lockout Policy*

For domain or local user accounts, determines when and for whom an account will be locked out of the system.

- Account lockout duration

  > *Default Setting: Not Defined*
  >
  > *When defined, default value is 30 minutes*

- Account lockout threshold

  > *Default Setting: 0 invalid logon attempts*

- Reset account lockout counter after

  > *Default Setting: Not Defined*
  >
  > *When defined, default value is 5 minutes*

*Kerberos Policy*

For domain user accounts, determines Kerberos-related settings, such as ticket lifetimes and enforcement.

- Enforce user logon restrictions

  > *Default Setting: Enabled*

- Maximum lifetime for service ticket

  > *Default Setting: 600 minutes*
  >
  > *Minimum setting is: 0 minutes, ticket doesn't expire*
  >
  > *Maximum setting is: 99,999 minutes*

- Maximum lifetime for user ticket

  *Default Setting: 10 hours*

  *Minimum setting is: 0 hours, ticket doesn't expire*

  *Maximum setting is: 99,999 hours*

- Maximum lifetime for user ticket renewal

  *Default Setting: 7 days*

  *Minimum setting is: 0 days, ticket doesn't expire*

  *Maximum setting is: 99,999 days*

- Maximum tolerance for computer clock synchronization

  *Default Setting: 5 minutes*

  *Minimum setting is: 0 minutes*

  *Maximum setting is: 99,999 minutes*

### Local Policies

These policies pertain to the computer. Local policies are based on the computer you are logged into, and the rights you have on that particular computer.

Local Policies, by definition, are local to a computer. When these settings are imported to a Group Policy object in Active Directory, they will affect the local security settings of any computer accounts to which that Group Policy object is applied. In either case, your user account rights may no longer apply if there is a local policy setting that overrides those privileges.

*Audit Policy*

Determines which security events are logged into the Security log on the computer (successful attempts, failed attempts or both). The Security log is part of Event Viewer.

- Audit account logon events

  *Default Setting: Not defined*

  *When defined, administrator may choose to audit these attempts: Success, Failure*

- Audit account management

  *Default Setting: Not defined*

  *When defined, administrator may choose to audit these attempts: Success, Failure*

- Audit directory service access

  *Default Setting: Not defined*

  *When defined, administrator may choose to audit these attempts: Success, Failure*

- Audit logon events

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may choose to audit these attempts: Success, Failure*

- Audit object access

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may choose to audit these attempts: Success, Failure*

- Audit policy change

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may choose to audit these attempts: Success, Failure*

- Audit privilege use

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may choose to audit these attempts: Success, Failure*

- Audit process tracking

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may choose to audit these attempts: Success, Failure*

- Audit system events

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may choose to audit these attempts: Success, Failure*

*User Rights Assignment*

- Access this computer from the network

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may select which users or groups this policy will apply.*

- Act as part of the operating system

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may select which users or groups this policy will apply.*

- Add workstations to domain

  > *Default Setting: Not defined*
  >
  > *When defined, administrator may select which users or groups this policy will apply.*

- Back up files and directories

  > *Default Setting: Not defined*

> *When defined, administrator may select which users or groups this policy will apply.*

- Bypass traverse checking

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Change the system time

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Create a pagefile

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Create a token object

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Create permanent shared objects

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Debug programs

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Deny access to this computer from the network

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Deny logon as a batch job

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Deny logon as a service

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

- Deny logon locally

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Enable computer and user accounts to be trusted for delegation

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Force shutdown from a remote system

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Generate security audits

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Increase quotas

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Increase scheduling priority

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Load and unload device drivers

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Lock pages in memory

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Log on as a batch job

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Log on as a service

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Log on locally

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Manage auditing and security log

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Modify firmware environment values

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Profile single process

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Profile system performance

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Remove computer from docking station

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Replace a process level token

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Restore files and directories

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Shut down the system

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Synchronize directory service data

  *Default Setting: Not defined*

  *When defined, administrator may select which users or groups this policy will apply.*

- Take ownership of files or other objects

> *Default Setting: Not defined*
>
> *When defined, administrator may select which users or groups this policy will apply.*

*Security Options*

- Additional restrictions for anonymous connections

> *Default Setting: Not defined*
>
> *When defined, default setting is: None. Rely on default permissions. Administrator may select from among the following:*
>
> *- None. Rely on default permissions*
>
> *- Do not allow enumeration of SAM accounts and shares*
>
> *- No access without explicit anonymous permissions*

- Allow server operators to schedule tasks (domain controllers only)

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enable, Disabled.*

- Allow system to be shut down without having to log on

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled.*

- Allowed to eject removable NTFS media

> *Default Setting: Not defined*
>
> *When defined, default setting is: Administrators Group. Administrators may choose from among the following:*
>
> *- Administrators*
>
> *- Administrators and Power Users*
>
> *- Administrators and Interactive Users*

- Amount of idle time required before disconnecting session

> *Default Setting: Not defined*
>
> *When defined, default setting is: 1 minute.*

- Audit the access of global system objects

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Audit use of Backup and Restore privilege

  > *Default Setting: Not defined*
  >
  > *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Automatically log off users when logon time expires

  > *Default Setting: Disabled*
  >
  > *Administrator may choose from among the following: Enabled, Disabled.*

- Automatically log off users when logon time expires (local)

  > *Default Setting: Not defined*
  >
  > *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Clear virtual memory pagefile when system shuts down

  > *Default Setting: Not defined*
  >
  > *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Digitally sign client communication (always)

  > *Default Setting: Not defined*
  >
  > *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Digitally sign client communication (when possible)

  > *Default Setting: Not defined*
  >
  > *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Digitally sign server communication (always)

  > *Default Setting: Not defined*
  >
  > *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Digitally sign server communication (when possible)

  > *Default Setting: Not defined*
  >
  > *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Disable CTRL+ALT+DEL requirement for logon

  > *Default Setting: Not defined*

> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Do not display last user name in logon screen

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- LAN Manager Authentication Level

> *Default Setting: Not defined*
>
> *When defined, default setting is: Send LM & NTLM responses. Administrator may choose from among the following:*
>
> *- Send LM & NTLM responses*
>
> *- Send LM & NTLM – use NTLM v2 session security if negotiated*
>
> *- Send NTLM response only*
>
> *- Send NTLMv2 response only*
>
> *- Send NTLMv2 response only\refuse LM*
>
> *- Send NTLMv2 response only\refuse LM & NTLM*

- Message text for users attempting to log on

> *Default Setting: Not defined*
>
> *When defined, administrator may add text.*

- Message title for users attempting to log on

> *Default Setting: Not defined*
>
> *When defined, administrator may add text.*

- Number of previous logons to cache (in case domain controller is not available)

> *Default Setting: Not defined*
>
> *When defined, default setting is: 1.*

- Prevent system maintenance of computer account password

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Prevent users from installing printer drivers

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Prompt user to change password before expiration

  *Default Setting: Not defined*

  *When defined, default setting is: 0 days.*

- Recovery Console: Allow automatic administrative logon

  *Default Setting: Not defined*

  *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Recovery Console: Allow floppy copy and access to all drives and all folders

  *Default Setting: Not defined*

  *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Rename administrator account

  *Default Setting: Not defined*

  *When defined, administrator may rename account.*

- Rename guest account

  *Default Setting: Not defined*

  *When defined, administrator may rename account.*

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

  *Default Setting: Not defined*

  *When defined, default setting is: Enabled. Administrator may choose from among the following: Enabled, Disabled.*

- Restrict floppy access to locally logged-on user only

  *Default Setting: Not defined*

  *When defined, default setting is: Enabled. Administrator may choose from among the following: Enabled, Disabled.*

- Secure Channel: Digitally encrypt secure channel data (always)

  *Default Setting: Not defined*

  *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Secure Channel: Digitally encrypt secure channel data (when possible)

  *Default Setting: Not defined*

> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Secure Channel: Digitally sign secure channel data (when possible)

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Secure Channel: Require strong (Windows 2000 or later) session key

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Secure system partition (for RISC platforms only)

> *Default Setting: Not defined*
>
> *When defined, default setting is: Enabled. Administrator may choose from among the following: Enabled, Disabled.*

- Send unencrypted password to connect to third-party SMB servers

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Shut down system immediately if unable to log security audits

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Smart card removal behavior

> *Default Setting: Not defined*
>
> *When defined, default setting is: No Action. Administrator may choose from among the following:*
>
> *- No Action*
>
> *- Lock Workstation*
>
> *- Force Logoff*

- Strengthen default permissions of global system objects (e.g. Symbolic links)

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Unsigned driver installation behavior

> *Default Setting: Not defined*
>
> *When defined, default setting is: Silently succeed. Administrator may choose from among the following:*
>
> *- Silently succeed*
>
> *- Warn but allow installation*
>
> *- Do not allow installation*

- Unsigned non-driver installation behavior

> *Default Setting: Not defined*
>
> *When defined, default setting is: Silently succeed. Administrator may choose from among the following:*
>
> *- Silently succeed*
>
> *- Warn but allow installation*
>
> *- Do not allow installation*

Event Log

*Setting for Event Logs*

- Maximum application log size

> *Default Setting: Not defined*
>
> *When defined, default setting is: 512 kilobytes. Minimum value is 64 bytes. Maximum value is 4194240 kilobytes.*

- Maximum security log size

> *Default Setting: Not defined*
>
> *When defined, default setting is: 512 kilobytes. Minimum value is 64 kilobytes. Maximum value is 4194240 kilobytes.*

- Maximum system log size

> *Default Setting: Not defined*
>
> *When defined, default setting is: 512 kilobytes. Minimum value is 64 kilobytes. Maximum value is 4194240 kilobytes.*

- Restrict guest access to application log

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Restrict guest access to security log

> *Default Setting: Not defined*

> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Restrict guest access to system log

> *Default Setting: Not defined*
>
> *When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

- Retain application log

> *Default Setting: Not defined*
>
> *When defined, default setting is: 7 days. Minimum value is 1 day. Maximum value is 365 days.*

- Retain security log

> *Default Setting: Not defined*
>
> *When defined, default setting is: 7 days. Minimum value is 1 day. Maximum value is 365 days.*

- Retain system log

> *Default Setting: Not defined*
>
> *When defined, default setting is: 7 days. Minimum value is 1 day. Maximum value is 365 days.*

- Retention method for application log

> *Default Setting: Not defined*
>
> *When defined, default setting is: Overwrite events by days. Administrator may choose from among the following:*
>
> *- Overwrite events by days*
>
> *- Overwrite events as needed*
>
> *- Do not overwrite events (clear log manually)*

- Retention method for security log

> *Default Setting: Not defined*
>
> *When defined, default setting is: Overwrite events by days. Administrator may choose from among the following:*
>
> *- Overwrite events by days*
>
> *- Overwrite events as needed*
>
> *- Do not overwrite events (clear log manually)*

- Retention method for system log

> *Default Setting: Not defined*
>
> *When defined, default setting is: Overwrite events by days. Administrator may choose from among the following:*

*- Overwrite events by days*

*- Overwrite events as needed*

*- Do not overwrite events (clear log manually)*

- Shut down the computer when the security audit log is full

*Default Setting: Not defined*

*When defined, default setting is: Disabled. Administrator may choose from among the following: Enabled, Disabled.*

### Restricted Groups

This provides an important new security feature that acts as a governor for group membership. Restricted Groups automatically provides security memberships for default Windows 2000 groups that have predefined capabilities, such as Administrators, Power Users, Print Operators, Server Operators, and Domain Admins. You can later add any groups that you consider sensitive or privileged to the Restricted Groups security list.

For example, the Power Users group is automatically part of Restricted Groups, since it is a default Windows 2000 group. Assume it contains two users: Alice and Bob. Bob adds Charles to the group, through the Active Directory Users and Computers snap-in, to cover for him while he is on vacation. However, no one remembers to remove Charles from the group when Bob comes back from vacation. In actual deployments, over time, these situations can add up, resulting in extra members in various groups, members who should no longer have these rights. Configuring security through Restricted Groups can prevent this situation. Since only Alice and Bob are listed in the Restricted Groups node for Power Users, when Group Policy settings are applied, Charles is removed from the group automatically.

Configuring Restricted Groups ensures that group memberships are set as specified. Groups and users not specified in Restricted Groups are removed from the specific group. In addition, the reverse membership configuration option ensures that each Restricted Group is a member of only those groups specified in the **Member Of** column. For these reasons, Restricted Groups should be used primarily to configure membership of local groups on workstation or member servers.

### System Services

The Administrator can configure security attributes for all existing system services on the local computer. System Services lists all services on the machine alphabetically. The administrator may determine which services are permitted to execute and by which users or Security Group (Everyone, Server Operators, etc…).

*All services have the following default settings:*

*Startup: Not defined*

*Permission: Not defined*

*When defined, default settings are:*

*Startup: Disabled*

*Permission: Everyone, Full Control*

*The Administrator may choose from among the following for Startup:*

*- Automatic*

*- Manual*

> *- Disabled*
>
> *- The Administrator may choose from among the following for Permission: Any Security Group or user.*

### Registry

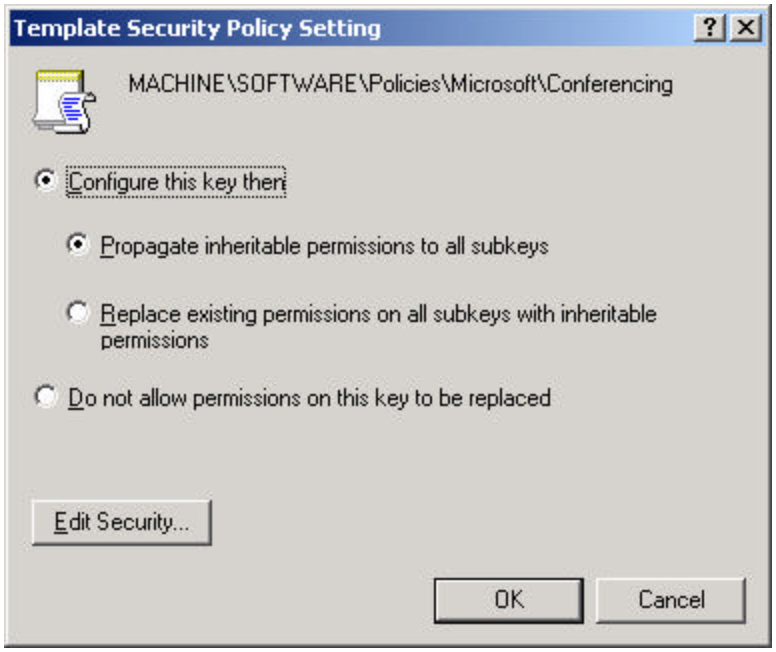
The Administrator can configure attributes for all existing registry keys on the local system. The Registry node is empty by default. The Administrator may add registry keys into this node, and configure the key with specific permissions. When adding and configuring a key, the following occurs:

> *Administrator may choose from among the following registry trees:*
>
> *CLASSES_ROOT*
>
> *MACHINE*
>
> *USERS*

Once a key is selected, the Administrator must set the permissions for the key.

> *Default Setting for Permission is: Everyone, Full Control*

Another dialog box appears titled Template Security Policy Setting. Below is a screen shot of the dialog box with its default settings.




Once **OK** is selected, the key is added to the Registry node with the following defaults:

> *Default Settings for Permission: nothing displayed*
>
> *Default Setting for Audit: nothing displayed*

### File System

The Administrator can configure the security attributes for all existing files and folders in the local file system. The File System node is empty by default. The Administrator may add files and folders to this node, and configure the file or folder with specific permissions. When adding and configuring, the following occurs:

> *The Administrator may browse among all valid drives on the system (A:, C:, etc…) to locate a particular file or folder.*

Once the file or folder is selected the Administrator must set permissions.

> *Default Setting for Permission: Everyone, Full Control*

Another dialog box appears titled Template Security Policy Setting. Below is a screen shot of the dialog box with its default settings.

Once **OK** is selected, the file or folder is added to the File System node with the following defaults:

> *Default Settings for Permission: nothing displayed*
>
> *Default Setting for Audit: nothing displayed*

### Public Key Policies

Using public key policy settings in Windows 2000 Group Policy you can:

Have computers automatically submit a certificate request to an enterprise certification authority and install the issued certificate. This is useful for ensuring that computers have the certificates that they need for performing public key cryptographic operations in your organization (to use for IP security or client authentication, for example). See Automatic certificate request settings for more information about certificate auto-enrollment for computers.

Create and distribute a certificate trust list. A certificate trust list is a signed list of root certification authority certificates that an administrator considers reputable for designated purposes such as client authentication or secure e-mail. If you want to trust a certification authority's certificates for IP security but not client authentication, then a certificate trust list is the way you can implement that trust relationship. See Enterprise trust policy for more information about certificate trust lists.

Establish common trusted root certification authorities. This policy setting is useful for making computers and users subject to common root certification authorities (in

addition to the ones they already individually trust). It is not necessary to use this policy setting for certification authorities in a Windows 2000 domain, since they are already trusted by all users and computers in the domain. This policy is primarily useful for establishing trust in a root certification authority that is not a part of your organization. See Policies to establish trust of root certification authorities for more information about certificate trust lists.

Add encrypted data recovery agents and change the encrypted data recovery policy settings. See Encrypting File System and data recovery in the Windows 2000 Help File for more information about this policy setting.

Using these public key policy settings in Group Policy is not necessary for deploying a public key infrastructure in your organization. However, these settings do give you additional flexibility and control when establishing trust in certification authorities, issuing certificates to computers, and deploying the encrypting file system (EFS).

The following four nodes are located within Public Key Policies: Encrypted Data Recovery Agents, Automatic Certificate Request Settings, Trusted Root Certification Authorities, and Enterprise Trust.

*Encrypted Data Recovery Agents*

A *recovery policy* refers to the policy that users in your computing environment adhere to when recovering encrypted data. A recovery policy is a type of public key policy.

When Windows 2000 Server is installed, a recovery policy is automatically implemented for the domain when the first domain controller is set up. The domain administrator is issued the self-signed certificate, which designates the domain administrator as the recovery agent.

EFS provides built-in data recovery by enforcing a recovery policy requirement. The requirement is that a recovery policy must be in place before users can encrypt files. The recovery policy provides for a person to be designated as the recovery agent. A recovery policy is automatically put in place when the administrator logs on to the system for the first time, making the administrator the recovery agent.

The following is the default settings for recovery agents:

> *Default Settings:*
>
> *Issued To: Administrator*
>
> *Issued By: Administrator*
>
> *Expiration Date: 1/4/2003*
>
> *Intended Purposes: File Recovery*
>
> *Friendly Name: <None>*

The default recovery policy is configured locally for stand-alone computers. For computers that are part of a network, the recovery policy is configured at either the domain, organizational unit, or individual computer level, and applies to all Windows 2000-based computers within the defined scope of influence. Recovery certificates are issued by a Certificate Authority (CA) and managed using Certificates in the Microsoft Management Console (MMC).

On a network, the recovery policy is set up by a domain administrator or recovery agent who controls the recovery keys for all computers in the scope of influence for the policy.

Because the security subsystem handles enforcing, replicating, and caching of the recovery policy, users can implement file encryption on a system that is temporarily

offline, such as a portable computer. (This process is similar to logging on to their domain account using cached credentials).

Administrators can define one of three kinds of policies: a no-recovery policy, an empty recovery policy, or a recovery policy with one or more recovery agents.

> ***Recovery-agent policy***. *When an administrator adds one or more recovery agents, a recovery-agent policy is in effect. These agents are responsible for recovering any encrypted data within their scope of administration. This is the most common type of recovery policy.*
>
> ***Empty recovery policy***. *When an administrator deletes all recovery agents and their public-key certificates, an empty recovery policy is in effect. An empty recovery policy means that no one is a recovery agent, and that users cannot encrypt data on computers within the scope of influence of the recovery policy. The effect of an empty recovery policy is to turn off EFS altogether.*
>
> ***No-recovery policy***. *When an administrator deletes the group recovery policy, a no-recovery policy is in effect. Because there is no group recovery policy, the default local policy on individual computers is used for data recovery. This means that local administrators control the recovery of data on their computers.*

*Automatic Certificate Request Settings*

Certificate enrollment is the process of requesting, receiving, and installing a certificate. By using automatic certificate settings in public key policies, you can have computers associated with a Group Policy object automatically enroll for certificates. This can save you the step of explicitly enrolling for computer-related certificates for each computer.

After establishing an automatic certificate request, the actual certificate requests will occur the next time the computers associated with the Group Policy object log on to the network.

Creating an automatic certificate request requires that you know the following two things:

The certificate type you want computers associated with the Group Policy object to enroll for automatically. Computers can only automatically request certificate types that have a purpose associated with computers, not users. Examples of computer-related certificates would be:

> *Computer certificates.*
>
> *IPSec certificates.*
>
> *Web Server certificates.*

The certification authority (CA) that can issue the certificate.

You can select from among a predefined list of CAs. The CA that you select must be capable of issuing a certificate of the type and purpose you have specified.

Note: Automatic certificate requests work *only* with Windows 2000 certification authorities (CAs) running the enterprise policy module. You also need to have administrative privileges to *establish* automatic certificate requests for a Group Policy object.

*Trusted Root Certification Authorities*

If your organization has its own Windows 2000 root CAs and uses Active Directory, you do not need to use the Group Policy mechanism to distribute root certificates.

If your organization has its own root CAs that are not installed on Windows 2000 servers, you should use the Trusted Root Certification Authority Policy to distribute your organization's root certificates.

To establish a trusted root certification authority (CA) using Group Policy, the Group Policy object that you create must have access to the root certificate. This requires that you import a copy of the root authority certificate. To import a trusted root certificate you will need the root certificate in the form of a PKCS #12 file (.pfx, .p12), a PKCS #7 file (.spc, .p7b), a certificate file (.cer, .crt), or a Microsoft Serialized Certificate Store file (.sst).

If your organization does not have its own CAs, you should use the Enterprise Trust Policy to create certificate trust lists to establish your organization's trust of external root CAs.

*Enterprise Trust*

If your organization does not have its own CAs, you should use the Enterprise Trust Policy to create certificate trust lists to establish your organization's trust of external root CAs.

A Certificate Trust List (CTL) allows you to control trust of the purpose and validity period of certificates issued by external certification authorities (CAs).

Typically, a CA can issue certificates for a wide variety of purposes such as secure e-mail or client authentication. But there may be reasons that you want to limit the trust of certificates issued by a particular CA, especially if the CA is external to your organization. This is where creating a certificate trust list and using it via Group Policy is useful.

Suppose, for example, a CA named "My CA" is capable of issuing certificates for server authentication, client authentication, code signing, and secure e-mail. However, you only want to trust certificates issued for the purpose of client authentication by "My CA". You can create a certificate trust list and limit the purpose for which you trust certificates issued by "My CA" so that they are only valid for client authentication. Any certificates issued for another purpose by "My CA" will not be accepted for use by any computer or user in the scope of the Group Policy object to which the certificate trust list is applied.

There can be multiple certificate trust lists in an organization. Since the uses and trusts of certificates for particular domains or organizational units may be different, you can create separate certificate trust lists to reflect these uses, and assign particular certificate trust lists to particular Group Policy objects.

### IP Security Policies on Active Directory

IPSec policies that are assigned to a Group Policy object in Active Directory become part of Group Policy, and are transferred to the member computers each time Group Policy propagates.

When assigning an IPSec policy in Active Directory, consider the following:

> *IPSec policies assigned to a domain policy will override any active, local IPSec policy only when that computer is connected to the domain.*
>
> *IPSec policies assigned to an organizational unit will override an IPSec policy assigned to the domain policy, for any member computers of that organizational unit. The IPSec policy assigned to the lowest-level organizational unit will override an IPSec policy assigned to a higher-level organizational unit, for any member computers of that organizational unit.*

Windows 2000 provides a set of predefined IPSec policies. By default, all predefined policies are designed for computers that are members of a Windows 2000 domain. They

may be assigned without further action, modified, or used as a template for defining custom policies. Each predefined policies comes with a set of predefined rules and predefined filter actions.

Predefined Rules: Like the predefined policies, the default response rule is provided for activation without further action or it may be modified to fit specific needs. It is added to each new policy you create, but not automatically activated. It is for any computers that do not require security, but must be able to appropriately respond when another computer requests secured communications.

Predefined Filter Actions: Like the predefined rules, these are provided for activation without further action, modification, or as a template for defining custom filter actions. They are available for activation in any new or existing rule:

> ***Require Security****. High security. Unsecured communication will not be allowed.*
>
> ***Request Security (Optional)****. Medium to low security. Unsecured communication is allowed, to enable communication with computers that do not or can not negotiate IPSec.*

The following three nodes are the predefined IPSec policies for Windows 2000:

- Client (Respond Only)
- Secure Server (Require Security)
- Server (Request Security).

*Client (Respond Only)*

This is used for computers which should not secure communications most of the time. For example, intranet clients may not require IPSec, except when requested by another computer. This policy enables the computer on which it is active to respond appropriately to requests for secured communications. The policy contains a default response rule, which enables negotiation with computers requesting IPSec. Only the requested protocol and port traffic for the communication is secured.

The following is the Predefined Rule for Client (Respond Only):

| IP Filter | Filter Action | Authentication | Tunnel Setting | Connection Type |
|---|---|---|---|---|
| Dynamic | Default Response | Kerberos | None | All |

Other default settings are:

> *Check for policy changes every 180 minutes. Minimum value is 0 minutes. Maximum value is 43,200 minutes.*
>
> ***Key Exchange Values***
>
> *Authenticate and generate a new key after every 480 minutes. Minimum value is 1 minute. Maximum value is 71,582,788 minutes.*
>
> *Authenticate and generate a new key after every 0 sessions. Minimum value is 0 sessions. Maximum value is 2,147,483,647 sessions.*

Default Settings for Security Methods are listed in the table below. Each security method defines the security requirements of any communications to which the associated rule applies. Creating multiple security methods increases the chance that a common method can be found between two computers.

The ISAKMP/Oakley service reads the list of security methods in descending order, and exchanges negotiation messages with the other peer until a common method is found.

| Type | Encryption | Integrity | Diffie-Hellman Group |
|---|---|---|---|
| IKE | 3DES | SHA1 | Medium(2) |
| IKE | 3DES | MD5 | Medium(2) |
| IKE | DES | SHA1 | Low(1) |
| IKE | DES | MD5 | Low(1) |

*Secure Server (Require Security)*

This is used for computers that always require secure communications. An example would be a server that transmits highly sensitive data, or a security gateway that protects the intranet from the outside. This policy rejects unsecured incoming communications, and outgoing traffic is always secured. Unsecured communication will not be allowed, even if a peer is not IPSec-enabled.

The following is the Predefined Rule for Secure Server (Require Security):

| IP Filter | Filter Action | Authentication | Tunnel Setting | Connection Type |
|---|---|---|---|---|
| All IP Traffic | Require Security | Kerberos | None | All |
| All ICMP Traffic | Permit | Kerberos | None | All |
| Dynamic | Default Response | Kerberos | None | All |

Other default settings are:

> *Check for policy changes every 180 minutes. Minimum value is 0. Maximum value is 43,200.*
>
> *Key Exchange Settings*
>
> *Authenticate and generate a new key after every 480 minutes. Minimum value is 1. Maximum value is 71,582,788.*
>
> *Authenticate and generate a new key after every 0 sessions. Minimum value is 0. Maximum value is 2,147,483,647*

Default Settings for Security Methods are listed in the table below. Each security method defines the security requirements of any communications to which the associated rule applies. Creating multiple security methods increases the chance that a common method can be found between two computers.

The ISAKMP/Oakley service reads the list of security methods in descending order, and exchanges negotiation messages with the other peer until a common method is found.

| Type | Encryption | Integrity | Diffie-Hellman Group |
|---|---|---|---|
| IKE | 3DES | SHA1 | Medium(2) |
| IKE | 3DES | MD5 | Medium(2) |
| IKE | DES | SHA1 | Low(1) |
| IKE | DES | MD5 | Low(1) |

*Server (Request Security)*

This is used for computers which should secure communications most of the time. An example would be servers that transmit sensitive data. In this policy, the computer accepts unsecured traffic, but always attempts to secure additional communications by requesting security from the original sender. This policy allows the entire communication to be unsecured if the other computer is not IPSec-enabled.

The following is the Predefined Rule for Secure Server (Request Security):

| IP Filter | Filter Action | Authentication | Tunnel Setting | Connection Type |
|---|---|---|---|---|
| All IP Traffic | Request Security (Optional) | Kerberos | None | All |
| All ICMP Traffic | Permit | Kerberos | None | All |
| Dynamic | Default Response | Kerberos | None | All |

Other default settings are:

> *Check for policy changes every 180 minutes. Minimum value is 0. Maximum value is 43,200.*
>
> *Key Exchange Settings*
>
> *Authenticate and generate a new key after every 480 minutes. Minimum value is 1. Maximum value is 71,582,788.*
>
> *Authenticate and generate a new key after every 0 sessions. Minimum value is 0. Maximum value is 2,147,483,647*

Default Settings for Security Methods are listed in the table below. Each security method defines the security requirements of any communications to which the associated rule applies. Creating multiple security methods increases the chance that a common method can be found between two computers.

The ISAKMP/Oakley service reads the list of security methods in descending order, and exchanges negotiation messages with the other peer until a common method is found.

| Type | Encryption | Integrity | Diffie-Hellman Group |
|---|---|---|---|
| IKE | 3DES | SHA1 | Medium(2) |
| IKE | 3DES | MD5 | Medium(2) |
| IKE | DES | SHA1 | Low(1) |
| IKE | DES | MD5 | Low(1) |

## Administrative Templates

Include registry-based Group Policy, used to mandate registry settings that govern the behavior and appearance of the desktop, including the operating system components and applications.

### Windows Components

#### NetMeeting

- Disable remote Desktop Sharing

> *Default Setting: Not configured*
>
> *Administrator may choose from among the following: Not Configured, Enabled, Disabled.*
>
> *Disables the remote desktop sharing feature of NetMeeting. Users will not be able to set it up or use it for controlling their computers remotely.*

#### Internet Explorer

- Security Zones: Use only machine settings

> *Default Setting: Not configured*
>
> *Administrator may choose from among the following: Not Configured, Enabled, Disabled.*
>
> *Applies security zone information to all users of the same computer. A security zone is a group of Web sites with the same security level*
>
> *If you enable this policy, changes that the user makes to a security zone will apply to all users of that computer.*
>
> *If you disable this policy or do not configure it, users of the same computer can establish their own security zone settings.*
>
> *This policy is intended to ensure that security zone settings apply uniformly to the same computer and do not vary from user to user.*
>
> *Also, see the "Security zones: Do not allow users to change policies" policy.*

- Security Zones: Do not allow users to change policies

> *Default Setting: Not configured*
>
> *Administrator may choose from among the following: Not Configured, Enabled, Disabled.*
>
> *Prevents users from changing security zone settings. A security zone is a group of Web sites with the same security level.*
>
> *If you enable this policy, the Custom Level button and security-level slider on the Security tab in the Internet Options dialog box are disabled.*
>
> *If you disable this policy or do not configure it, users can change the settings for security zones.*
>
> *This policy prevents users from changing security zone settings established by the administrator.*
>
> *Note: The "Disable the Security page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Security tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*
>
> *Also, see the "Security zones: Use only machine settings" policy.*

- Security Zones: Do not allow users to add/delete sites

> *Default Setting: Not configured*
>
> *Administrator may choose from among the following: Not Configured, Enabled, Disabled.*
>
> *Prevents users from adding or removing sites from security zones. A security zone is a group of Web sites with the same security level.*
>
> *If you enable this policy, the site management settings for security zones are disabled. (To see the site management settings for security zones, in the Internet Options dialog box, click the Security tab, and then click the Sites button.)*
>
> *If you disable this policy or do not configure it, users can add Web sites to or remove sites from the Trusted Sites and Restricted Sites zones, and alter settings for the Local Intranet zone.*
>
> *This policy prevents users from changing site management settings for security zones established by the administrator.*
>
> *Note: The "Disable the Security page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Security tab from the interface, takes precedence over this policy. If it is enabled, this policy is ignored.*
>
> *Also, see the "Security zones: Use only machine settings" policy.*

- Make proxy settings per-machine (rather than per-user)

> *Default Setting: Not Configured*
>
> *Administrator may choose from among the following: Not Configured, Enabled, Disabled.*
>
> *Applies proxy settings to all users of the same computer.*
>
> *If you enable this policy, users cannot set user-specific proxy settings. They must use the zones created for all users of the computer.*
>
> *If you disable this policy or do not configure it, users of the same computer can establish their own proxy settings.*

*This policy is intended to ensure that proxy settings apply uniformly to the same computer and do not vary from user to user.*

- Disable Automatic Install of Internet Explorer components

*Default Setting: Not configured*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents Internet Explorer from automatically installing components.*

*If you enable this policy, it prevents Internet Explorer from downloading a component when users browse to a Web site that needs that component.*

*If you disable this policy or do not configure it, users will be prompted to download and install a component when visiting a Web site that uses that component.*

*This policy is intended to help the administrator control which components the user installs.*

- Disable Periodic Check for Internet Explorer software updates

*Default Setting: Not configured*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents Internet Explorer from checking whether a new version of the browser is available.*

*If you enable this policy, it prevents Internet Explorer from checking to see whether it is the latest available browser version and notifying users if a new version is available.*

*If you disable this policy or do not configure it, Internet Explorer checks every 30 days by default, and then notifies users if a new version is available.*

*This policy is intended to help the administrator maintain version control for Internet Explorer by preventing users from being notified about new versions of the browser.*

- Disable software update shell notifications on program launch

*Default Setting: Not configured*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Specifies that programs using the Microsoft Software Distribution Channel will not notify users when they install new components. The Software Distribution Channel is a means of updating software dynamically on users' computers by using Open Software Distribution (.osd) technologies.*

*If you enable this policy, users will not be notified if their programs are updated using Software Distribution Channels.*

*If you disable this policy or do not configure it, users will be notified before their programs are updated.*

*This policy is intended for administrators who want to use Software Distribution Channels to update their users' programs without user intervention.*

- Disable showing the splash screen

*Default Setting: Not configured*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents the Internet Explorer splash screen from appearing when users start the browser.*

*If you enable this policy, the splash screen, which displays the program name, licensing, and copyright information, is not displayed.*

*If you disable this policy or do not configure it, the splash screen will be displayed when users start their browsers.*

### Task Scheduler

- Hide Property Pages

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents users from viewing and changing the properties of an existing task.*

*This policy removes the Properties item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview.*

*This policy prevents users from viewing and changing characteristics such as the program the task runs, its schedule details, idle time and power management settings, and its security context.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: This policy affects existing tasks only. To prevent users from changing the properties of newly created tasks, use the "Disable Advanced Menu" policy.*

- Prevent Task Run or End

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents users from starting and stopping tasks manually.*

*This policy removes the Run and End Task items from the context menu that appears when you right-click a task. As a result, users cannot start tasks manually or force tasks to end before they are finished.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Disable Drag-and-Drop

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder.*

*This policy disables the Cut, Copy, Paste, and Paste shortcut items on the context menu and the Edit menu in Scheduled Tasks. It also disables the drag-and-drop features of the Scheduled Tasks folder.*

*As a results, users cannot add new scheduled tasks by dragging, moving, or copying a document or program into the Scheduled tasks folder.*

*This policy does not prevent users from using other methods to create new tasks and it does not prevent users from deleting tasks.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Disable New Task Creation

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents users from creating new tasks.*

*This policy removes the Add Scheduled Task item that starts the New Task wizard. Also, the system does not respond when users try to move, paste, or drag programs or documents into the Scheduled Tasks folder.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Important: This policy does not prevent administrators of a computer from using At.exe to create new tasks or prevent administrators from submitting tasks from remote computers.*

- Disable Task Deletion

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents users from deleting tasks from the Scheduled Tasks folder.*

*This policy removes the Delete item from the Edit menu in the Scheduled Tasks folder and from the menu that appears when you right-click a task. Also, the system does not respond when users try to cut or drag a task from the Scheduled Tasks folder.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Important: This policy does not prevent administrators of a computer from using At.exe to delete tasks.*

- Disable Advanced Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Prevents users from viewing or changing the properties of newly created tasks.*

*This policy removes the "Open advanced properties for this task when I click Finish" item from the last page of the Scheduled Task wizard.*

*This policy prevents users from viewing and changing task characteristics, such as the program the task runs, details of its schedule, idle time and power management settings, and its security context. It is designed to simplify task creation for beginning users.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: This policy affects newly created tasks only. To prevent users from changing the properties of existing tasks, use the "Hide Property Pages" policy.*

- Prohibit Browse

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, Disabled.*

*Limits newly scheduled to items on the user's Start menu and prevents the user from changing the scheduled program for existing tasks.*

*This policy removes the Browse button from the Schedule Task wizard and from the Task tab of the properties dialog box for a task. Also, users cannot edit the "Run" box or the "Start in" box that determine the program and path for a task.*

*As a result, when users create a task, they must select a program from the list in the Scheduled Task wizard, which displays only the tasks that appear on the Start menu and its submenus. Once a task is created, users cannot change the program a task runs.*

*Important: This policy does not prevent users from creating a new task by pasting or dragging any program into the Scheduled Tasks folder. To prevent this action, use the "Disable Drag-and-Drop" policy.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

### Windows Installer

- Disable Windows Installer

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, default setting is: Never. The administrator may choose from among the following: Never, For non-managed apps only, and Always.*

*Disables or restricts the use of Windows Installer.*

*This policy can prevent users from installing software on their systems or permit users to install only those programs offered by a system administrator.*

*If you enable this policy, you can use the options in the Disable Windows Installer box to establish an installation policy.*

*-- The "Never" option indicates that Windows Installer is fully enabled. Users can install and upgrade software. Windows Installer is enabled by default on Windows 2000.*

*-- The "For non-managed apps only" option permits users to install only those programs that a system administrator assigns (offers on the desktop) or publishes (adds them to Add/Remove Programs).*

*-- The "Always" option indicates that Windows Installer is disabled.*

*This policy affects Windows Installer only. It does not prevent users from using other methods to install and upgrade programs.*

- Always install with elevated privileges

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*
>
> *When enabled, the default setting is Off. The administrator may force this setting to be On.*
>
> *Directs Windows Installer to use system permissions when it installs any program on the system.*
>
> *This policy extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add/Remove Programs in Control Panel. This policy lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.*
>
> *If you disable this policy or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.*
>
> *Note: This policy appears both in the Computer Configuration and User Configuration folders. To make this policy effective, you must enable the policy in both folders.*
>
> *Caution: Skilled users can take advantage of the permissions this policy grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this policy is not guaranteed to be secure.*

- Disable rollback

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*
>
> *When enabled, the default setting is: Off. The administrator may force this setting to be On.*
>
> *Prohibits Windows Installer from generating and saving the files it needs to reverse an interrupted or unsuccessful installation.*
>
> *This policy prevents Windows Installer from recording the original state of the system and sequence of changes it makes during installation. It also prevents Windows Installer from retaining files it intends to delete later. As a result, Windows installer cannot restore the computer to its original state if the installation does not complete.*
>
> *This policy is designed to reduce the amount of temporary disk space required to install programs. Also, it prevents malicious users from interrupting an installation to gather data about the internal state of the computer or to search secure system files. However, because an incomplete installation can render the system or a program inoperable, do not use this policy unless essential.*
>
> *This policy appears in the Computer Configuration and User Configuration folders. If the policy is enabled in either folder, it is considered be enabled, even if it is explicitly disabled in the other folder.*

- Disable browse dialog box for new source

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not Configured, Enabled, and Disabled*
>
> *When enabled, the default setting is: Off. The administrator may force this setting to be On..*

*Prevents users from searching for installation files when they add features or components to an installed program.*

*This policy disables the Browse button beside the Use feature from list in the Windows Installer dialog box. As a result, users must select an installation file source from the Use features from list that the system administrator configures.*

*This policy applies even when the installation is running in the user's security context.*

*If you disable this policy or do not configure it, the Browse button is enabled when an installation is running in the user's security context, but only system administrators can browse when an installation is running with elevated system privileges, such as installations offered on the desktop or in Add/Remove Programs.*

*This policy affects Windows Installer only. It does not prevent users from selecting other browsers, such Windows Explorer or My Network Places, to search for installation files.*

- Disable patching

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: Off. The administrator may force this setting to be On.*

*Prevents users from using Windows Installer to install patches.*

*Patches are updates or upgrades that replace only those program files that have changed. Because patches can be easy vehicles for malicious programs, some installations prohibit their use.*

*Note: This policy applies only to installations that run in the user's security context. By default, users who are not system administrators cannot apply patches to installations that run with elevated system privileges, such as those offered on the desktop or in Add/Remove Programs.*

*Also, see the "Enable user to patch elevated products" policy.*

- Disable IE security prompt for Windows Installer scripts

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: Off. The administrator may choose to force this setting to be On.*

*Allows Web-based programs to install software on the computer without notifying the user.*

*By default, when a script hosted by an Internet browser tries to install a program on the system, the system warns users and allows them to select or refuse the installation. This policy suppresses the warning and allows the installation to proceed.*

*This policy is designed for enterprises that use Web-based tools to distribute programs to their employees. However, because this policy can pose a security risk, it should be applied cautiously.*

- Enable user control over installs

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: Off. The administrator may choose to force this setting to be On.*

*Permits users to change installation options that typically are available only to system administrators.*

*This policy bypasses some of the security features of Windows Installer. It permits installations to complete that otherwise would be halted due to a security violation.*

*The security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user.*

*This policy is designed for less restrictive environments. It can be used to circumvent errors in an installation program that prevent software from being installed.*

- Enable user to browse for source while elevated

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: Off. The administrator may choose to force this setting to be On.*

*Allows users to search for installation files during privileged installations.*

*This policy enables the Browse button on the "Use feature from" dialog box. As a result, users can search for installation files, even when the installation program is running with elevated system privileges. By default, only system administrators can browse during installations with elevated privileges, such as installations offered on the desktop or displayed in Add/Remove Programs.*

*Because the installation is running with elevated system privileges, users can browse through directories that their own permissions would not allow.*

*This policy does not affect installations that run in the user's security context. Also, see the "Disable browse dialog box for new source" policy.*

- Enable user to use media source while elevated

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: Off. The administrator may choose to force this setting to be On.*

*Allows users to install programs from removable media, such as floppy disks and CD-ROMs, during privileged installations.*

*This policy permits all users to install programs from removable media, even when the installation program is running with elevated system privileges. By default, users can install programs from removable media only when the installation runs in the user's security context. During privileged installations, such as those offered on the desktop or displayed in Add/Remove Programs, only system administrators can install from removable media.*

*This policy does not affect installations that run in the user's security context. By default, users can install from removable media when the installation runs in their own security context.*

*Also, see the "Disable media source for any install" policy in User Configuration\Administrative Templates\Windows Components\Windows Installer.*

- Enable user to patch elevated products

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: Off. The administrator may choose to force this setting to be On.*

*Allows users to upgrade programs during privileged installations.*

*This policy permits all users to install patches, even when the installation program is running with elevated system privileges. Patches are updates or upgrades that replace only those program files that have changed. Because patches can easily be vehicles for malicious programs, some installations prohibit their use.*

*By default, only system administrators can apply patches during installations with elevated privileges, such as installations offered on the desktop or displayed in Add/Remove Programs.*

*This policy does not affect installations that run in the user's security context. By default, users can install patches to programs that run in their own security context. Also, see the "Disable patching" policy.*

- Allow admin to install from Terminal Services session

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: Off. The administrator may choose to force this setting to be On.*

*Allows Terminal Services administrators to install and configure programs remotely.*

*By default, system administrators can install programs only when system administrators are logged on to the computer on which the program is being installed. This policy creates a special exception for computers running Terminal Services.*

*This policy affects system administrators only. Other users cannot install programs remotely.*

- Cache transforms in secure location on workstation

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: Off. The administrator may choose to force this setting to be On.*

*Saves copies of transform files in a secure location on the local computer.*

*Transform files consist of instructions to modify or customize a program during installation. By default, Windows Installer stores transform files in the Application Data directory in the user's profile. When a user reinstalls, removes, or repairs an installation, the transform file is available, even if the user is on a different computer or isn't connected to the network.*

*If you enable this policy, the transform file is saved in a secure location on the user's computer instead of in the user profile. Because Windows Installer requires the transform file in order to repeat an installation in which the transform file was used, the user must be using the same*

*computer or be connected to the original or identical media to reinstall, remove, or repair the installation.*

*This policy is designed for enterprises that must take special precautions to prevent unauthorized or malicious editing of transform files.*

- Logging

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not Configured, Enabled, and Disabled.*

*When enabled, the default setting is: iweap. IWEARUCMPVO will log everything, but adds time to the install.*

*- I: Status messages*

*- W: Non-fatal warnings*

*- E: All error messages*

*- A: Start up of actions*

*- R: Action-specific records*

*- U: User requests*

*- C: Initial parameters*

*- M: Out-of-memory*

*- P: Terminal properties*

*- V: Verbose output*

*- 0: Out of disk space messages*

*Specifies the types of events that Windows Installer records in its transaction log for each installation. The log, Msi.log, appears in the Temp directory of the system volume.*

*When you enable this policy, you can specify the types of events you want Windows Installer to record. To indicate that an event type is recorded, type the letter representing the event type. You can type the letters in any order and list as many or as few event types as you desire.*

*To disable logging, delete all of the letters from the box.*

*If you disable this policy or do not configure it, Windows Installer logs the default event types, represented by the letters "iweap."*

## System

- Remove Security option from Start Menu (Terminal Services Only)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Windows Security item from the Settings menu on Terminal Services clients.*

*If you enable this policy, the Windows Security item does not appear in Settings menu on the Start menu. As a result, users must type a security attention sequence, such as Ctrl+Alt+End, to open the Windows Security dialog box on a Terminal Services client.*

*This policy is designed to prevent inexperienced users from logging on to Terminal Services inadvertently.*

- Remove Disconnect item from Start Menu (Terminal Services Only)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Disconnect item from the Shut Down Windows dialog box on Terminal Services clients.*

*If you enable this policy, the Disconnect item does not appear in the drop-down list of options in the Shut Down Windows dialog box. As a result, Terminal Services users cannot use this familiar method to disconnect their client from a Terminal Services server.*

*This policy affects the Shut Down Windows dialog box only. It does not prevent users from using other methods of disconnecting from a Terminal Services server.*

- Disable Boot/Shutdown/Logon/Logoff status messages

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Suppresses system status messages.*

*If you enable this policy, the system does not display a message reminding users to wait while their system starts or shuts down, or while users log on or off.*

- Verbose vs normal status messages

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Directs the system to display highly detailed status messages.*

*If you enable this policy, the system displays status message that reflect each step in the process of starting, shutting down, logging on or logging off the system.*

*This policy is designed for sophisticated users that require this information.*

*Note: This policy is ignored if the "Disable Boot / Shutdown / Logon / Logoff status messages" policy is enabled.*

- Disable Autoplay

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: CD-ROM drives.*

*The administrator may choose from among the following: CD-ROM drives or All drives.*

*Disables the Autoplay feature.*

*Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media starts immediately.*

*By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.*

*If you enable this policy, you can also disable Autoplay on CD-ROM drives, or disable Autoplay on all drives.*

*This policy disables Autoplay on additional types of drives. You cannot use this policy to enable Autoplay on drives on which it is disabled by default.*

*Note: This policy appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Don't display welcome screen at logon

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Suppresses the "Getting Started with Windows 2000" welcome screen.*

*This policy hides the welcome screen that is displayed on Windows 2000 Professional each time the user logs on.*

*Users can still display the "Getting Started with Windows 2000" welcome screen by selecting it from the Start menu or by typing "Welcome" in the Run dialog box.*

*This policy applies only to Windows 2000 Professional. It does not affect the "Configure Your Server on a Windows 2000 Server" screen on Windows 2000 Server.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To display the welcome screen, click Start, point to Programs, point to Accessories, point to System Tools, and then click "Getting Started." To suppress the welcome screen without setting a policy, clear the "Show this screen at startup" check box on the welcome screen.*

- Run these programs at user logon

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may browse for the program.*

*Specifies additional programs or documents that Windows starts automatically when a user logs on to the system.*

*To use this policy, click Show, click Add and, in the text box, type the name of the executable program (.exe) file or document file. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the system starts the programs specified in the Computer Configuration policy just before it starts the programs specified in the User Configuration policy.*

*Also, see the "Disable legacy run list" and the "Disable the run once list" policies.*

- Disable the run once list

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Ignores customized run-once lists.*

*You can create a customized list of additional programs and documents that are started automatically the next time the system starts (but not thereafter). These programs are added to the standard list of programs and services that the system starts.*

*If you enable this policy, the system ignores the run-once list.*

*If you disable this policy, or do not configure it, the system runs the programs in the run-once list.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: Customized run-once lists are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce.*

*Also, see the "Disable legacy run list" policy.*

- Disable legacy run list

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Ignores the customized run list for Windows NT 4.0 and earlier.*

*On Windows 2000 and Windows NT 4.0 and earlier, you can create a customized list of additional programs and documents that the system starts automatically when it starts. These programs are added to the standard run list of programs and services that the system starts.*

*If you disable this policy, or do not configure it, Windows 2000 adds any customized run list configured for Windows NT 4.0 and earlier to its run list.*

*If you enable this policy, the system ignores the run list for Windows NT 4.0 and earlier.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To create a customized run list by using a policy, use the "Run these applications at startup" policy.*

*The customized run lists for Windows NT 4.0 and earlier are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run and HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run. They can be configured by using the "Run" policy in System Policy Editor for Windows NT 4.0 and earlier.*

*Also, see the "Disable the run once list" policy.*

- Do not automatically encrypt files moved to encrypted folders

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents Windows Explorer from encrypting files that are moved to an encrypted folder.*

*If you disable this policy or do not configure it, Windows Explorer automatically encrypts files that are moved to an encrypted folder.*

*This policy applies only to files moved within a volume. When files are moved to other volumes, or if you create a new file in an encrypted folder, Windows Explorer encrypts those files automatically.*

- Download missing COM components

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Directs the system to search Active Directory for missing Component Object Model (COM) components that a program requires.*
>
> *Many Windows programs, such as the MMC snap-ins, use the interfaces provided by the COM. These programs cannot perform all of their functions unless Windows 2000 has internally registered the required components.*
>
> *If you enable this policy and a component registration is missing, the system searches for it in Active Directory and if it is found, downloads it. The resulting searches might make some programs start or run slowly.*
>
> *If you disable this policy or do not configure it, the program continues without the registration. As a result, the program might not perform all of its functions, or it might stop.*
>
> *This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

### Logon

- Run logon scripts synchronously

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Directs the system to wait for the logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop.*
>
> *If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.*
>
> *If you disable this policy or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously.*
>
> *This policy appears in the Computer Configuration and User Configuration folders. The policy set in Computer Configuration takes precedence over the policy set in User Configuration.*

- Run startup scripts asynchronously

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Lets the system run startup scripts simultaneously.*
>
> *Startup scripts are batch files that run before the user is invited to log on. By default, the system waits for each startup script to complete before it runs the next startup script.*
>
> *If you enable this policy, the system does not coordinate the running of startup scripts. As a result, startup scripts can run simultaneously.*

*If you disable this policy or do not configure it, a startup cannot run until the previous script is complete.*

- Run startup scripts visible

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Displays the instructions in startup scripts as they run.*

*Startup scripts are batch files of instructions that run before the user is invited to log on. By default, the system does not display the instructions in the startup script.*

*If you enable this policy, the system displays each instruction in the startup script as it runs. The instructions appear in a command window. This setting is designed for advanced users.*

*If you disable this policy or do not configure it, the instructions are suppressed.*

- Run shutdown scripts visible

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Displays the instructions in shutdown scripts as they run.*

*Shutdown scripts are batch files of instructions that run when the user restarts the system or shuts it down. By default, the system does not display the instructions in the shutdown script.*

*If you enable this policy, the system displays each instruction in the shutdown script as it runs. The instructions appear in a command window.*

*If you disable this policy or do not configure it, the instructions are suppressed.*

- Maximum wait time for Group Policy scripts

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 600 seconds. Minimum value is 0, use 0 for infinite wait time. Maximum value is 32,000.*

*Determines how long the system waits for scripts applied by Group Policy to run.*

*This policy limits the total time allowed for all logon, startup, and shutdown scripts applied by Group Policy to finish running. If the scripts have not finished running when the specified time expires, the system stops script processing and records an error event.*

*By default, the system lets the combined set of scripts run for up to 600 seconds (10 minutes), but you can use this policy to adjust this interval.*

*To use this policy, in the Seconds box, type a number from 1 to 32,000 for the number of seconds you want the system to wait for the set of scripts to finish. To direct the system to wait until the scripts have finished, no matter how long they take, type 0.*

*This interval is particularly important when other system tasks must wait while the scripts complete. By default, each startup script must complete before the next one runs. Also, you can use the "Run logon scripts synchronously" policy to direct the system to wait for the logon scripts to complete before loading the desktop.*

*An excessively long interval can delay the system and inconvenience users. However, if the interval is too short, prerequisite tasks might not be done, and the system can appear to be ready prematurely.*

- Delete cached copies of roaming profiles

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether the system saves a copy of a user's roaming profile on the local computer's hard drive when the user logs off.*

*This policy, and related policies in this folder, together describe a strategy for managing user profiles residing on remote servers. In particular, they tell the system how to respond when a remote profile is slow to load.*

*Roaming profiles reside on a network server. By default, when users with roaming profiles log off, the system also saves a copy of their roaming profile on the hard drive of the computer they are using in case the server that stores the roaming profile is unavailable when the user logs on again. The local copy is also used when the remote copy of the roaming user profile is slow to load.*

*If you enable this policy, any local copies of the user's roaming profile are deleted when the user logs off. The roaming profile still remains on the network server that stores it.*

*Important: Do not enable this policy if you are using the slow link detection feature of Windows 2000. To respond to a slow link, the system requires a local copy of the user's roaming profile.*

- Do not detect slow network connections

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the slow link detection feature.*

*Slow link detection measures the speed of the connection between a user's computer and the remote server that stores the roaming user profile. When the system detects a slow link, the related policies in this folder tell the system how to respond.*

*If you enable this policy, the system does not detect slow connections or recognize any connections as being slow. As a result, the system does not respond to slow connections to user profiles and it ignores the policies that tell the system how to respond to a slow connection.*

*If you disable this policy or do not configure it, slow link detection is enabled. The system measures the speed of the connection between the user's computer and profile server. If the connection is slow (as defined by the "Slow network connection timeout for user profiles" policy), the system applies the other policies set in this folder to determine how to proceed. By default, when the connection is slow, the system loads the local copy of the user profile.*

- Slow network connection timeout for user profiles

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting for connection is: 500 Kbps for Connections speed. Connections below this speed are considered slow. Minimum value is 0. Maximum value is 967,196*

*Default setting for time is: 120 milliseconds for time.*

*Defines a slow connection for roaming user profiles.*

*If the server on which the user's roaming user profile resides takes longer to respond than the thresholds set by this policy allow, then the system considers the connection to the profile to be slow.*

*This policy and related policies in this folder together define the system's response when roaming user profiles are slow to load.*

*This policy establishes thresholds for two tests. For computers connected to IP networks, the system measures the rate at which the remote server returns data in response to an IP ping message. To set a threshold for this test, in the Connection speed box, type a decimal number between 0 and 4,294,967,200, representing the minimum acceptable transfer rate in kilobits per second. By default, if the server returns fewer than 500 kilobits of data per second, it is considered to be slow.*

*For non-IP computers, the system measures the responsiveness of the remote server's file system. To set a threshold for this test, in the Time box, type a decimal number between 0 and 20,000, representing the maximum acceptable delay, in milliseconds. By default, if the server's file system does not respond within 120 milliseconds, it is considered to be slow.*

*Consider increasing this value for clients using DHCP Service-assigned addresses or for computers accessing profiles across dial-up connections.*

*Important: If the "Do not detect slow network connections" policy is enabled, this policy is ignored. Also, if the "Delete cached copies of roaming profiles" policy is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection.*

- Wait for remote user profile

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Directs the system to wait for the remote copy of the roaming user profile to load, even when loading is slow. Also, the system waits for the remote copy when the user is notified about a slow connection, but does not respond in the time allowed.*

*This policy and related policies in this folder together define the system's response when roaming user profiles are slow to load.*

*If you disable this policy or do not configure it, then when a remote profile is slow to load, the system loads the local copy of the roaming user profile. The local copy is also used when the user is consulted (as set in the "Prompt user when slow link is detected" policy), but does not respond in the time allowed (as set in the "Timeout for dialog boxes" policy).*

*Waiting for the remote profile is appropriate when users move between computers frequently and the local copy of their profile is not always current. Using the local copy is desirable when quick logging on is a priority.*

*Important: If the "Do not detect slow network connections" policy is enabled, this policy is ignored. Also, if the "Delete cached copies of roaming profiles" policy is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection.*

- Prompt user when slow link is detected

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Notifies users when their roaming profile is slow to load. The notice lets users decide whether to use a local copy or to wait for the roaming user profile.*

*If you disable this policy or do not configure it, when a roaming user profile is slow to load, the system does not consult the user. Instead, it loads the local copy of the profile. If you have enabled the "Wait for remote user profile" policy, then the system loads the remote copy without consulting the user.*

*This policy and related policies in this folder together define the system's response when roaming user profiles are slow to load.*

*To adjust the time within which the user must respond to this notice, use the "Timeout for dialog boxes" policy.*

*Important: If the "Do not detect slow network connections" policy is enabled, this policy is ignored. Also, if the "Delete cached copies of roaming profiles" policy is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection.*

- Timeout for dialog boxes

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 30 seconds.*

*Determines how long the system waits for a user response before it uses a default value.*

*The default value is applied when the user does not respond to messages explaining that any of the following events has occurred:*

*-- The system detects a slow connection between the user's computer and the server that stores users' roaming user profiles.*

*-- The system cannot access users' server-based profiles when users log on or off.*

*-- Users' local profiles are newer than their server-based profiles.*

*You can use this policy to override the system's default value of 30 seconds. To use this policy, type a decimal number between 0 and 600 for the length of the interval.*

- Log users off when roaming profile fails

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Logs a user off automatically when the system cannot load the user's roaming user profile.*

*This policy is used when the system cannot find the roaming user profile or the profile contains errors which prevent it from loading correctly.*

*If you disable this policy or do not configure it, when the roaming profile fails, the system loads a local copy of the roaming user profile, if one is available. Otherwise, the system loads the default user profile (stored in %Systemroot%\Documents and Settings\Default User).*

*Also, see the "Delete cached copies of roaming profiles" policy.*

- Maximum retries to unload and update user profile

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 60 retries.*

*Determines how many times the system tries to unload and update the registry portion of a user profile. When the number of trials specified by this policy is exhausted, the system stops trying. As a result, the user profile might not be current, and local and roaming user profiles might not match.*

*When a user logs off of the computer, the system unloads the user-specific section of the registry (HKEY_CURRENT_USER) into a file (NTUSER.DAT) and updates it. However, if another program or service is reading or editing the registry, the system cannot unload it. The system tries repeatedly (at a rate of once per second) to unload and update the registry settings. By default, the system repeats its periodic attempts 60 times (over the course of one minute).*

*If you enable this policy, you can adjust the number of times the system tries to unload and update the user's registry settings. (You cannot adjust the retry rate.)*

*If you disable this policy or do not configure it, the system repeats its attempt 60 times.*

*If you set the number of retries to 0, the system tries just once to unload and update the user's registry settings. It does not try again.*

*Note: This policy is particularly important to servers running Terminal Services. Because Terminal Services edits the user's registry settings when they log off, the system's first few attempts to unload the user settings are more likely to fail.*

*This policy does not affect the system's attempts to update the files in the user profile.*

*Tip: Consider increasing the number of retries specified in this policy if there are many user profiles stored in the computer's memory. This indicates that the system has not been able to unload the profile.*

*Also, check the Application Log in Event Viewer for events generated by Userenv. The system records an event whenever it tries to unload the registry portion of the user profile. The system also records an event when it fails to update the files in a user profile.*

### Disk Quotas

- Enable disk quotas

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Enables and disables disk quota management on all NTFS volumes of the computer, and prevents users from changing the setting.*

*If you enable this policy, disk quota management is enabled, and users cannot disable it.*

*If you disable the policy, disk quota management is disabled, and users cannot enable it.*

*If this policy is not configured, disk quota management is disabled by default, but administrators can enable it.*

*To prevent users from changing the setting while a policy is in effect, the system disables the "Enable quota management" option on the Quota tab of NTFS volumes.*

*Note: This policy enables disk quota management but does not establish or enforce a particular disk quota limit. To specify a disk quota limit, use the "Default quota limit and warning level" policy. Otherwise, the system uses the physical space on the volume as the quota limit.*

*Tip: To enable or disable disk quota management without setting a policy, in My Computer, right-click the name of an NTFS volume, click Properties, click the Quota tab, and then click the "Enable quota management" option.*

- Enforce disk quota limit

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Determines whether disk quota limits are enforced and prevents users from changing the setting.*
>
> *If you enable this policy, disk quota limits are enforced. If you disable this policy, disk quota limits are not enforced. When you enable or disable the policy, the system disables the "Deny disk space to users exceeding quota limit" option on the Quota tab so administrators cannot change the setting while a policy is in effect.*
>
> *If the policy is not configured, the disk quota limit is not enforced by default, but administrators change the setting.*
>
> *Enforcement is optional. When users reach an enforced disk quota limit, the system responds as though the physical space on the volume were exhausted. When users reach an unenforced limit, their status in the Quota Entries window changes, but they can continue to write to the volume as long as physical space is available.*
>
> *Note: This policy overrides user settings that enable or disable quota enforcement on their volumes.*
>
> *Tip: To specify a disk quota limit, use the "Default quota limit and warning level" policy. Otherwise, the system uses the physical space on the volume as the quota limit.*

- Default quota limit and warning level

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the default setting is: 100 MB. Default warning level is 100 MB*
>
> *Specifies the default disk quota limit and warning level for new users of the volume.*
>
> *This policy determines how much disk space can be used by each user on each of the NTFS file system volumes on a computer. It also specifies the warning level, the point at which the user's status in the Quota Entries window changes to indicate that the user is approaching the disk quota limit.*
>
> *This policy overrides new users' settings for the disk quota limit and warning level on their volumes, and it disables the corresponding options in the "Select the default quota limit for new users of this volume" section on the Quota tab.*
>
> *This policy applies to all new users as soon as they write to the volume. It does not affect disk quota limits for current users or affect customized limits and warning levels set for particular users (on the Quota tab in Volume Properties).*
>
> *If you disable this policy or do not configure it, the disk space available to users is not limited. The disk quota management feature uses the physical space on each volume as its quota limit and warning level.*
>
> *When you select a limit, remember that the same limit applies to all users on all volumes, regardless of actual volume size. Be sure to set the limit and warning level so that it is reasonable for the range of volumes in the group.*
>
> *This policy is effective only when disk quota management is enabled on the volume. Also, if disk quotas are not enforced, users can exceed the quota limit you set. When users reach the quota limit, their status in the Quota Entries window changes, but users can continue to write to the volume.*

- Log event when quota limit exceeded

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Determines whether the system records an event in the local Application log when users reach their disk quota limit on a volume, and prevents users from changing the logging setting.*
>
> *If you enable this policy, the system records an event when the user reaches their limit. If you disable this policy, no event is recorded. Also, when you enable or disable this policy, the system disables the "Log event when a user exceeds their quota limit" option on the Quota tab so adminstrators cannot change the setting while a policy is in effect.*
>
> *If the policy is not configured, no events are recorded, but administrators can use the Quota tab option to change the setting.*
>
> *This policy is independent of the enforcement policies for disk quotas. As a result, you can direct the system to log an event regardless of whether or not you choose to enforce the disk quota limit.*
>
> *Also, this policy does not affect the Quota Entries window on the Quota tab. Even without the logged event, users can detect that they have reached their limit because their status in the Quota Entries window changes.*
>
> *Tip: To find the logging option, in My Computer, right-click the name of an NTFS file system volume, click Properties, and then click the Quota tab.*

- Log event when quota warning level exceeded

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Determines whether the system records an event in the Application log when users reach their disk quota warning level on a volume.*
>
> *If you enable this policy, the system records an event. If you disable this policy, no event is recorded. When you enable or disable the policy, the system disables the corresponding "Log event when a user exceeds their warning level" option on the Quota tab, so that administrators cannot change the logging setting while a policy is in effect.*
>
> *If the policy is not configured, no event is recorded, but administrators can use the Quota tab option to change the logging setting.*
>
> *This policy does not affect the Quota Entries window on the Quota tab. Even without the logged event, users can detect that they have reached their warning level because their status in the Quota Entries window changes.*
>
> *Tip: To find the logging option, in My Computer, right-click the name of an NTFS file system volume, click Properties, and then click the Quota tab.*

- Apply policy to removable media

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Extends the disk quota policies in this folder to NTFS file system volumes on removable media.*
>
> *If you disable this policy or do not configure it, the disk quota policies established in this folder apply to fixed-media NTFS volumes only.*

## DNS Client

- Primary DNS Suffix

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the administrator may enter a primary DNS suffix.*
>
> *Specifies the primary Domain Name System (DNS) suffix for all affected computers. The primary DNS suffix is used in DNS name registration and DNS name resolution.*
>
> *This policy lets you specify a primary DNS suffix for a group of computers, and prevents users, including administrators, from changing it.*
>
> *If you disable this policy or do not configure it, each computer uses its local primary DNS suffix, which is usually the DNS name of Active Directory domain to which it is joined. However, administrators can use System in Control Panel to change the primary DNS suffix of a computer.*
>
> *To use this policy, in the text box provided, type the entire primary DNS suffix you want to assign. For example, microsoft.com.*
>
> *This policy does not disable the DNS Suffix and NetBIOS Computer Name dialog box that administrators use to change the primary DNS suffix of a computer. However, if administrators enter a suffix, that suffix is ignored while this policy is enabled.*
>
> *Important: To make changes to this policy effective, you must restart Windows 2000 on all computers affected by the policy.*
>
> *Note: This policy has no effect on domain controllers.*
>
> *Tip: To change the primary DNS suffix of a computer without setting a policy, click System in Control Panel, click the Network Identification tab, click Properties, click More, and then enter a suffix in the "Primary DNS suffix of this computer" box.*
>
> *For more information about DNS, see "Domain Name System (DNS)" in Windows 2000 Help.*

## Group Policy

- Apply Group Policy for computers asynchronously during startup

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Lets the system display the logon prompt before it finishes updating computer Group Policy.*
>
> *If you enable this policy, the system does not wait for Group Policy updates to complete before inviting the user to log on. As a result, the Windows interface might appear to be ready before computer Group Policy is applied.*
>
> *If you disable this policy or do not configure it, users cannot log on until computer Group Policy is updated.*
>
> *Also, see the "Apply Group Policy for users asynchronously during logon" policy.*

- Apply Group Policy for users asynchronously during logon

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Lets the system display the Windows desktop before it finishes updating user Group Policy.*

*If you enable this policy, the system does not coordinate the tasks of loading desktop and updating user Group Policy. As a result, Windows might appear ready for use before user Group Policy is updated.*

*If you disable this policy or do not configure it, the system does not make the desktop available to users until user Group Policy is updated.*

*Also, see the "Apply Group Policy for computers asynchronously during startup" policy.*

- Disable background refresh of Group Policy

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents Group Policy from being updated while the computer is in use. This policy applies to Group Policies for computers, users, and domain controllers.*

*If you enable this policy, the system waits until the current user logs off the system before updating the computer and user policies.*

*If you disable this policy, updates can be applied while users are working. The frequency of updates is determined by the "Group Policy refresh interval for computers" and "Group Policy refresh interval for users" policies.*

- Disk Quota policy processing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following:*

*- Allow processing across a slow network connection*

*- Do not apply during periodic background processing*

*- Process even if the Group Policy objects have not changed*

*- Determines when disk quota policies are updated.*

*This policy affects all policies that use the disk quota component of Group Policy, such as those in Computer Configuration\Administrative Templates\System\File System\Disk Quotas.*

*It overrides customized settings that the program implementing the disk quota policy set when it was installed.*

*If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*

*The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.*

*The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.*

*The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- EFS recovery policy processing

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the administrator may choose from among the following:*
>
> *Allow processing across a slow network connection*
>
> *Do not apply during periodic background processing*
>
> *Process even if the Group Policy objects have not changed*
>
> *Determines when encryption polices are updated.*
>
> *This policy affects all policies that use the encryption component of Group Policy, such as policies related to encryption in Windows Settings\Security Settings.*
>
> *It overrides customized settings that the program implementing the encryption policy set when it was installed.*
>
> *If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*
>
> *The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.*
>
> *The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.*
>
> *The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- Folder Redirection policy processing

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the administrator may choose from among the following:*
>
> *Allow processing across a slow network connection*
>
> *Process even if the Group Policy objects have not changed*
>
> *Determines when folder redirection policies are updated.*
>
> *This policy affects all policies that use the folder redirection component of Group Policy, such as those in WindowsSettings\Folder Redirection. You can only set folder redirection policy for Group Policy objects, stored in Active Directory, not for Group Policy objects on the local computer.*
>
> *This policy overrides customized settings that the program implementing the folder redirection policy set when it was installed.*
>
> *If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*

*The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.*

*The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- Group Policy refresh interval for computers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 90 minutes. The range is from 0 to 64800 minutes (45 days).*

*The default setting for random time added to the refresh interval to prevent all client from requesting Group Policy at the same time is: 30 minutes. The range is from 0 to 1440 minutes (24 hours).*

*Specifies how often Group Policy for computers is updated while the computer is in use (in the background). This policy specifies a background update rate only for Group Policies in the Computer Configuration folder.*

*In addition to background updates, Group Policy for the computer is always updated when the system starts.*

*By default, computer Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes.*

*You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.*

*If you disable this policy, Group Policy is updated every 90 minutes (the default). To specify that Group Policy should never be updated while the computer is in use, select the "Disable background refresh of Group Policy" policy.*

*The Group Policy refresh interval for computers policy also lets you specify how much the actual update interval varies. To prevent clients with the same update interval from requesting updates simultaneously, the system varies the update interval for each client by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that client requests overlap. However, updates might be delayed significantly.*

*This policy establishes the update rate for computer Group Policy. To set an update rate for user policies, use the "Group Policy refresh interval for users" policy (located in User Configuration\Administrative Templates\System\Group Policy).*

*This policy is only used when the "Disable background refresh of Group Policy" policy is not enabled.*

*Note: Consider notifying users that their policy is updated periodically so that they recognize the signs of a policy update. When Group Policy is updated, the Windows desktop is refreshed; it flickers briefly and closes open menus. Also, restrictions imposed by Group Policies, such as those that limit the programs users can run, might interfere with tasks in progress.*

- Group Policy refresh interval for domain controllers

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the default setting is: 5 minutes. The range is from 0 to 64800 minutes (45 days).*
>
> *The default setting for random time added to the refresh interval to prevent all client from requesting Group Policy at the same time is: 0 minutes. The range is from 0 to 1440 minutes (24 hours).*
>
> *Specifies how often Group Policy is updated on domain controllers while they are running (in the background). The updates specified by this policy occur in addition to updates performed when the system starts.*
>
> *By default, Group Policy on the domain controllers is updated every five minutes.*
>
> *You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the domain controller tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.*
>
> *If you disable this policy, the domain controller updates Group Policy every 5 minutes (the default). To specify that Group Policies for users should never be updated while the computer is in use, select the "Disable background refresh of Group Policy" policy.*
>
> *This policy also lets you specify how much the actual update interval varies. To prevent domain controllers with the same update interval from requesting updates simultaneously, the system varies the update interval for each controller by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that update requests overlap. However, updates might be delayed significantly.*
>
> *Note: This policy is used only when you are establishing policy for a domain, site, organizational unit (OU), or customized group. If you are establishing policy for a local computer only, the system ignores this policy.*

- Group Policy slow link detection

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the default setting is: 500 Kbps. Connections below this speed are considered slow. Enter 0 to disable slow link detection.*
>
> *Defines a slow connection for purposes of applying and updating Group Policy.*
>
> *If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this policy, the system considers the connection to be slow.*
>
> *The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, the policy processing policies in this folder let you override the programs' specified responses to slow links.*
>
> *To use this policy, in the "Connection speed" box, type a decimal number between 0 and 4,294,967,200 (0xFFFFFFA0), indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast.*

*If you disable this policy or do not configure it, the system uses the default value of 500 kilobits per second.*

*This policy appears in the Computer Configuration and User Configuration folders. The policy in Computer Configuration defines a slow link for policies in the Computer Configuration folder. The policy in User Configuration defines a slow link for policies in the User Configuration folder.*

*Also, see the "Automatically detect slow network connections" and related policies in Computer Configuration\Administrative Templates\System\Logon.*

- IP Security policy processing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following:*

*- Allow processing across a slow network connection*

*- Do not apply during periodic background processing*

*- Process even if the Group Policy objects have not changed*

*- Determines when IP security polices are updated.*

*This policy affects all policies that use the IP security component of Group Policy, such as policies in Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Local Machine.*

*It overrides customized settings that the program implementing the IP security policy set when it was installed.*

*If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*

*The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.*

*The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.*

*The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- Internet Explorer Maintenance policy processing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following:*

*- Allow processing across a slow network connection*

*- Do not apply during periodic background processing*

*- Process even if the Group Policy objects have not changed*

*Determines when Internet Explorer Maintenance policies are updated.*

*This policy affects all policies that use the Internet Explorer Maintenance component of Group Policy, such as those in Windows Settings\Internet Explorer Maintenance.*

*It overrides customized settings that the program implementing the Internet Explorer Maintenance policy set when it was installed.*

*If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*

*The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.*

*The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.*

*The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- Registry policy processing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following:*

*- Do not apply during periodic background processing*

*- Process even if the Group Policy objects have not changed*

*- Determines when registry policies are updated.*

*This policy affects all policies in the Administrative Templates folder and any other policies that store values in the registry.*

*It overrides customized settings that the program implementing a registry policy set when it was installed.*

*If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*

*The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.*

*The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- Scripts policy processing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following:*

*Allow processing across a slow network connection*

*Do not apply during periodic background processing*

*Process even if the Group Policy objects have not changed*

*Determines when policies that assign shared scripts are updated.*

*This policy affects all policies that use the scripts component of Group Policy, such as those in WindowsSettings\Scripts.*

*It overrides customized settings that the program implementing the scripts policy set when it was installed.*

*If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*

*The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.*

*The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.*

*The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- Security policy processing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from the following:*

*- Do not apply during periodic background processing*

*- Process even if the Group Policy objects have not changed*

*Determines when security policies are updated.*

*This policy affects all policies that use the security component of Group Policy, such as those in Windows Settings\Security Settings.*

*It overrides customized settings that the program implementing the security policy set when it was installed.*

*If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*

*The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.*

*The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.*

*The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that*

*they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- Software Installation policy processing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following:*

*- Allow processing across a slow network connection*

*- Process even if the Group Policy objects have not changed*

*Determines when software installation polices are updated.*

*This policy affects all policies that use the software installation component of Group Policy, such as policies in Software Settings\Software Installation. You can set software installation policy only for Group Policy objects stored in Active Directory, not for Group Policy objects on the local computer.*

*This policy overrides customized settings that the program implementing the software installation policy set when it was installed.*

*If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.*

*The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.*

*The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.*

- User Group Policy loopback processing mode

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: Replace. The administrator may choose from among the following: Replace or Merge*

*Applies alternate user policies when a user logs on to a computer affected by this policy.*

*This policy directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this policy. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user policy based on the computer that is being used.*

*By default, the user's Group Policy objects determine which user policies apply. If this policy is enabled, then, when a user logs on to this computer, the computer's Group Policy objects determine which set of Group Policy objects applies.*

*To use this policy, select one of the following policy modes from the Mode box:*

*-- "Replace" indicates that the user policies defined in the computer's Group Policy objects replace the user policies normally applied to the user.*

*-- "Merge" indicates that the user policies defined in the computer's Group Policy objects and the user policies normally applied to the user are combined. If the policy settings conflict, the*

*user policies in the computer's Group Policy objects take precedence over the user's normal policies.*

*If you disable this policy or do not configure it, the user's Group Policy objects determines which user policies apply.*

*Note: This policy is effective only when both the computer account and the user account are in Windows 2000 domains.*

### Windows File Protection

- Hide the file scan progress window

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Hides the file scan progress window.*

*This window provides status information to sophisticated users, but might confuse novices.*

*If you enable this policy, the file scan window does not appear during file scanning.*

*If you disable this policy or do not configure it, the file scan progress window appears.*

- Limit Windows File Protection cache size

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 50 MB. Maximum value is 4,294,967,295.*

*Specifies the maximum amount of disk space that can be used for the Windows File Protection file cache.*

*Windows File Protection adds protected files to the cache until the cache content reaches the quota. If the quota is greater than 50 MB, WFP adds other important Windows 2000 files to the cache until the cache size reaches the quota.*

*To use this policy, enable the policy, and enter the maximum amount of disk space to be used (in MB). To indicate that the cache size is unlimited, select "4294967295" as the maximum amount of disk space.*

*If you disable this policy or do not configure it, the default value is set to 50 MB on Windows 2000 Professional and is unlimited (4294967295 MB) on Windows 2000 Server.*

- Set Windows File Protection scanning

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: Do not scan during startup. The administrator may choose from among the following:*

*Do not scan during startup*

*Scan during startup*

*Scan once*

*Determines when Windows File Protection scans protected files. This policy directs Windows File Protection to enumerate and scan all system files for changes.*

*You can use this policy to direct Windows File Protection to scan files more often. By default, files are scanned only during setup.*

*To use this policy, enable the policy and select a rate from the "Scanning Frequency" box.*

*-- "Do not scan during startup," the default, scans files only during setup.*

*-- "Scan during startup" also scans files each time you start Windows 2000. This setting delays each startup.*

*-- "Scan once" scans files the next time you start the system.*

*Note: This policy affects file scanning only. It does not affect the standard background file change detection that Windows File Protection provides.*

- Specify Windows File Protection cache location

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may enter the cache file path.*

*Specifies an alternate location for the Windows File Protection cache.*

*To use the policy, enable the policy, and enter the fully qualified local path to the new location in the "Cache file path" box.*

*If you disable this policy or do not configure it, the Windows File Protection cache is located in the %Systemroot%\System32\Dllcache directory.*

*Note: Do not put the cache on a network shared directory.*

## Network

### Offline Files

- Action on server disconnect

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, .the administrator specifies how the system is to respond when a network server becomes unavailable. The default settings is: Work offline, meaning that the server's files are available to the local computer.*

*The other option available to the administrator is: Never go offline, meaning the server's files are unavailable to the local computer.*

*Determines whether network files remain available if the computer is suddenly disconnected from the server hosting the files.*

*This policy also disables the "When a network connection is lost" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*

*If you enable this policy, you can use the "Action" box to specify how computers in the group respond.*

*-- "Work offline" indicates that the computer can use local copies of network files while the server is inaccessible.*

*-- "Never go offline" indicates that network files are not available while the server is inaccessible.*

*If you disable this policy or select the "Work offline" option, users can work offline if disconnected.*

*If you do not configure this policy, users can work offline by default, but they can change this option.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To configure this setting without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, click Advanced, and then select an option in the "When a network connection is lost" section.*

*Also, see the "Non-default server disconnect actions" policy.*

- Administratively assigned offline files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may specify network files and folders that are always available offline. The administrator must type the fully qualified UNC path for each file or folder.*

*Lists network files and folders that are always available for offline use. This policy makes the specified files and folders available offline to users of the computer.*

*To assign a folder, click Show and then click Add. In the "Type the name of the item to be added" box, type the fully qualified UNC path to the file or folder. Leave the "Enter the value of the item to be added" field blank.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- At logoff, delete local copy of user's offline files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, this causes the local copy of any offline file accessed by the user to be deleted when the user logs off of the computer.*

*Deletes local copies of the user's offline files when the user logs off.*

*This policy specifies that automatically and manually cached offline files are retained only while the user is logged on to the computer. When the user logs off, the system deletes all local copies of offline files.*

*If you disable this policy or do not configure it, automatically and manually cached copies are retained on the user's computer for later offline use.*

*Caution: Files are not synchronized before they are deleted. Any changes to local files since the last synchronization are lost.*

- Default cache size

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 10% of disk.*

*Limits the percentage of the computer's disk space that can be used to store automatically-cached offline files.*

*This policy also disables the "Amount of disk space to use for temporary offline files" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*

*Automatic caching can be set on any network share. When a user opens a file on the share, the system automatically stores a copy of the file on the user's computer.*

*This policy does not limit the disk space available for files that user's make available offline manually.*

*If you enable this policy, you can specify an automatic-cache disk space limit.*

*If you disable this policy, the system limits the space that automatically-cached files occupy to 10 percent of the space on the system drive.*

*If you do not configure this policy, disk space for automatically-cached files is limited to 10 percent of the system drive by default, but users can change it.*

*Tip: To change the amount of disk space used for automatic caching without setting a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then use the slider bar associated with the "Amount of disk space to use for temporary offline files" option.*

- Disable ‘Make Available Offline’

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, prevent users from making files and folders available for offline use.*

*Prevents users from making network files and folders available offline.*

*This policy removes the "Make Available Offline" option from the File menu and from all context menus in Windows Explorer. As a result, users cannot designate files to be saved on their computer for offline use.*

*However, this policy does not prevent the system from saving local copies of files that reside on network shares designated for automatic caching.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Disable reminder balloons

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, prevents reminder balloons from displaying above Offline Files icon in the system try notification area*

*Hides or displays reminder balloons, and prevents users from changing the setting.*

*Reminder balloons appear above the Offline Files icon in the status area to notify users when they have lost the connection to a networked file and are working on a local copy of the file. Users can then decide how to proceed.*

*If you enable this policy, the system hides the reminder balloons, and prevents users from displaying them.*

*If you disable the policy, the system displays the reminder balloons, and prevents users from hiding them.*

*If this policy is not configured, reminder balloons are displayed by default when you enable offline files, but users can change the setting.*

*To prevent users from changing the setting while a policy is in effect, the system disables the "Enable reminders" option on the Offline Files tab*

- Disable user configuration of Offline Files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, prevents users from changing any cache configuration settings.*

*Prevents users from enabling, disabling, or changing the configuration of Offline Files.*

*This policy removes the Offline Files tab from the Folder Options dialog box. It also removes the Settings item from the Offline Files context menu and disables the Settings button on the Offline Files Status dialog box. As a result, users cannot view or change the options on the Offline Files tab or Offline Files dialog box.*

*This is a comprehensive policy that locks down the configuration you establish by using other policies in this folder.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: This policy provides a quick method for locking down the default settings for Offline Files. To accept the defaults, just enable this policy. You do not have to disable any other policies in this folder.*

- Enabled

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, files from auto-cache shared folders are cached on the local computer. Users can also select specific folders and files to always be available when working offline.*

*Determines whether the Offline Files feature is enabled.*

*This policy also disables the "Enable Offline Files" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*

*Offline Files saves a copy of network files on the user's computer for use when the computer is not connected to the network.*

*If you enable this policy, Offline Files is enabled and users cannot disable it.*

*If you disable this policy, Offline Files is disabled and users cannot enable it.*

*By default, Offline Files is enabled on Windows 2000 Professional and is disabled on Windows 2000 Server.*

*Tip: To enable Offline Files without setting a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click "Enable Offline Files."*

*Note: To make changes to this policy effective, you must restart Windows 2000.*



- Event logging level

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 0, cache data corrupted.*

*Administrator may choose from among the following:*

*-- 0 = Cache data corrupted*

*-- 1 = Log 'server offline'*

*-- 2 = Level 1 + log 'net stopped' and 'net started'*

*-- 3 = Level 2 + log 'server available for reconnection'*

*Determines which events the Offline Files feature records in the event log.*

*Offline Files records events in the Application log in Event Viewer when it detects errors. By default, Offline Files records an event only when the offline files storage cache is corrupted. However, you can use this policy to specify additional events you want Offline Files to record.*

*To use this policy, from the "Enter" box, select the number corresponding to the events you want the system to log. The levels are cumulative; that is, each level includes the events in all preceding levels.*

*"0" records an error when the offline storage cache is corrupted.*

*"1" also records an event when the server hosting the offline file is disconnected from the network.*

*"2" also records events when the local computer is connected and disconnected from the network.*

*"3" also records an event when the server hosting the offline file is reconnected to the network.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Files not cached

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, files may be excluded from caching on auto-cache shared folders based on their extension. The administrator may enter a list of extensions to be excluded.*

*Lists types of files that cannot be used offline.*

*This policy lets you exclude certain types of files from automatic and manual caching for offline use. The system does not cache files of the type specified in this policy even when they reside on a network share configured for automatic caching. Also, if users try to make a file of this type available offline, the operation will fail and the following message will be displayed in the Synchronization Manager progress dialog box: "Files of this type cannot be made available offline."*

*This policy is designed to protect files that cannot be separated, such as database components.*

*To use this policy, type the file name extension in the "Extensions" box. To type more than one extension, separate the extensions with a semicolon (;).*

*Note: To make changes to this policy effective, you must log off and log on again.*

- Initial reminder balloon lifetime

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 30 seconds.*

*Determines how long the first reminder balloon for a network status change is displayed.*

*Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the duration of the first reminder.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Non-default server disconnect actions

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may specify non-default actions for servers that become unavailable.*

*Determines how computers respond when they are disconnected from particular offline file servers. This policy overrides the default response, a user-specified response, and the response specified in the "Action on server disconnect" policy.*

*This policy also disables the "Exception list" section on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*

*To use this policy, click Show, and then click Add. In the "Type the name of the item to be added" box, type the server's computer name. Then, in the "Type the value of the item to be added" box, type "0" if users can work offline when they are disconnected from this server, or type "1" if they cannot.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To configure this setting without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click Advanced. This policy corresponds to the settings in the "Exception list" section.*

- Prevent use of Offline Files folder

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, prevents users from accessing offline files through the Offline File folder.*

*Disables the Offline Files folder.*

*This policy disables the "View Files" button on the Offline Files tab. As a result, users cannot use the Offline Files folder to view or open copies of network files stored on their computer.*

*Also, they cannot use the folder to view characteristics of offline files, such as their server status, type, or location.*

*This policy does not prevent users from working offline or from saving local copies of files available offline. Also, it does not prevent them from using other programs, such as Windows Explorer, to view their offline files.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To view the Offline Files Folder, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click "View Files."*

- Reminder balloon frequency

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 60 minutes.*

*Determines how often reminder balloon updates appear.*

*This policy also removes the "Display reminder balloon every ... minutes" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*

*Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the update interval.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To set reminder balloon frequency without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This policy corresponds to the "Display reminder balloons every ... minutes" option.*

- Reminder balloon lifetime

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 15 seconds.*

*Determines how long updated reminder balloons are displayed.*

*Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the duration of the update reminder.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Subfolders always available offline

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, ensures all subfolders are available offline when a folder is made available for offline use.*

*Makes subfolders available offline whenever their parent folder is made available offline.*

*This policy automatically extends the "make available offline" setting to all new and existing subfolders of a folder. Users do not have the option of excluding subfolders.*

*If you enable this policy, then when you make a folder available offline, all folders within that folder are also made available offline. Also, new folders that you create within a folder that is available offline are made available offline when the parent folder is synchronized.*

*If you disable this policy or do not configure it, the system asks users whether they want subfolders to be made available offline when they make a parent folder available offline.*

- Synchronize all offline files before logging off

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, control the level of synchronization performed at logoff.*

*Determines whether offline files are fully synchronized when users log off.*

*This policy also disables the "Synchronize all offline files before logging off" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*

*If you enable this policy, offline files are fully synchronized. Full synchronization ensures that offline files are complete and current.*

*If you disable this policy, the system only performs a quick synchronization. Quick synchronization ensures that files are complete, but does not ensure that they are current.*

*If you do not configure this policy, the system performs a quick synchronization by default, but users can change this option.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To change the synchronization method without setting a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then select the "Synchronize all offline files before logging off" option.*

### Network and Dial-up Connections

- Allow configuration of connection sharing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether administrators can enable, disable, and configure the Internet Connection Sharing feature of a dial-up connection.*

*If you enable this policy or do not configure it, the system displays the Internet Connection Sharing (ICS) tab in the Properties dialog box for a dial-up connection. On Windows 2000 Server, it also displays the Internet Connection Sharing page in the Network Connection wizard. (This page is available only in Windows 2000 Server.)*

*If you disable this policy, the Internet Connection Sharing (ICS) tab and Internet Connection Sharing wizard page are removed.*

*Internet Connection Sharing lets users configure their system as an Internet gateway for a small network. It provides network services, such as name resolution, to the network.*

*By default, Internet Connection Sharing is disabled when you create a dial-up connection, but administrators can use the Internet Connection Sharing (ICS) tab and Internet Connection Sharing wizard page to enable it.*

## Printers

- Allow printers to be published

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, allows machine to publish printers.*

*Determines whether the computer's shared printers can be published in Active Directory.*

*If you enable this policy or do not configure it, users can use the "List in directory" option in the Printers folder or the Add Printer wizard to publish shared printers in Active Directory.*

*If you disable this policy, this computer's shared printers cannot be published in Active Directory and the "List in directory" option is disabled.*

- Allow pruning of published printers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, allows pruning of publish printers.*

*Determines whether the domain controller can prune (delete from Active Directory) the printers published by this computer.*

*By default, the pruning service on the domain controller prunes printer objects from Active Directory if the computer that published them does not respond to contact requests. When the computer that published the printers restarts, it republishes any deleted printer objects.*

*If you enable this policy or do not configure it, the domain controller prunes this computer's printers when the computer does not respond.*

*If you disable this policy, the domain controller does not prune this computer's printers. This setting is designed to prevent printers from being pruned when the computer is temporarily disconnected from the network.*

*Note: You can use the "Directory Pruning Interval" and "Directory Pruning Retry" policies to adjust the contact interval and number of contact attempts.*

- Automatically publish new printers in Active Directory

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, newly created shared printers are published in the Active Directory.*

*Determines whether the Add Printer wizard automatically publishes the computer's shared printers in Active Directory.*

*If you enable this policy or do not configure it, the Add Printer wizard automatically publishes all shared printers.*

*If you disable this policy, the Add Printer wizard does not automatically publish printers. However, you can publish shared printers manually.*

*Note: This policy is ignored if the "Allow printers to be published" policy is disabled.*

- Check published state

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: Never. The administrator may choose from among the following:*

*- Never*

*- 30 minutes*

*- 1 hour*

*- 4 hours*

*- 8 hours*

*- 12 hours*

*- 1 day*

*Directs the system to periodically verify that the printers published by this computer still appear in Active Directory. Also, this policy specifies how often the system repeats the verification.*

*By default, the system verifies published printers when it starts. This policy provides for periodic verification while the computer is operating.*

*To enable this additional verification, enable this policy, and then select a verification interval.*

*To disable verification, disable or do not configure this policy, or set the verification interval to "Never.*

- Computer location

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, administrator may enter the location of this computer.*

*Specifies the default location criteria used when searching for printers.*

*This policy is a component of the Location Tracking feature of Windows 2000 printers. To use this policy, enable Location Tracking by enabling the "Pre-populate printer search location text" policy.*

*When Location Tracking is enabled, the system uses the specified location as a criteria when users search for printers. The value you type here overrides the actual location of the computer conducting the search.*

*Type the location of the user's computer. When users search for printers, the system uses the specified location (and other search criteria) to find a printer nearby. You can also use this policy to direct users to a particular printer or group of printers that you want them to use.*

*If you disable this policy or do not configure it and the user does not type a location as a search criteria, the system searches for a nearby printer based on the IP address and subnet mask of the user's computer.*

- Custom support URL in the Printers folder's left pane

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the administrator may specify the support URL title name, and the URL.*
>
> *Adds a customized Web page link to the Printers folder.*
>
> *By default, the Printers folder includes a link to the Microsoft Support Web page. It can also include a link to a Web page supplied by the vendor of the currently selected printer.*
>
> *You can use this policy to replace these default links with a link to a Web page customized for your enterprise.*
>
> *If you disable this policy or do not configure it, or if you do not enter an alternate Internet address, the default links appear in the Printers folder.*
>
> *Note: Web pages links only appear in the Printers folder when Web view is enabled. If Web view is disabled, the policy has no effect. (To enable Web view, open the Printers folder, and from the Tools menu, click Folder Options, click the General tab, and then click "Enable Web content in folders.")*
>
> *Also, see the "Web-based printing" policy in this policy folder and the "Browse a common web site to find printers" policy in User Configuration\Administrative Templates\Control Panel\Printers.*
>
> *Web view is affected by the "Enable Classic Shell" and "Remove the Folder Options menu item from the Tools menu" policies in User Configuration\Administrative Templates\Windows Components\Windows Explorer, and by the "Enable Active Desktop" policy in User Configuration\Administrative Templates\Desktop\Active Desktop.*

- Directory pruning interval

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the default setting is: 8 hours. The administrator may choose from among the following:*
>
> *- 8 hours*
>
> *- 12 hours*
>
> *- 1 day*
>
> *- 2 days*
>
> *- 3 days*
>
> *- 4 days*
>
> *- 5 days*
>
> *Specifies how often the pruning service on a domain controller contacts computers to verify that their printers are operational.*
>
> *The pruning service periodically contacts computers that have published printers. If a computer does not respond to the contact message (optionally, after repeated attempts), the pruning service "prunes" (deletes from Active Directory) printer objects the computer has published.*
>
> *By default, the pruning service contacts computers every eight hours and allows two repeated contact attempts before deleting printers from Active Directory. You can use this policy to*

*change the interval between contact attempts. To change the number of attempts, use the "Directory Pruning Retry" policy.*

*Note: This policy is used only on domain controllers.*

- Directory pruning priority

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: Normal. The administrator may choose from among the following:*

*- Lowest*

*- Below Normal*

*- Normal*

*- Above Normal*

*- Highest*

*Sets the priority of the pruning thread.*

*The pruning thread, which runs only on domain controllers, deletes printer objects from Active Directory if the printer that published the object does not respond to contact attempts. This process keeps printer information in Active Directory current.*

*The thread priority influences the order in which the thread receives processor time and determines how likely it is to be preempted by higher priority threads.*

*By default, the pruning thread runs at normal priority. However, you can adjust the priority to improve the performance of this service.*

*Note: This policy is used only on domain controllers.*

- Directory pruning retry

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 2 Retries. The administrator may choose form among the following:*

*- No Retry*

*- 1 Retry*

*- 2 Retries*

*- 3 Retries*

*- 4 Retries*

*- 5 Retries*

*- 6 Retries*

*Specifies how many times the pruning service on a domain controller repeats its attempt to contact a computer before pruning the computer's printers.*

*The pruning service periodically contacts computers that have published printers to verify that the printers are still available for use. If a computer does not respond to the contact message, the message is repeated for the specified number of times. If the computer still fails to respond,*

*then the pruning service "prunes" (deletes from Active Directory) printer objects the computer has published.*

*By default, the pruning service contacts computers every eight hours and allows two retries before deleting printers from Active Directory. You can use this policy to change the number of retries. To change the interval between attempts, use the "Directory Pruning Interval" policy.*

*Note: This policy is used only on domain controllers.*

- Pre-populate printer search location text

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the location search text when searching for printers in the Active Directory is pre-populated.*

*Enables the physical Location Tracking support feature of Windows 2000 printers.*

*Location tracking lets you design a location scheme for your enterprise and assign computers and printers to locations in your scheme. Location tracking overrides the standard method of locating and associating users and printers, which uses the IP address and subnet mask of a computer to estimate its physical location and proximity to other computers.*

*If you enable Location Tracking, a Browse button appears beside the Location field in the Find Printers dialog box. (To go to the Browse button, click Start, click Search, and click For printers.) The Browse button also appears on the General tab of the Properties dialog box for a printer. It lets users browse for printers by location without their having to know the precise location (or location naming scheme). Also, if you enable the "Computer location" policy, the default location you type appears in the Location field.*

*If you disable this policy or do not configure it, Location Tracking is disabled. Printer proximity is estimated based on IP address and subnet mask.*

- Printer browsing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, will cause the print subsystem to announce shared printers for printer browsing.*

*Announces the presence of shared printers to print browse master servers for the domain.*

*On Windows 2000 domains with Active Directory, shared printer resources are available in Active Directory and are not announced.*

*If you enable this policy, the print spooler announces shared printers to the print browse master servers. As a result, shared printers appear in the domain list in the Browse for Printer dialog box of the Add Printer wizard.*

*If you disable this policy, shared printers are not announced to print browse master servers, even if Active Directory is not available.*

*If you do not configure this policy, shared printers are announced to browse master servers only when Active Directory is not available.*

*Note: A client license is used each time a client computer announces a printer to a print browse master on the domain.*

- Prune printers that are not automatically republished

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the default setting is: Never. The administrator may choose from among the following:*
>
> *- Never*
>
> *- Only if Print Server is found*
>
> *- Whenever printer is not found*
>
> *Determines whether the system prunes (deletes from Active Directory) printers that are not automatically republished. This policy applies to printers running operating systems other than Windows 2000 and to Windows 2000 printers published outside of their domain.*
>
> *The Windows 2000 pruning service prunes printer objects from Active Directory when the computer that published them does not respond to contact requests. Computers running Windows 2000 detect and republish deleted printer objects when they rejoin the network. However, because non-Windows 2000 computers and computers in other domains cannot republish printers in Active Directory automatically, then, by default, the system never prunes their printer objects.*
>
> *You can enable this policy to change the default behavior. To use this policy, select one of the following options from the "Prune non-republishing printers" box:*
>
> *-- "Never" specifies that printer objects that are not automatically republished are never pruned. "Never" is the default.*
>
> *-- "Only if Print Server is found" prunes printer objects that are not automatically republished only when the print server responds, but the printer is unavailable.*
>
> *-- "Whenever printer is not found" prunes printer objects that are not automatically republished whenever the host computer does not respond, just as it does with Windows 2000 printers.*
>
> *Note: This policy applies to printers published by using Active Directory Users and Computers or Pubprn.vbs. It does not apply to printers published by using Printers in Control Panel.*
>
> *Tip: If you disable automatic pruning, remember to delete printer objects manually whenever you remove a printer or print server.*

- Web-based printing

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, allows Internet printing.*
>
> *Determines whether Internet printing is supported on this server.*
>
> *Internet printing lets you display printers on Web pages so the printers can be viewed, managed, and used across the Internet or an intranet.*
>
> *Internet printing is supported by default on Windows 2000. If you enable this policy or do not configure it, Internet printing remains supported. If you disable this policy, Internet printing is not supported.*
>
> *Note: This policy affects the server side of Internet printing only. It does not prevent the print client on the computer from printing across the Internet. Also, see the "Custom support URL in the Printers folder's left pane" policy in this folder and the "Browse a common web site to find printers" policy in User Configuration\Administrative Templates\Control Panel\Printers.*

Chapter

2

# User Configuration

This includes all user-related policies that specify operating system behavior, desktop settings, security settings, assigned and published applications options, user logon and logoff scripts, and folder redirection options. User-related Group Policy is applied when users log on to the computer and during the periodic refresh cycle.

## Software Settings

### Software Installation

The Software Installation snap-in, a software management feature of Windows 2000, is the administrator's primary tool for managing software throughout its life cycle within the organization.

Before you can use Software Installation, you need a Windows Installer package for the program you want to install. The package is often supplied with the software. If a program does not have a Windows Installer package, you need to generate one. Third-party utilities are available for repackaging a program you plan to install. You can then use transforms to further customize a package.

The next step is creating a network share, called a software distribution point, that contains the packages, any transforms, and the program files and components. Administration is simpler if packages and program files are kept together, although they don't have to be. (Packages and transforms do have to be kept together.) Administrators might also benefit from using distributed file systems to help manage these software distribution points.

Finally, you need to make sure that users can read from the software distribution point, and write to the target of the installation, particularly if the program is being written to a network file server.

Software Installation works in conjunction with Group Policy and Active Directory. It is one of the three Software Installation and Maintenance tools provided with Windows 2000 Server. These are described in the following table.

| Component | Role |
|---|---|
| The Software Installation extension of the Group Policy snap-in | Used by administrators to manage software. |
| Windows Installer | Installs software packaged in Windows Installer files. |
| Add/Remove Programs in Control Panel | Used by users to manage software on their own computers. |

When you **assign** an application to a user, the application is advertised to the user the next time that user logs onto a workstation. The application advertisement follows the user regardless of which physical computer he or she actually uses. This application is installed the first time the user activates the application on the computer, either by selecting the application on the **Start** menu, or by activating a document associated with the application.

When you **publish** the application to users, the application does not appear installed on the users' computers. No shortcuts are visible on the desktop or **Start** menu, and no changes are made to the local registry on the users' computers. Instead, published applications store their advertisement attributes in Active Directory. Then, information such as the application's name and file associations is exposed to the users in the Active Directory container. The application is then available for the user to install using Add/Remove Programs in Control Panel or by clicking a file associated with the application (such as an .xls file for Microsoft Excel).

For every published or assigned application in a particular Group Policy object, an application assignment script (.aas file) is generated and is stored in that domain's Group Policy object. These script files contain the advertisement information about the application configuration.

At the user's computer, system components including Winlogon, the shell, object linking and embedding (OLE), the Lightweight Directory Access Protocol (LDAP) client, and the local registry provide the user's view of software installation. Winlogon is the privileged agent that applies software installation policy. The shell and OLE are enhanced to be Active Directory–aware and to communicate with Windows Installer to perform setup actions. The LDAP client provides the capability to search and query Active Directory.

Using Add/Remove Programs, users can browse for and install software from Active Directory in a managed environment, or from local media (in a non-managed environment, or if policy permits, installation from local media in a managed environment).

# Windows Settings

## Internet Explorer Maintenance

### Browser User Interface

- Browser Title

> *You can customize the text that appears in the title bar of your Internet Explorer browser. This text is appended to the string "Microsoft Internet Explorer provided by." You can also customize the toolbar background bitmap.*
>
> *Note: If you included Outlook Express in your package, then the text you enter below will also be added to the Outlook Express title bar.*
>
> *The administrator may check "Customize Title Bars" and/or "Customize Toolbar background bitmap."*

- Animated Bitmaps

> *You can replace the animated Internet Explorer logo in the upper-right corner of the Internet Explorer window with an animated logo of you choice.*

*The bitmap must contain a vertical stack of images that follow these specific rules in order to be displayed correctly.*

*Cells 1 through 4 are lead-in cells, which are played when Internet Explorer begins to browse.*

*Cells 5 through X, where X is the total number of cells, loop until the browse operation is complete.*

*The administrator may enter the path of the large and small bitmaps.*

- Custom Logo

*You can replace the static Internet Explorer logo in the upper-right corner of the Internet Explorer window with a static logo of your choice.*

*The administrator may enter the path of the customized static logo bitmaps.*

- Browser Toolbar Buttons

*You can add browse toolbar buttons to your browser. You will be prompted for information about the toolbar button when you click Add.*

### Connection

- Connection Settings

*You can import your connection settings. If you choose to import, all of your connection settings will be installed with this package. Go to the Internet Control Panel Connections tab to make changed to these settings.*

*You can also restrict how users are able to interact with connection settings via the System Policies and Restrictions page. It is not necessary to import your current settings in order to set these restrictions.*

*The administrator may choose from among the following connection settings:*

*Do not customize Connection Settings*

*Import the current Connection Settings*

*Delete existing Connection Settings, if present*

- Automatic Browser Configuration

*Automatic Configuration (auto-config) allows you to make updates to the user's machine after deployment. You can specify a URL to a .INS file or an auto-proxy URL, or both.*

*The administrator may choose from among the following:*

*Automatically detect configuration settings*

*Enable Automatic Configuration*

*You can set the interval in minutes for when auto-config will happen. If you leave this value blank, or at zero, auto-config will only happen when the browser has been started and navigates to a page.*

- Proxy Settings

*You can specify what proxy servers, if any, you want your users to connect to.*

*The administrator has the option of using the same proxy server for all addresses, or setting an address for each of the following:*

*- HTTP*

*- Secure*

*- FTP*

*- Gopher*

*- Socks*

- User Agent String

*The user agent string is what the browser send to visited servers to identify itself. It is often used to keep Internet traffic statistics.*

*You can enter in custom text that will be appended to the default Internet Explorer string. The default string is different for each platform.*

*The administrator may use the check box to enable customizing the string.*

URLS

- Favorites and Links

*You can customize Favorites and Links by specifying URLs. You can also specify the order of each folder, add an icon for each Favorite and Link, and import an existing folder structure.*

- Important URLs

*You can specify a custom homepage, search bar URL, and online support page. The home page is opened when the browser is started or when the user clicks on the Home button.*

- Channels

*You can customize the channels in your package. You will be prompted for the information about the channel or category when you click Add.*

Security

- Security Zones and Content Ratings

*You can customize the settings for each security zone. These settings must be made through the Modify Settings button on the dialog box.*

*- The administrator may choose from among the following Security Zones options:*

*- Do not customize security zones (default)*

*Import the current security zones settings*

*Content ratings allow you to prevent users from viewing sites with risky content. Ratings are set on a per-site basis and are rated by the author for degrees of risky language, nudity, and violence.*

*- The administrator may choose from among the following Content Ratings options:*

*- Do not customize Context Ratings (default)*

*Import the current Content Ratings settings*

- Authenticode Settings

> *Authenticode allows you to designate software publishers and credentials agencies as trustworthy.*
>
> *To customize these settings, you must first import them from the current machine. After selecting to import the settings, you can then modify them.*
>
> *The administrator may choose from among the following Authenticode Security options:*
>
> *- Do no customize Authenticode Security (default)*
>
> *- Import current Authenticode Security information*
>
> *You can prevent users from adding new trusted publishers while using the browser. Enabling this lockdown does not prevent access to the Content control panel, but this option is available via policy.*
>
> *The administrator may use the check box to enable trusted publisher lockdown.*

### Programs

- Programs

> *You can import the current default programs settings. The programs selected specify which program Windows automatically uses for each Internet service.*
>
> *The Internet services you can set the default program are: HTML editor, E-mail, Newsgroups, Internet call, Calendar, and Contact list.*
>
> *The administrator may choose from among the following program settings options:*
>
> *- Do not customize Program Settings(default)*
>
> *- Import the current Program Settings*

## Scripts (Logon/Logoff)

Lists all scripts currently assigned to the selected Group Policy object. If you assign multiple scripts, the scripts are processed according to the order you specify.

## Security Settings

This node contains a folder titled Public Key Policies. A child folder of Public Key Policies is Enterprise Trust. While in the Enterprise Trust folder, on the **Action** menu, point to **New**, and then click **Certificate Trust List**. This starts the Certificate Trust List wizard.

You can assign a certificate trust list (CTL) to a Group Policy object either by creating a new certificate trust list or by importing an existing one. If you are creating a new certificate trust list, you must sign the certificate trust list with a certificate issued for this purpose by a certification authority (CA).

In addition to being signed by a CTL signing certificate, creating a certificate trust list also requires:

1) The root certificates you want to include in the certificate trust list.

2) Knowing the purposes for which you want to trust the root certificates in the certificate trust list.

A certificate trust list (CTL) allows you to control trust of the purpose and validity period of certificates issued by external certification authorities (CAs).

Typically, a CA can issue certificates for a wide variety of purposes such as secure e-mail or client authentication. But there may be reasons that you want to limit the trust of certificates issued by a particular CA, especially if the CA is external to your organization. This is where creating a certificate trust list and using it via Group Policy is useful.

## Remote Installation Services

You use the Remote Installation Preparation wizard to prepare an existing Windows 2000 Professional installation and to replicate that image to an available Remote Installation Services server on the network.

The image conversion process consists of the following steps:

1) You use Remote Installation Services to remotely install the base Windows 2000 Professional operating system.

2) You install client computer applications that do not adhere to the Windows Installer technology.

3) You configure the source computer to conform to any company desktop standards required. For example, you might want to define specific screen colors, set the background bitmap to a company-based logo, remove any games installed by the base operating system, and configure Internet Explorer proxy settings.

4) You close all applications and run the Remote Installation Preparation wizard.

5) The wizard configures the source computer to a generic state, removing anything that is unique to the client installation, such as the computer's unique security ID (SID), computer name, and any registry settings unique to the client source computer.

6) The wizard prompts you for the installation information required by the image conversion process. This information includes the location where the client installation image should be replicated, the name of the directory it should be copied to on the server, and a friendly description and associated Help text describing the installation image to users running the Client Installation wizard.

7) After the replication is complete, the installation image is automatically added to the list of available operating system installation options and is available to client computers that use the remote boot technology.

One important feature of the Remote Installation Preparation wizard process is that a remote boot–enabled client computer does not need to contain hardware identical to that of the source computer used to create the installation image. The Remote Installation Preparation wizard uses the Plug and Play feature of Windows 2000 to detect any differences between the source and destination computer's hardware during the image installation process.

## Folder Redirection

You use the Folder Redirection extension to Group Policy to redirect certain Windows 2000 special folders to network locations. Special folders are those folders such as My Documents and My Pictures that are located under Documents and Settings.

The folders located in this node are: Application Data, Desktop, My Documents (with a child folder titled My Pictures), and Start Menu. Each folder's settings may be accessed by right-clicking on the folder and selecting **Properties**. Each has the following settings and options:

> *Default Target Setting: No administrative policy specified.*
>
> *The administrator may choose from among the following options:*
>
> *- No administrative policy specified*
>
> *- Basic – Redirect everyone's folder to the same location*
>
> *- Advanced – Specify locations for various user groups*
>
> *Only by setting the Basic option will the following default Settings options be active:*
>
> *- Grant the user exclusive rights to <Folder Name>. (checked by default)*
>
> *- Move the contents of <Folder Name> to the new location. (checked by default)*
>
> *The default Policy Removal option is: Leave the folder in the new location when policy is removed. The administrator may choose from among the following Policy Removal options:*
>
> *- Leave the folder in the new location when policy is removed.*
>
> *- Redirect the folder back to the local user profile location when policy is removed.*

# Administrative Templates

## Windows Components

### NetMeeting

- Enable Automatic Configuration

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the administrator may enter the Configuration URL.*
>
> *Configures NetMeeting to download settings for users each time it starts.*
>
> *The settings are downloaded from the URL listed in the "Configuration URL:" text box.*
>
> *Group Policy based settings have precedence over any conflicting settings set by downloading them from this URL.*

- Disable Directory Services

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the directory feature of NetMeeting.*

*Users will not logon to a directory (ILS) server when NetMeeting starts. Users will also not be able to view or place calls via a NetMeeting directory.*

*This policy is for deployers who have their own location or calling schemes such as a Web site or an address book.*

- Prevent adding Directory Servers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from adding directory (ILS) servers to the list of those they can use for placing calls.*

- Prevent viewing Web Directory

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from viewing directories as Web pages in a browser.*

- Set the intranet support Web page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may enter the Support Web page URL.*

*Sets the URL NetMeeting will display when the user chooses the Help Online Support command.*

- Set Call Security options

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: empty, nothing displayed. The administrator may choose from among the following: Disabled, or Required. The dialog box will not close until one these options is selected.*

*Sets the level of security for both outgoing and incoming NetMeeting calls.*

- Prevent changing Call placement method

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing the way calls are placed, either directly or via a gatekeeper server.*

- Prevent automatic acceptance of Calls

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from turning on automatic acceptance of incoming calls.*

*This ensures that others cannot call and connect to NetMeeting when the user is not present.*

*This policy is recommended when deploying NetMeeting to run always.*

- Prevent sending files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from sending files to others in a conference.*

- Prevent receiving files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from receiving files from others in a conference.*

- Limit the size of sent files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the maximum size in bytes is: empty, nothing displayed. The administrator must enter a valid number for the policy to take effect.*

*Limits the size of files users can send to others in a conference.*

- Disable Chat

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the Chat feature of NetMeeting.*

- Disable NetMeeting 2.x Whiteboard

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the 2.x whiteboard feature of NetMeeting.*

*The 2.x whiteboard is available for compatibility with older versions of NetMeeting only.*

*Deployers who do not need it can save bandwidth by disabling it.*

- Disable Whiteboard

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the T.126 whiteboard feature of NetMeeting.*

*Application Sharing*

- Disable application Sharing

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Disables the application sharing feature of NetMeeting completely. Users will not be able to host or view shared applications.*

- Prevent Sharing

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from sharing anything themselves. They will still be able to view shared applications/desktops from others.*

- Prevent Desktop Sharing

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from sharing the whole desktop. They will still be able to share individual applications.*

- Prevent Sharing Command Prompts

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from sharing command prompts. This prevents users from inadvertently sharing out applications, since command prompts can be used to launch other applications.*

- Prevent Sharing Explorer windows

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from sharing Explorer windows. This prevents users from inadvertently sharing out applications, since Explorer windows can be used to launch other applications.*

- Prevent Control

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from allowing others in a conference to control what they have shared. This enforces a read-only mode; the other participants cannot change the data in the shared application.*

- Prevent Application Sharing in true color

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from sharing applications in true color. True color sharing uses more bandwidth in a conference.*

*Audio & Video*

- Limit the bandwidth of Audio and Video

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting for maximum bandwidth is: 621700 Kbps.*

*Limits the bandwidth audio and video will consume when in a conference. This setting will guide NetMeeting to choose the right formats and send rate so that the bandwidth is limited.*

- Disable Audio

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the audio feature of NetMeeting. Users will not be able to send or receive audio.*

- Disable full duplex Audio

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables full duplex mode audio. Users will not be able to listen to incoming audio while speaking into the microphone. Older audio hardware does not perform well when in full duplex mode.*

- Prevent changing DirectSound Audio setting

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents user from changing the DirectSound audio setting. DirectSound provides much better audio quality, but older audio hardware may not support it.*

- Prevent sending Video

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from sending video if they have the hardware. Users will still be able to receive video from others.*

- Prevent receiving Video

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from receiving video. Users will still be able to send video provided they have the hardware.*



*Options Page*

- Hide the General page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Hides the General page of the Tools Options dialog. Users will not then be able to change personal identification and bandwidth settings.*

- Disable the Advanced Calling button

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the Advanced Calling button on the General Options page. Users will not then be able to change the call placement method and the servers used.*

- Hide the Security page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Hides the Security page of the Tools Options dialog. Users will not then be able to change call security and authentication settings.*

- Hide the Audio page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Hides the Audio page of the Tools Options dialog. Users will not then be able to change audio settings.*

- Hide the Video page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Hides the Video page of the Tools Options dialog. Users will not then be able to change video settings.*

Internet Explorer

- Search: Disable Search Customization

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Makes the Customize button in the Search Assistant appear dimmed.*

*The Search Assistant is a tool that appears in the Search bar to help users search the Internet.*

*If you enable this policy, users cannot change their Search Assistant settings, such as setting default search engines for specific tasks.*

*If you disable this policy or do not configure it, users can change their settings for the Search Assistant.*

*This policy is designed to help administrators maintain consistent settings for searching across an organization.*

- Search: Disable Find Files via F3 within the browser

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables using the F3 key to search in Internet Explorer and Windows Explorer.*

*If you enable this policy, the search functionality of the F3 key is disabled. Users cannot press F3 to search the Internet (from Internet Explorer) or to search the hard disk (from Windows Explorer). If the user presses F3, a prompt appears that informs the user that this feature has been disabled.*

*If you disable this policy or do not configure it, users can press F3 to search the Internet (from Internet Explorer) or the hard disk (from Windows Explorer).*

*This policy is intended for situations in which administrators do not want users to explore the Internet or the hard disk.*

*This policy can be used in coordination with the "File Menu: Disable Open menu option" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser Menus), which prevents users from opening files by using the browser.*

- Disable external branding of Internet Explorer

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents branding of Internet programs, such as customization of Internet Explorer and Outlook Express logos and title bars, by a third party.*

*If you enable this policy, it prevents customization of the browser by a third party, such as an Internet service provider or Internet content provider.*

*If you disable this policy or do not configure it, users could install customizations from a third party—for example, when signing up for Internet services.*

*This policy is intended for administrators who want to maintain a consistent browser across an organization.*

- Disable importing and exporting favorites

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from exporting or importing favorite links by using the Import/Export wizard.*

*If you enable this policy, the Import/Export wizard cannot import or export favorite links or cookies, which are small text files that contain settings for Web sites.*

*If you disable this policy or do not configure it, users can import and export favorites in Internet Explorer by clicking the File menu, clicking Import and Export, and then running the Import/Export wizard.*

*Note: If you enable this policy, users can still view screens in the wizard, but when users click Finish, a prompt will appear that states that this feature has been disabled.*

- Disable changing Advanced home page settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing settings on the Advanced tab in the Internet Options dialog box.*

*If you enable this policy, users are prevented from changing advanced Internet settings, such as security, multimedia, and printing. Users cannot select or clear the check boxes on the Advanced tab.*

*If you disable this policy or do not configure it, users can select or clear settings on the Advanced tab.*

*If you set the "Disable the Advanced page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the Advanced page" policy removes the Advanced tab from the interface.*

- Disable changing home page settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing the home page of the browser. The home page is the first page that appears when users start the browser.*

*If you enable this policy, the settings in the Home Page area on the General tab in the Internet Options dialog box appear dimmed.*

*If you disable this policy or do not configure it, users can change their home page.*

*If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.*

*This policy is intended for administrators who want to maintain a consistent home page across their organization.*

- Use Automatic Detection for dial-up connections

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Specifies that Automatic Detection will be used to configure dial-up settings for users.*

*Automatic Detection uses a DHCP (Dynamic Host Configuration Protocol) or DNS (Domain Name System) server to customize the browser the first time it is started.*

*If you enable this policy, users' dial-up settings will be configured by Automatic Detection.*

*If you disable this policy or do not configure it, dial-up settings will not be configured by Automatic Detection, unless specified by the user.*

- Disable caching of Auto-Proxy scripts

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents automatic proxy scripts, which interact with a server to automatically configure users' proxy settings, from being stored in the users' cache.*

*If you enable this policy, automatic proxy scripts will not be stored temporarily on the users' computer.*

*If you disable this policy or do not configure it, automatic proxy scripts can be stored in the users' cache.*

- Display error message on proxy script download failure

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Specifies that error messages will be displayed to users if problems occur with proxy scripts.*

*If you enable this policy, error messages will be displayed when the browser does not download or run a script to set proxy settings.*

*If you disable this policy or do not configure it, error messages will not be displayed when problems occur with proxy scripts.*

- Disable changing Temporary Internet files settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing the browser cache settings, such as the location and amount of disk space to use for the Temporary Internet Files folder.*

*If you enable this policy, the browser cache settings appear dimmed. These settings are found in the dialog box that appears when users click the General tab and then click the Settings button in the Internet Options dialog box.*

*If you disable this policy or do not configure it, users can change their cache settings.*

*If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.*

- Disable changing history settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing the history settings for the browser.*

*If you enable this policy, the settings in the History area on the General tab in the Internet Options dialog box appear dimmed.*

*If you disable this policy or do not configure it, users can change the number of days to store Web page information and clear Web page history.*

*If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.*

- Disable changing color settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing the default Web page colors.*

*If you enable this policy, the color settings for Web pages appear dimmed. The settings are located in the Colors area in the dialog box that appears when the user clicks the General tab and then clicks the Colors button in the Internet Options dialog box.*

*If you disable this policy or do not configure it, users can change the default background and text color of Web pages.*

*If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.*

*Note: The default Web page colors are ignored on Web pages in which the author has specified the background and text colors.*

- Disable changing link color settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing the colors of links on Web pages.*

*If you enable this policy, the color settings for links appear dimmed. The settings are located in the Links area of the dialog box that appears when users click the General tab and then click the Colors button in the Internet Options dialog box.*

*If you disable this policy or do not configure it, users can change the default color of links on Web pages.*

*If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.*

*Note: The default link colors are ignored on Web pages on which the author has specified link colors.*

- Disable changing font settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing font settings.*

*If you enable this policy, the Font button on the General tab in the Internet Options dialog box appears dimmed.*

*If you disable this policy or do not configure it, users can change the default fonts for viewing Web pages.*

*If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.*

*Note: The default font settings colors are ignored in cases in which the Web page author has specified the font attributes.*

- Disable changing language settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing language settings.*

*If you enable this policy, the Languages button on the General tab in the Internet Options dialog box appears dimmed.*

*If you disable this policy or do not configure it, users can change the language settings for viewing Web sites for languages in which the character set has been installed.*

*If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.*

- Disable changing accessibility settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing accessibility settings.*

*If you enable this policy, the Accessibility button on the General tab in the Internet Options dialog box appears dimmed.*

*If you disable this policy or do not configure it, users can change accessibility settings, such as overriding fonts and colors on Web pages.*

*If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.*

- Disable Internet Connection wizard

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from running the Internet Connection wizard.*

*If you enable this policy, the Setup button on the Connections tab in the Internet Options dialog box appears dimmed.*

*Users will also be prevented from running the wizard by clicking the Connect to the Internet icon on the desktop or by clicking Start, pointing to Programs, pointing to Accessories, pointing to Communications, and then clicking Internet Connection wizard*

*If you disable this policy or do not configure it, users can change their connection settings by running the Internet Connection wizard.*

*Note: This policy overlaps with the "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from the interface. Removing the Connections tab from the interface, however, does not prevent users from running the Internet Connection wizard from the desktop or the Start menu.*

- Disable changing connection settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing dial-up settings.*

*If you enable this policy, the Settings button on the Connections tab in the Internet Options dialog box appears dimmed.*

*If you disable this policy or do not configure it, users can change their settings for dial-up connections.*

*If you set the "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the Connections page" policy removes the Connections tab from the interface.*

- Disable changing proxy settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing proxy settings.*

*If you enable this policy, the proxy settings appear dimmed. These settings are in the Proxy Server area of the Local Area Network (LAN) Settings dialog box, which appears when the user clicks the Connections tab and then clicks the LAN Settings button in the Internet Options dialog box.*

*If you set the "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the Connections page" policy removes the Connections tab from the interface.*

- Disable changing Automatic Configuration settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing automatic configuration settings. Automatic configuration is a process that administrators can use to update browser settings periodically.*

*If you enable this policy, the automatic configuration settings appear dimmed. The settings are located in the Automatic Configuration area of the Local Area Network (LAN) Settings dialog*

*box. To see the Local Area Network (LAN) Settings dialog box, users open the Internet Options dialog box, click the Connections tab, and then click the LAN Settings button.*

*If you disable this policy or do not configure it, the user can change automatic configuration settings.*

*This policy is intended to enable administrators to ensure that users' settings are updated uniformly through automatic configuration.*

*The "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable changing rating settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing ratings that help control the type of Internet content that can be viewed.*

*If you enable this policy, the settings in the Content Advisor area on the Content tab in the Internet Options dialog box appear dimmed.*

*If you disable this policy or do not configure it, users can change their ratings settings.*

*The "Disable the Ratings page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Ratings tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable changing certificate settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers.*

*If you enable this policy, the settings in the Certificates area on the Content tab in the Internet Options dialog box appear dimmed.*

*If you disable this policy or do not configure it, users can import new certificates, remove approved publishers, and change settings for certificates that have already been accepted.*

*The "Disable the Content page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

*Caution: If you enable this policy, users can still run the Certificate Manager Import wizard by double-clicking a software publishing certificate (.spc) file. This wizard enables users to import and configure settings for certificates from software publishers that haven't already been configured for Internet Explorer.*

- Disable changing Profile Assistant settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing Profile Assistant settings.*

*If you enable this policy, the My Profile button appears dimmed in the Personal Information area on the Content tab in the Internet Options dialog box.*

*If you disable this policy or do not configure it, users can change their profile information, such as their street and e-mail addresses.*

*The "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable AutoComplete for forms

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents Internet Explorer from automatically completing forms, such as filling in a name or a password that the user has entered previously on a Web page.*

*If you enable this policy, the Forms check box appears dimmed. To display the Forms check box, users open the Internet Options dialog box, click the Content tab, and then click the AutoComplete button.*

*If you disable this policy or do not configure it, users can enable the automatic completion of forms.*

*The "Disable the Content page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

*Caution: If you enable this policy after users have used their browser with form automatic completion enabled, it will not clear the automatic completion history for forms that users have already filled out.*

- Do not allow AutoComplete to save passwords

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables automatic completion of user names and passwords in forms on Web pages, and prevents users from being prompted to save passwords.*

*If you enable this policy, the User Names and Passwords on Forms and Prompt Me to Save Passwords check boxes appear dimmed. To display these check boxes, users open the Internet Options dialog box, click the Content tab, and then click the AutoComplete button.*

*If you disable this policy or don't configure it, users can determine whether Internet Explorer automatically completes user names and passwords on forms and prompts them to save passwords.*

*The "Disable the Content page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable changing Messaging settings

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from changing the default programs for messaging tasks.*
>
> *If you enable this policy, the E-mail, Newsgroups, and Internet Call options in the Internet Programs area appear dimmed. To display these options, users open the Internet Options dialog box, and then click the Programs tab.*
>
> *If you disable this policy or do not configure it, users can determine which programs to use for sending mail, viewing newsgroups, and placing Internet calls, if programs that perform these tasks are installed.*
>
> *The "Disable the Programs page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable changing Calendar and Contact settings

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from changing the default programs for managing schedules and contacts.*
>
> *If you enable this policy, the Calendar and Contact check boxes appear dimmed in the Internet Programs area. To display these options, users open the Internet Options dialog box, and then click the Programs tab.*
>
> *If you disable this policy or do not configure it, users can determine which programs to use for managing schedules and contacts, if programs that perform these tasks are installed.*
>
> *This "Disable the Programs Page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable the Reset Web Settings feature

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from restoring default settings for home and search pages.*
>
> *If you enable this policy, the Reset Web Settings button on the Programs tab in the Internet Options dialog box appears dimmed.*
>
> *If you disable this policy or do not configure it, users can restore the default settings for home and search pages.*
>
> *The "Disable the Programs page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable changing default browser check

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents Internet Explorer from checking to see whether it is the default browser.*

*If you enable this policy, the Internet Explorer Should Check to See Whether It Is the Default Browser check box on the Programs tab in the Internet Options dialog box appears dimmed.*

*If you disable this policy or do not configure it, users can determine whether Internet Explorer will check to see if it is the default browser. When Internet Explorer performs this check, it prompts the user to specify which browser to use as the default.*

*This policy is intended for organizations that do not want users to determine which browser should be their default.*

*The "Disable the Programs page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.*

- Identity Manager: prevent user from using Identities

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from configuring unique identities by using Identity Manager.*

*Identity Manager enables users to create multiple accounts, such as e-mail accounts, on the same computer. Each user has a unique identity, with a different password and different program preferences.*

*If you enable this policy, users will not be able to create new identities, manage existing identities, or switch identities. The Switch Identity option will be removed from the File menu in Address Book.*

*If you disable this policy or do not configure it, users can set up and change identities*

*Internet Control Panel*

- Disable the General page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the General tab from the interface in the Internet Options dialog box.*

*If you enable this policy, users are unable to see and change settings for the home page, the cache, history, Web page appearance, and accessibility.*

*If you disable this policy or do not configure it, users can see and change these settings.*

*When you set this policy, you do not need to set the following Internet Explorer policies (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\), because this policy removes the General tab from the interface:*

*"Disable changing home page settings"*

*"Disable changing Temporary Internet files settings"*

*"Disable changing history settings"*

*"Disable changing color settings"*

*"Disable changing link color settings"*

*"Disable changing font settings"*

*"Disable changing language settings"*

*"Disable changing accessibility settings"*

- Disable the Security page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Security tab from the interface in the Internet Options dialog box.*

*If you enable this policy, it prevents users from seeing and changing settings for security zones, such as scripting, downloads, and user authentication.*

*If you disable this policy or do not configure it, users can see and change these settings.*

*When you set this policy, you do not need to set the following Internet Explorer policies, because this policy removes the Security tab from the interface:*

*"Security zones: Do not allow users to change policies"*

*"Security zones: Do not allow users to add/delete sites"*

*"Only allow controls from Trusted Publishers"*

- Disable the Content page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Content tab from the interface in the Internet Options dialog box.*

*If you enable this policy, users are prevented from seeing and changing ratings, certificates, AutoComplete, Wallet, and Profile Assistant settings.*

*If you disable this policy or do not configure it, users can see and change these settings.*

*When you set this policy, you do not need to set the following policies for the Content tab, because this policy removes the Content tab from the interface:*

*"Disable changing ratings settings"*

*"Disable changing certificate settings"*

*"Disable changing Profile Assistant settings"*

*"Disable AutoComplete for forms"*

*"Do not allow AutoComplete to save passwords"*

- Disable the Connections page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Connections tab from the interface in the Internet Options dialog box.*

*If you enable this policy, users are prevented from seeing and changing connection and proxy settings.*

*If you disable this policy or do not configure it, users can see and change these settings.*

*When you set this policy, you do not need to set the following policies for the Content tab, because this policy removes the Connections tab from the interface*

*:*

*"Disable Internet Connection Wizard"*

*"Disable changing connection settings"*

*"Disable changing proxy settings"*

*"Disable changing Automatic Configuration settings"*

- Disable the Programs page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Programs tab from the interface in the Internet Options dialog box.*

*If you enable this policy, users are prevented from seeing and changing default settings for Internet programs.*

*If you disable this policy or do not configure it, users can see and change these settings.*

*When you set this policy, you do not need to set the following policies for the Programs tab, because this policy removes the Programs tab from the interface:*

*"Disable changing Messaging settings"*

*"Disable changing Calendar and Contact settings"*

*"Disable the Reset Web Settings feature"*

*"Disable changing default browser check"*

- Disable the Advanced page

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Advanced tab from the interface in the Internet Options dialog box.*

*If you enable this policy, users are prevented from seeing and changing advanced Internet settings, such as security, multimedia, and printing.*

*If you disable this policy or do not configure it, users can see and change these settings.*

*When you set this policy, you do not need to set the "Disable changing Advanced page settings" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\), because this policy removes the Advanced tab from the interface.*

*Offline Pages*

- Disable adding channels

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from adding channels to Internet Explorer.*

*Channels are Web sites that are updated automatically on your computer according to a schedule specified by the channel provider.*

*If you enable this policy, the Add Active Channel button, which appears on a channel that users haven't yet subscribed to, will be disabled. Users also cannot add content that is based on a channel, such as some of the Active Desktop items from Microsoft's Active Desktop Gallery, to their desktop.*

*If you disable this policy or do not configure it, users can add channels to the Channel bar or to their desktop.*

*Note: Most channel providers use the words Add Active Channel for this option; however, a few use different words, such as Subscribe.*

- Disable removing channels

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from disabling channel synchronization in Internet Explorer.*

*Channels are Web sites that are automatically updated on your computer according to a schedule specified by the channel provider.*

*If you enable this policy, users cannot prevent channels from being synchronized.*

*If you disable this policy or do not configure it, users can disable the synchronization of channels.*

*This policy is intended to help administrators ensure that users' computers are being updated uniformly across their organization.*

*Note: This policy does not prevent users from removing active content from the desktop interface.*

- Disable adding schedules for offline pages

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from specifying that Web pages can be downloaded for viewing offline. When users make Web pages available for offline viewing, they can view the content when their computer is not connected to the Internet.*

*If you enable this policy, users cannot add new schedules for downloading offline content. The Make Available Offline check box will be dimmed in the Add Favorite dialog box.*

*If you disable this policy or do not configure it, users can add new offline content schedules.*

*This policy is intended for organizations that are concerned about server load for downloading content.*

*The "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable editing schedules for offline pages

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from editing an existing schedule for downloading Web pages for offline viewing.*
>
> *When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet.*
>
> *If you enable this policy, users cannot display the schedule properties of pages that have been set up for offline viewing. If users click the Tools menu, click Synchronize, select a Web page, and then click the Properties button, no properties are displayed. Users do not receive an alert stating that the command is unavailable.*
>
> *If you disable this policy or do not configure it, users can edit an existing schedule for downloading Web content for offline viewing.*
>
> *This policy is intended for organizations that are concerned about server load for downloading content.*
>
> *The "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable removing schedules for offline pages

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from clearing the preconfigured settings for Web pages to be downloaded for offline viewing.*
>
> *When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet.*
>
> *If you enable this policy, the Make Available Offline check box in the Organize Favorites Favorite dialog box and the Make This Page Available Offline check box will be selected but dimmed. To display the Make This Page Available Offline check box, users click the Tools menu, click Synchronize, and then click the Properties button.*
>
> *If you disable this policy or do not configure it, users can remove the preconfigured settings for pages to be downloaded for offline viewing.*
>
> *This policy is intended for organizations that are concerned about server load for downloading content.*
>
> *The "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable offline page hit logging

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents channel providers from recording information about when their channel pages are viewed by users who are working offline.*

*If you enable this policy, it disables any channel logging settings set by channel providers in the channel definition format (.cdf) file. The .cdf file determines the schedule and other settings for downloading Web content.*

*If you disable this policy or do not configure it, channel providers can record information about when their channel pages are viewed by users who are working offline.*

- Disable all scheduled offline pages

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables existing schedules for downloading Web pages for offline viewing.*

*When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet.*

*If you enable this policy, the check boxes for schedules on the Schedule tab of the Web page properties are cleared and users cannot select them. To display this tab, users click the Tools menu, click Synchronize, select a Web page, click the Properties button, and then click the Schedule tab.*

*If you disable this policy, then Web pages can be updated on the schedules specified on the Schedule tab.*

*This policy is intended for organizations that are concerned about server load for downloading content.*

*The "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored.*

- Disable channel user interface completely

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from viewing the Channel bar interface. Channels are Web sites that are automatically updated on their computer according to a schedule specified by the channel provider.*

*If you enable this policy, the Channel bar interface will be disabled, and users cannot select the Internet Explorer Channel Bar check box on the Web tab in the Display Properties dialog box.*

*If you disable this policy or do not configure it, users can view and subscribe to channels from the Channel bar interface.*

- Disable downloading of site subscription content

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents content from being downloaded from Web sites that users have subscribed to.*

*When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet.*

*If you enable this policy, content will not be downloaded from Web sites that users have subscribed to. However, synchronization with the Web pages will still occur to determine if any content has been updated since the last time the user synchronized with or visited the page.*

*If you disable this policy or do not configure it, content will not be prevented from being downloaded.*

*The "Disable downloading of site subscription content" policy and the "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) take precedence over this policy. If either policy is enabled, this policy is ignored.*

- Disable editing and creating of schedule groups

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from adding, editing, or removing schedules for offline viewing of Web pages and groups of Web pages that users have subscribed to.*

*A subscription group is a favorite Web page plus the Web pages it links to.*

*If you enable this policy, the Add, Remove, and Edit buttons on the Schedule tab in the Web page Properties dialog box are dimmed. To display this tab, users click the Tools menu, click Synchronize, select a Web page, click the Properties button, and then click the Schedule tab.*

*If you disable this policy or do not configure it, users can add, remove, and edit schedules for Web sites and groups of Web sites.*

*The "Disable editing schedules for offline pages" policy and the "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) take precedence over this policy. If either policy is enabled, this policy is ignored.*

- Subscription Limits

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must fill in all required fields for the policy to be applied. The administrator may choose from among the following:*

*- Maximum size of subscription in kilobytes*

*- Maximum number of offline pages*

*- Minimum number of minutes between scheduled updates*

*- Time to begin preventing scheduled updates*

*- Time to end preventing scheduled updates*

*- Maximum offline page crawl depth*

*Restricts the amount of information downloaded for offline viewing.*

*If you enable this policy, you can set limits to the size and number of pages that users can download. If users attempt to exceed the number of subscriptions, a prompt will appear that states that they cannot set up more Web sites for offline viewing.*

*If you disable this policy or do not configure it, then users can determine the amount of content that is searched for new information and downloaded.*

*Caution: Although the Maximum Number of Offline Pages option determines how many levels of a Web site are searched for new information, it does not change the user interface in the Offline Favorites wizard.*

> *Note: The begin and end times for downloading are measured in minutes after midnight. The Maximum Offline Page Crawl Depth setting specifies how many levels of a Web site are searched for new information.*

*Browser Menus*

- File menu: Disable Save As… menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from saving Web pages from the browser File menu to their hard disk or to a network share.*
>
> *If you enable this policy, the Save As command on the File menu will be removed.*
>
> *If you disable this policy or do not configure it, users can save Web pages for later viewing.*
>
> *This policy takes precedence over the "File Menu: Disable Save As Web Page Complete" policy, which prevents users from saving the entire contents that are displayed or run from a Web Page, such as graphics, scripts, and linked files, but does not prevent users from saving the text of a Web page.*
>
> *Caution: If you enable this policy, users are not prevented from saving Web content by pointing to a link on a Web page, clicking the right mouse button, and then clicking Save Target As.*

- File menu: Disable New menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from opening a new browser window from the File menu.*
>
> *If this policy is enabled, users cannot open a new browser window by clicking the File menu, pointing to the New menu, and then clicking Window. The user interface is not changed, but a new window will not be opened, and users will be informed that the command is not available.*
>
> *If you disable this policy or do not configure it, users can open a new browser window from the File menu.*
>
> *Caution: This policy does not prevent users from opening a new browser window by right clicking, and then clicking the Open in New Window command. To prevent users from using the shortcut menu to open new browser windows, you should also set the "Disable Open in New Window menu option" policy, which disables this command on the shortcut menu, or the "Disable context menu" policy, which disables the entire shortcut menu.*

- File menu: Disable Open menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from opening a file or Web page from the File menu in Internet Explorer.*
>
> *If you enable this policy, the Open dialog box will not appear when users click the Open command on the File menu. If users click the Open command, they will be notified that the command is not available.*
>
> *If you disable this policy or do not configure it, users can open a Web page from the browser File menu.*

*Caution: This policy does not prevent users from right-clicking a link on a Web page, and then clicking the Open or Open in New Window command. To prevent users from opening Web pages by using the shortcut menu, set the "Disable Open in New Window menu option" policy, which disables this command on the shortcut menu, or the "Disable context menu" policy, which disables the entire shortcut menu.*

- File menu: Disable Save As Web Page Complete

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from saving the complete contents that are displayed on or run from a Web page, including the graphics, scripts, linked files, and other elements. It does not prevent users from saving the text of a Web page.*

*If you enable this policy, the Web Page, Complete file type option will be removed from the Save as Type drop-down box in the Save Web Page dialog box. Users can still save Web pages as hypertext markup language (HTML) files or as text files, but graphics, scripts, and other elements are not saved. To display the Save Web Page dialog box, users click the File menu, and then click the Save As command.*

*If you disable this policy or do not configure it, users can save all elements on a Web page.*

*The "File menu: Disable Save As... menu option" policy, which removes the Save As command, takes precedence over this policy. If it is enabled, this policy is ignored.*

- File menu: Disable closing the browser and Explorer windows

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from closing Internet Explorer and Windows Explorer.*

*If you enable this policy, the Close command on the File menu will appear dimmed.*

*If you disable this policy or do not configure it, users are not prevented from closing the browser or Windows Explorer.*

*Note: The X button in the top right corner of the program will not work; if users click the X button, they will be informed that the command is not available.*

- View menu: Disable Source menu option

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from viewing the HTML source of Web pages by clicking the Source command on the View menu.*

*If you enable this policy, the Source command on the View menu will appear dimmed.*

*If you disable this policy or do not configure it, then users can view the HTML source of Web pages from the browser View menu.*

*Caution: This policy does not prevent users from viewing the HTML source of a Web page by right-clicking a Web page to open the shortcut menu, and then clicking View Source. To prevent users from viewing the HTML source of a Web page from the shortcut menu, set the "Disable context menu" policy, which disables the entire shortcut menu.*

- View menu: Disable Full Screen menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from displaying the browser in full-screen (kiosk) mode, without the standard toolbar.*
>
> *If you enable this policy, the Full Screen command on the View menu will appear dimmed, and pressing F11 will not display the browser in a full screen.*
>
> *If you disable this policy or do not configure it, users can display the browser in a full screen.*
>
> *This policy is intended to prevent users from displaying the browser without toolbars, which might be confusing for some beginning users.*

- Hide Favorites menu

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from adding, removing, or editing the list of Favorite links.*
>
> *The Favorites list is a way to store popular links for future use.*
>
> *If you enable this policy, the Favorites menu is removed from the interface, and the Favorites button on the browser toolbar appears dimmed. The Add to Favorites command on the shortcut menu is disabled; when users click it, they are informed that the command is unavailable.*
>
> *If you disable this policy or do not configure it, users can manage their Favorites list.*
>
> *This policy is intended to ensure that users maintain consistent lists of favorites across your organization.*
>
> *Note: If you enable this policy, users also cannot click Synchronize on the Tools menu to manage their favorite links that are set up for offline viewing.*

- Tools menu: Disable Internet Options…menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from opening the Internet Options dialog box from the Tools menu in Internet Explorer.*
>
> *If you enable this policy, users cannot change their Internet options, such as default home page, cache size, and connection and proxy settings, from the browser Tools menu. When users click the Internet Options command on the Tools menu, they are informed that the command is unavailable.*
>
> *If you disable this policy or do not configure it, users can change their Internet settings from the browser Tools menu.*
>
> *Caution: This policy does not prevent users from viewing and changing Internet settings by clicking the Internet Options icon in Windows Control Panel.*
>
> *Also, see policies for Internet options in the \Administrative Templates\Windows Components\Internet Explorer and in \Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel folders.*

- Help menu: Disable Remove ‘Tip of the Day’ menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from viewing or changing the Tip of the Day interface in Internet Explorer.*
>
> *If you enable this policy, the Tip of the Day command is removed from the Help menu.*
>
> *If you disable this policy or do not configure it, users can enable or disable the Tip of the Day, which appears at the bottom of the browser.*

- Help menu: Remove ‘For Netscape Users’ menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from displaying tips for users who are switching from Netscape.*
>
> *If you enable this policy, the For Netscape Users command is removed from the Help menu.*
>
> *If you disable this policy or do not configure it, users can display content about switching from Netscape by clicking the For Netscape Users command on the Help menu.*
>
> *Caution: Enabling this policy does not remove the tips for Netscape users from the Internet Explorer Help file.*

- Help menu: Remove ‘Tour’ menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from running the Internet Explorer Tour from the Help menu in Internet Explorer.*
>
> *If you enable this policy, the Tour command is removed from the Help menu.*
>
> *If you disable this policy or do not configure it, users can run the tour from the Help menu.*

- Help menu: Remove ‘Send Feedback’ menu option

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from sending feedback to Microsoft by clicking the Send Feedback command on the Help menu.*
>
> *If you enable this policy, the Send Feedback command is removed from the Help menu.*
>
> *If you disable this policy or do not configure it, users can fill out an Internet form to provide feedback about Microsoft products.*

- Disable Context menu

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents the shortcut menu from appearing when users click the right mouse button while using the browser.*

*If you enable this policy, the shortcut menu will not appear when users point to a Web page, and then click the right mouse button.*

*If you disable this policy or do not configure it, users can use the shortcut menu.*

*This policy can be used to ensure that the shortcut menu isn't used as an alternate method of running commands that have been removed from other parts of the interface.*

- Disable Open in New Window menu option

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents using the shortcut menu to open a link in a new browser window.*

*If you enable this policy, users cannot point to a link, click the right mouse button, and then click the Open in New Window command.*

*If you disable this policy or do not configure it, users can open a Web page in a new browser window by using the shortcut menu.*

*This policy can be used in coordination with the "File menu: Disable New menu option" policy, which prevents users from opening the browser in a new window by clicking the File menu, pointing to New, and then clicking Window.*

*Note: When users click the Open in New Window command, the link will not open in a new window and they will be informed that the command is not available.*

- Disable Save this program to disk option

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from saving a program or file that Internet Explorer has downloaded to the hard disk.*

*If you enable this policy, users cannot save a program to disk by clicking the Save This Program to Disk command while attempting to download a file. The file will not be downloaded and users will be informed that the command is not available.*

*If you disable this policy or do not configure it, users can download programs from their browsers.*

*Toolbars*

- Disable customizing browser toolbar buttons

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from determining which buttons appear on the Internet Explorer and Windows Explorer standard toolbars.*

*If you enable this policy, the Customize command on the Toolbars submenu of the View menu will be removed.*

*If you disable this policy or do not configure it, users can customize which buttons appear on the Internet Explorer and Windows Explorer toolbars.*

> *This policy can be used in coordination with the "Disable customizing browser toolbars" policy, which prevents users from determining which toolbars are displayed in Internet Explorer and Windows Explorer.*

- Disable customizing browser toolbars

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from determining which toolbars are displayed in Internet Explorer and Windows Explorer.*
>
> *If you enable this policy, the list of toolbars, which users can display by clicking the View menu and then pointing to the Toolbars command, will appear dimmed.*
>
> *If you disable this policy or do not configure it, users can determine which toolbars are displayed in Windows Explorer and Internet Explorer.*
>
> *This policy can be used in coordination with the "Disable customizing browser toolbar buttons" policy, which prevents users from adding or removing toolbars from Internet Explorer.*

- Configure Toolbar Buttons

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the administrator may configure which toolbar buttons appear on the toolbar.*
>
> *Specifies which buttons will be displayed on the standard toolbar in Internet Explorer.*
>
> *If you enable this policy, you can specify whether or not each button will be displayed by selecting or clearing the check boxes for each button.*
>
> *If you disable this policy or do not configure it, the standard toolbar will be displayed with its default settings, unless users customize it.*

### *Persistence Behavior*

- File size limits for Local Machine zone

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the default setting per domain is: 1024 kilobytes. The default setting per document is: 128 kilobytes.*
>
> *Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Local Computer security zone.*
>
> *If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.*
>
> *If you disable this policy or do not configure it, you cannot set this limit.*
>
> *Note: This setting does not appear in the user interface.*

- File size limits for Intranet zone

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting per domain is: 10,240 kilobytes. The default setting per document is: 512 kilobytes.*

*Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Local Intranet security zone.*

*If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.*

*If you disable this policy or do not configure it, you cannot set this limit.*

*Note: This setting does not appear in the user interface.*

- File size limits for Trusted Sites zone

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting per domain is: 1024 kilobytes. The default setting per document is: 128 kilobytes.*

*Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Trusted Sites security zone.*

*If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.*

*If you disable this policy or do not configure it, you cannot set this limit.*

*Note: This setting does not appear in the user interface.*

- File size limits for Internet zone

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting per domain is: 1024 kilobytes. The default setting per document is: 128 kilobytes.*

*Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Internet security zone.*

*If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.*

*If you disable this policy or do not configure it, you cannot set this limit.*

*Note: This setting does not appear in the user interface.*

- File size limits for Restricted Sites zone

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting per domain is: 640 kilobytes. The default setting per document is: 64 kilobytes.*

*Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Restricted Sites security zone.*

*If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.*

*If you disable this policy or do not configure it, you cannot set this limit.*

*Note: This setting does not appear in the user interface.*



### *Administrator Approved Controls*

- Media Player

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following: Active Movie Control or Windows Media Player.*

*Designates the Media Player ActiveX control as administrator approved.*

*This control is used for playing sounds, videos, and other media.*

*If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run.*

*If you disable this policy or do not configure it, this control will not be designated as administrator approved.*

*To specify how administrator-approved controls are handled for each security zone, carry out the following steps:*

*1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.*

*2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.*

*3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.*

*4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.*

- Menu Controls

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following: MCSiMenu, PopupMenu Object, or Ikonic Menu Control.*

*Designates a set of Microsoft ActiveX controls used to manipulate pop-up menus in the browser as administrator approved.*

*If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run.*

*If you disable this policy or do not configure it, these controls will not be designated as administrator approved.*

*To specify a control as administrator approved, click Enabled, and then select the check box for the control:*

*-- MCSiMenu - enables Web authors to control the placement and appearance of Windows pop-up menus on Web pages*

*-- Popup Menu Object - enables Web authors to add pop-up menus to Web pages*

*To specify how administrator-approved controls are handled for each security zone, carry out the following steps:*

*1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.*

*2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.*

*3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.*

*4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.*

- Microsoft Agent

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use the check box to allow Microsoft Agent Control.*

*Designates the Microsoft Agent ActiveX control as administrator approved.*

*Microsoft Agent is a set of software services that supports the presentation of software agents as interactive personalities within the Microsoft Windows interface.*

*If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run.*

*If you disable this policy or do not configure it, these controls will not be designated as administrator approved.*

*To specify how administrator-approved controls are handled for each security zone, carry out the following steps:*

*1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.*

*2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.*

*3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.*

*4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.*

- Microsoft Chat

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use the check box to activate MSChat Control.*

*Designates the Microsoft Chat ActiveX control as administrator approved.*

*This control is used by Web authors to build text- and graphical-based Chat communities for real-time conversations on the Web.*

*If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run.*

*If you disable this policy or do not configure it, this control will not be designated as administrator approved.*

*To specify how administrator-approved controls are handled for each security zone, carry out the following steps:*

*1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.*

*2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.*

*3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.*

*4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.*

- Microsoft Survey Control

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use the check box to activate the Microsoft Survey Control.*

*No explanation given.*

- Shockwave Flash

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use the check box to activate Shockwave Flash.*

*No explanation given.*

- NetShow File Transfer Control

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use the check box to activate NetShow Transfer Control.*

*No explanation given.*

- DHTML Edit Control

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use the check box to activate the DHTML Edit Control.*

*No explanation given.*

- Microsoft Scriptlet Component

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use the check box to activate the Microsoft Scriptlet Component.*

*No explanation given.*

- Carpoint

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled ,the administrator may use the check box to activate the CarPoint AutoPricer Control.*

*Designates the Microsoft Network (MSN) Carpoint automatic pricing control as administrator approved.*

*This control enables enhanced pricing functionality on the Carpoint Web site, where users can shop for and obtain information about vehicles.*

*If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run.*

*If you disable this policy or do not configure it, this control will not be designated as administrator approved.*

*To specify how administrator-approved controls are handled for each security zone, carry out the following steps:*

*1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.*

*2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.*

*3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.*

*4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.*

- Investor

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may choose from among the following: MSN Investor Chart Control or MS Investor Ticker*

*Designates a set of Microsoft Network (MSN) Investor controls as administrator approved.*

*These controls enable users to view updated lists of stocks on their Web pages.*

*If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run.*

*If you disable this policy or do not configure it, these controls will not be designated as administrator approved.*

*Select the check boxes for the controls that you want to designate as administrator approved.*

*To specify how administrator-approved controls are handled for each security zone, carry out the following steps:*

*1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.*

*2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.*

*3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.*

*4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.*

- MSNBC

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use the check box to activate the MSNBC News Control.*

*Designates a set of MSNBC controls as administrator approved.*

*These controls enable enhanced browsing of news reports on the MSNBC Web site.*

*If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run.*

*If you disable this policy or do not configure it, these controls will not be designated as administrator approved.*

*Select the check boxes for the controls that you want to designate as administrator approved.*

*To specify how administrator-approved controls are handled for each security zone, carry out the following steps:*

*1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.*

*2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.*

*3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.*

*4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved.*

### Windows Explorer

- Enable Classic Shell

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables Active Desktop, Web view, and thumbnail views. Also, users cannot configure their system to open items by single-clicking (such as in Mouse in Control Panel). As a result, the user interface looks and operates like the interface for Windows NT 4.0 and users cannot restore the new features.*

*Note: This policy takes precedence over the "Enable Active Desktop" policy. If both policies are enabled, Active Desktop is disabled.*

*Also, see the "Disable Active Desktop" policy in User Configuration\Administrative Templates\Desktop\Active Desktop and the "Remove the Folder Options menu item from the Tools menu" policy in User Configuration\Administrative Templates\Windows Components\Windows Explorer.*

- Remove the Folder Options menu item from the Tool menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Folder Options item from all Windows Explorer menus and removes the Folder Options item from Control Panel. As a result, users cannot use the Folder Options dialog box.*

*The Folder Options dialog box lets users set many properties of Windows Explorer, such as Active Desktop, Web view, Offline Files, hidden system files, and file types.*

*Also, see the "Enable Active Desktop" policy in User Configuration\AdministrativeTemplates\Desktop\Active Desktop and the "Disable user configuration of Offline Files" policy in User Configuration\Administrative Templates\Network\Offline Files.*

- Remove File menu from Windows Explorer

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the File menu from My Computer and Windows Explorer.*

*This policy does not prevent users from using other methods to perform tasks available on the File menu.*

- Remove “Map Network Drive” and “Disconnect Network Drive”

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from using Windows Explorer or My Network Places to connect to other computers or to close existing connections.*

*If you enable this policy, the system removes the Map Network Drive and Disconnect Network Drive commands from the toolbar and Tools menus in Windows Explorer and My Network Places and from menus that appear when you right-click the Windows Explorer or My Network Places icons. It also removes the Add Network Place option from My Network Places.*

*This policy does not prevent users from connecting to another computer by typing the name of a shared folder in the Run dialog box.*

- Remove Search button from Windows Explorer

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Search button from the Windows Explorer toolbar.*

*This policy removes the Search button from the Standard Buttons toolbar that appears in Windows Explorer and other programs that use the Windows Explorer window, such as My Computer and My Network Places.*

*It does not remove the Search button or affect any search features of Internet browser windows, such as the Internet Explorer window.*

*This policy does not affect the Search items on the Windows Explorer context menu or on the Start menu. To remove Search from the Start menu, use the "Remove Search menu from Start menu" policy (in User Configuration\Administrative Templates\Start Menu & Taskbar). To hide all context menus, use the "Disable Windows Explorer's default context menu" policy.*

- Disable Windows Explorer's default context menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes shortcut menus from the desktop and Windows Explorer. Shortcut menus appear when you right-click an item.*

*If you enable this policy, menus do not appear when you right-click the desktop or when you right-click the items in Windows Explorer. This policy does not prevent users from using other methods to issue commands available on the shortcut menus.*

- Hide the Manage item on the Windows Explorer context menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Manage item from the Windows Explorer context menu. This context menu appears when you right-click Windows Explorer or My Computer.*

*The Manage item opens Computer Management (Compmgmt.msc), a console tool which includes many of the primary Windows 2000 administrative tools, such as Event Viewer, Device Manager, and Disk Management. You must be an administrator to use many of the features of these tools.*

*This policy does not remove the Computer Management item from the Start Menu (Start, Programs, Administrative Tools, Computer Management), nor does it prevent users from using other methods to start Computer Management.*

*Tip: To hide all context menus, use the "Disable Windows Explorer's default context menu" policy.*

- Only allow approved Shell extensions

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Directs Windows to start only the user interface extensions that the system security or the user have approved.*

*When the system detects that the user is downloading an external program that runs as part of the Windows user interface, the system searches for a digital certificate or requests that the user approve the action. If you enable this policy, Windows only starts approved programs.*

*This policy is designed to protect the system from damage from programs that do not operate correctly or are intended to cause harm.*

*Note: To view the approved user interface extensions for a system, start a registry editor (Regedt32 or Regedit). The system stores entries representing approved user interface extensions on a system in the following registry key:*

*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved.*

- Do not track Shell shortcuts during roaming

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether Windows traces shortcuts back to their sources when it cannot find the target on the user's system.*

*Shortcut files typically include an absolute path to the original target file as well as the relative path to the current target file. When the system cannot find the file in the current target path, then, by default, it searches for the target in the original path. If the shortcut has been copied to a different computer, the original path might lead to a network computer, including external resources, such as an Internet server.*

*If you enable this policy, Windows only searches the current target path. It does not search for the original path even when it cannot find the target file in the current target path.*

- Hide these specified drives in My Computer

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled the default setting is: Restrict all drives. The administrator may choose from among the following:*

*- Restrict A and B drives only*

*- Restrict C drive only*

*- Restrict D drive only*

*- Restrict A, B, and C drives only*

*- Restrict A, B,C, and D drives only*

*- Restrict all drives*

*- Do not restrict drives*

*Removes the icons representing selected hard drives from My Computer, Windows Explorer, and My Network Places. Also, the drive letters representing the selected drives do not appear in the standard Open dialog box.*

*To use this policy, select a drive or combination of drives from the drop-down list. To display all drives, disable this policy or select the "Do not restrict drives" option from the drop-down list.*

*Note: This policy removes the drive icons. Users can still gain access to drive contents by using other methods, such as by typing the path to a directory on the drive in the Map Network Drive dialog box, in the Run dialog box, or in a command window.*

*Also, this policy does not prevent users from using programs to access these drives or their contents. And, it does not prevent users from using the Disk Management snap-in to view and change drive characteristics.*

*Also, see the "Prevent access to drives from My Computer" policy.*

- Prevent access to drives from My Computer

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: Restrict all drives. The administrator may choose from among the following:*

*- Restrict A and B drives only*

*- Restrict C drive only*

*- Restrict D drive only*

*- Restrict A, B, and C drives only*

*- Restrict A, B,C, and D drives only*

*- Restrict all drives*

*- Do not restrict drives*

*Prevents users from using My Computer to gain access to the content of selected drives.*

*If you enable this policy, users cannot view the contents of the selected drives in My Computer, Windows Explorer, or My Network Places. Also, they cannot use the Run dialog box, the Map Network Drive dialog box, or the Dir command to view the directories on these drives.*

*To use this policy, select a drive or combination of drives from the drop-down list. To allow access to all drive directories, disable this policy or select the "Do not restrict drives" option from the drop-down list.*

*Note: The icons representing the specified drives still appear in My Computer, but if users double-click the icons, a message appears explaining that a policy prevents the action.*

*Also, this policy does not prevent users from using programs to access local and network drives. And, it does not prevent them from using the Disk Management snap-in to view and change drive characteristics.*

*Also, see the "Hide these specified drives in My Computer" policy.*

- Hide Hardware tab

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Hardware tab.*

*This policy removes the Hardware tab from Mouse, Keyboard, and Sounds and Multimedia in Control Panel. It also removes the Hardware tab from the Properties dialog box for all local drives, including hard drives, floppy disk drives, and CD-ROM drives. As a result, users cannot use the Hardware tab to view or change the device list or device properties, or use the Troubleshoot button to resolve problems with the device.*

- Disable UI to change menu animation settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from selecting the option to animate the movement of windows, menus, and lists.*

*If you enable this policy, the "Use transition effects for menus and tooltips" option in Display in Control Panel is disabled.*

*Effects, such as animation, are designed to enhance the user's experience but might be confusing or distracting to some users.*

- Disable UI to change keyboard navigation indicator setting

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the "Hide keyboard navigation indicators until I use the ALT key" option in Display in Control Panel.*

*When this Display Properties option is selected, the underlining that indicates a keyboard shortcut character (hot key) does not appear on menus until you press ALT.*

*Effects, such as transitory underlines, are designed to enhance the user's experience but might be confusing or distracting to some users.*

- Disable DFS tab

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the DFS tab from Windows Explorer.*

*This policy removes the DFS tab from Windows Explorer and from other programs that use the Windows Explorer browser, such as My Computer. As a result, users cannot use this tab to view or change the properties of the Distributed File System (DFS) shares available from their computer.*

*This policy does not prevent users from using other methods to configure DFS.*

- No “Computers Near Me” in My Network Places

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes computers in the user's workgroup and domain from lists of network resources in Windows Explorer and My Network Places.*

*If you enable this policy, the system removes the "Computers Near Me" option and the icons representing nearby computers from My Network Places. This policy also removes these icons from the Map Network Drive browser.*

*This policy does not prevent users from connecting to computers in their workgroup or domain by other commonly used methods, such as typing the share name in the Run dialog box or the Map Network Drive dialog box.*

*To remove network computers from lists of network resources, use the "No Entire Network in My Network Places" policy.*

- No “Entire Network” in My Network Places

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes all computers outside of the user's workgroup or local domain from lists of network resources in Windows Explorer and My Network Places.*

*If you enable this policy, the system removes the Entire Network option and the icons representing networked computers from My Network Places and from the browser associated with the Map Network Drive option.*

*This policy does not prevent users from viewing or connecting to computers in their workgroup or domain. It also does not prevent users from connecting to remote computers by other commonly used methods, such as by typing the share name in the Run dialog box or the Map Network Drive dialog box.*

*To remove computers in the user's workgroup or domain from lists of network resources, use the "No "Computers Near Me" in My Network Places" policy.*

- Maximum number of recent documents

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 15.The minimum permitted value is 1. The maximum permitted value is 9999.*

*Determines how many shortcuts the system can display in the Documents menu on the Start menu.*

*The Documents menu contains shortcuts to the non-program files the user has most recently opened. By default, the system displays shortcuts to the 15 most recently opened documents.*

- Do not request alternate credentials

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from submitting alternate logon credentials to install a program.*

*This policy suppresses the "Install Program As Other User" dialog box for local and network installations. This dialog box, which prompts the current user for the user name and password of an administrator, appears when users who are not administrators try to install programs locally on their computers. This policy allows administrators who have logged on as regular users to install programs without logging off and logging on again using their administrator credentials.*

*Many programs can be installed only by an administrator. If you enable this policy and a user does not have sufficient permissions to install a program, the installation continues with the current user's logon credentials. As a result, the installation might fail, or it might complete but not include all features. Or it might appear to complete successfully, but the installed program might not operate correctly.*

*If you disable this policy, or do not configure it, the "Install Program As Other User" dialog box appears whenever users install programs locally on the computer.*

*By default, users are not prompted for alternate logon credentials when installing programs from a network share. If enabled, this policy overrides the "Request credentials for network installations" policy.*

- Request credential for network installations

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prompts users for alternate logon credentials during network-based installations.*

*This policy displays the "Install Program As Other User" dialog box even when a program is being installed from files on a network computer across a local area network connection.*

*If you disable this policy or do not configure it, this dialog box appears only when users are installing programs from local media.*

*The "Install Program as Other User" dialog box prompts the current user for the user name and password of an administrator. This policy allows administrators who have logged on as regular users to install programs without logging off and logging on again using their administrator credentials.*

*If the dialog box does not appear, the installation proceeds with the current user's permissions. If these permissions are not sufficient, the installation might fail, or it might complete but not include all features. Or, it might appear to complete successfully, but the installed program might not operate correctly.*

*Note: If enabled, the "Do not request alternate credentials" policy takes precedence over the setting for this policy. When that policy is enabled, users are not prompted for alternate logon credentials on any installation.*

### *Common Open File Dialog*

- Hide the common dialog places bar

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the shortcut bar from the Open dialog box.*

*This policy, and others in this folder, lets you remove new features added in Windows 2000, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs.*

*To see an example of the standard Open dialog box, run Notepad and, from the File menu, click Open.*

- Hide the common dialog back button

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Back button from the Open dialog box.*

*This policy, and others in this folder, lets you remove new features added in Windows 2000, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs.*

*To see an example of the standard Open dialog box, run Notepad and, from the File menu, click Open.*

- Hide the dropdown list of recent files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the list of most recently used files from the Open dialog box.*

*If you disable this policy or do not configure it, the "File name" field includes a dropdown list of recently used files. If you enable this policy, the "File name" field is a simple text box. Users must browse directories to find a file or type a file name in the text box.*

*This policy, and others in this folder, lets you remove new features added in Windows 2000, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs.*

*To see an example of the standard Open dialog box, run Notepad and, from the File menu, click Open.*

### Microsoft Management Console

- Restrict the user from entering author mode

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from entering author mode.*

*This policy prevents users from opening the MMC in author mode, from explicitly opening console files in author mode, and from opening any console files that open in author mode by default.*

*As a result, users cannot create console files or add or remove snap-ins. Also, because they cannot open author-mode console files, they cannot use the tools that the files contain.*

*This policy permits users to open MMC user-mode console files, such as those on the Administrative Tools menu in Windows 2000 Server. However, users cannot open a blank MMC console window, on the Start menu. (To open the MMC, click Start, click Run, and type MMC.) Users also cannot open a blank MMC console window from a command prompt.*

*If you disable this policy or do not configure it, users can enter author mode and open author-mode console files.*

- Restrict users to the explicitly permitted use of snap-ins

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Lets you selectively permit or prohibit the use of Microsoft Management Console (MMC) snap-ins.*

*-- If you enable this policy, all snap-ins are prohibited, except those that you explicitly permit. Use this setting if you plan to prohibit use of most snap-ins.*

*To explicitly permit a snap-in, open the Restricted/Permitted snap-ins policy folder and then enable the policies representing the snap-in you want to permit. If a snap-in policy in the folder is disabled or not configured, the snap-in is prohibited.*

*-- If you disable this policy or do not configure it, all snap-ins are permitted, except those that you explicitly prohibit. Use this setting if you plan to permit use of most snap-ins.*

*To explicitly prohibit a snap-in, open the Restricted/Permitted snap-ins policy folder and then disable the policies representing the snap-ins you want to prohibit. If a snap-in policy in the folder is enabled or not configured, the snap-in is permitted.*

*When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.*

*Note: If you enable this policy, and do not enable any policies in the Restricted/Permitted snap-ins folder, users cannot use any MMC snap-ins.*

*Restricted/Permitted snap-ins*

- Active Directory Users and Computers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Active Directory Domains and Trusts

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Active Directory Sites and Services

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Certificates

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Component Services

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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 Management

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Device Manager

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Disk Management

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Disk Defragmenter

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Distributed File System

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Event Viewer

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- FAX Service

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Indexing Service

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Internet Authentication Service (IAS)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Internet Information Services

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*



- IP Security

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Local Users and Groups

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Performance Logs and Alerts

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- QoS Admission Control

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Removable Storage Management

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Routing and Remote Access

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Security Configuration and Analysis

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Security Templates

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Services

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Shared Folders

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- System Information

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Telephony

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Terminal Services Configuration

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- WMI Control

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

*Extension snap-ins*

- AppleTalk Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Certification Authority

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Connection Sharing (NAT)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- DCOM Configuration Extension

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Device Manager

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- DHCP Relay Management

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Event Viewer

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- IAS Logging

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- IGMP Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- IP Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- IPX RIP Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- IPX Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- IPX SAP Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Logical and Mapped Drives

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- OSPF Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Public Key Policies

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- RAS Dialin – User Mode

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Remote Access

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Removable Storage

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- RIP Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Routing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Send Console Message

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Service Dependencies

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- SMTP Protocol

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- SNMP

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- System Properties

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

### *Group Policy*

- Group Policy snap-in

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Group Policy Tab for Active Directory Tools

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Administrative Templates (Computers)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Administrative Templates (Users)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Folder Redirection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Internet Explorer Maintenance

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Remote Installation Services

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Permits or prohibits use of this snap-in.*
>
> *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*
>
> *If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Scripts (Logon/Logoff)

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Scripts (Startup/Shutdown)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Security Settings

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Software Installation (Computers)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

- Software Installation (Users)

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits or prohibits use of this snap-in.*

*If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

*If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy 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 policy. If this policy 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 policy. If this policy 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.*

### Task Scheduler

- Hide Property Pages

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from viewing and changing the properties of an existing task.*

*This policy removes the Properties item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview.*

*This policy prevents users from viewing and changing characteristics such as the program the task runs, its schedule details, idle time and power management settings, and its security context.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: This policy affects existing tasks only. To prevent users from changing the properties of newly created tasks, use the "Disable Advanced Menu" policy.*

- Prevent Task Run or End

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from starting and stopping tasks manually.*

*This policy removes the Run and End Task items from the context menu that appears when you right-click a task. As a result, users cannot start tasks manually or force tasks to end before they are finished.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Disable Drag-and-Drop

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder.*

*This policy disables the Cut, Copy, Paste, and Paste shortcut items on the context menu and the Edit menu in Scheduled Tasks. It also disables the drag-and-drop features of the Scheduled Tasks folder.*

*As a results, users cannot add new scheduled tasks by dragging, moving, or copying a document or program into the Scheduled tasks folder.*

*This policy does not prevent users from using other methods to create new tasks and it does not prevent users from deleting tasks.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Disable New Task Creation

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from creating new tasks.*

*This policy removes the Add Scheduled Task item that starts the New Task wizard. Also, the system does not respond when users try to move, paste, or drag programs or documents into the Scheduled Tasks folder.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Important: This policy does not prevent administrators of a computer from using At.exe to create new tasks or prevent administrators from submitting tasks from remote computers.*

- Disable Task Deletion

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from deleting tasks from the Scheduled Tasks folder.*

*This policy removes the Delete item from the Edit menu in the Scheduled Tasks folder and from the menu that appears when you right-click a task. Also, the system does not respond when users try to cut or drag a task from the Scheduled Tasks folder.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Important: This policy does not prevent administrators of a computer from using At.exe to delete tasks.*

*Disable Advanced Menu*

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from viewing or changing the properties of newly created tasks.*

*This policy removes the "Open advanced properties for this task when I click Finish" item from the last page of the Scheduled Task wizard.*

*This policy prevents users from viewing and changing task characteristics, such as the program the task runs, details of its schedule, idle time and power management settings, and its security context. It is designed to simplify task creation for beginning users.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: This policy affects newly created tasks only. To prevent users from changing the properties of existing tasks, use the "Hide Property Pages" policy.*

- Prohibit Browse

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Limits newly scheduled to items on the user's Start menu and prevents the user from changing the scheduled program for existing tasks.*

*This policy removes the Browse button from the Schedule Task wizard and from the Task tab of the properties dialog box for a task. Also, users cannot edit the "Run" box or the "Start in" box that determine the program and path for a task.*

*As a result, when users create a task, they must select a program from the list in the Scheduled Task wizard, which displays only the tasks that appear on the Start menu and its submenus. Once a task is created, users cannot change the program a task runs.*

*Important: This policy does not prevent users from creating a new task by pasting or dragging any program into the Scheduled Tasks folder. To prevent this action, use the "Disable Drag-and-Drop" policy.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

### Windows Installer

- Always install with elevated privileges

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must use the check box to force this setting on. This policy must be set for the machine and the user to be enforced.*

*Directs Windows Installer to use system permissions when it installs any program on the system.*

*This policy extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add/Remove Programs in Control Panel. This policy lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.*

*If you disable this policy or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.*

*Note: This policy appears both in the Computer Configuration and User Configuration folders. To make this policy effective, you must enable the policy in both folders.*

*Caution: Skilled users can take advantage of the permissions this policy grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this policy is not guaranteed to be secure.*

- Search order

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: nmu. Order to which to search the three types of sources.*

*Leave letter(s) out to remove that type of source from the search.*

*Specifies the order in which Windows Installer searches for installation files.*

*By default, the Windows Installer searches the network first, then removable media (floppy drive, CD-ROM, or DVD), and finally, the Internet (URL).*

*To change the search order, enable the policy, and then type the letters representing each file source in the order that you want Windows Installer to search.:*

*-- "n" represents the network;*

*-- "m" represents media;*

*-- "u" represents URL, or the Internet.*

*To exclude a file source, omit or delete the letter representing that source type.*

- Disable rollback

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must use the checkbox to force this setting on. This policy may be set for the machine or for the user.*

*Prohibits Windows Installer from generating and saving the files it needs to reverse an interrupted or unsuccessful installation.*

*This policy prevents Windows Installer from recording the original state of the system and sequence of changes it makes during installation. It also prevents Windows Installer from retaining files it intends to delete later. As a result, Windows installer cannot restore the computer to its original state if the installation does not complete.*

*This policy is designed to reduce the amount of temporary disk space required to install programs. Also, it prevents malicious users from interrupting an installation to gather data about the internal state of the computer or to search secure system files. However, because an incomplete installation can render the system or a program inoperable, do not use this policy unless essential.*

*This policy appears in the Computer Configuration and User Configuration folders. If the policy is enabled in either folder, it is considered be enabled, even if it is explicitly disabled in the other folder.*

- Disable media source for any install

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must use the checkbox to force this setting on.*

*Prevents users from installing programs from removable media.*

*If a user tries to install a program from removable media, such as CD-ROMs, floppy disks, and DVDs, a message appears, stating that the feature cannot be found.*

*This policy applies even when the installation is running in the user's security context.*

*If you disable this policy or do not configure it, users can install from removable media when the installation is running in their own security context, but only system administrators can use removable media when an installation is running with elevated system privileges, such as installations offered on the desktop or in Add/Remove Programs.*

*Also, see the "Enable user to use media source while elevated policy" in Computer Configuration\Administrative Templates\Windows Components\Windows Installer.*

*Also, see the "Hide the "Add a program from CD-ROM or floppy disk"" policy in User Configuration\Administrative Templates\Control Panel\Add/Remove Programs.*

## Start Menu & Taskbar

- Remove user's folder from the Start Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden.*

*This policy is designed for use with redirected folders. Redirected folders appear on the main (bottom) section of the Start menu. However, the original, user-specific version of the folder still appears on the top section of the Start menu. Because the appearance of two folders with the same name might confuse users, you can use this policy to hide user-specific folders.*

*Note that this policy hides all user-specific folders, not just those associated with redirected folders.*

*If you enable this policy, no folders appear on the top section of the Start menu. If users add folders to the Start Menu directory in their user profiles, the folders appear in the directory but not on the Start menu.*

*If you disable this policy or do not configured it, Windows 2000 displays folders on both sections of the Start menu.*

- Disable and remove links to Windows Update

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from connecting to the Windows Update Web site.*

*This policy blocks user access to the Windows Update Web site at http://windowsupdate.microsoft.com. Also, the policy removes the Windows Update hyperlink from the Start Menu and from the Tools menu in Internet Explorer.*

*Windows Update, the online extension of Windows, offers software updates to keep a user's system up-to-date. The Windows Update Product Catalog determines any system files, security*

*fixes, and Microsoft updates that users need and shows the newest versions available for download.*

*Also, see the "Hide the "Add programs from Microsoft" option" policy.*

- Remove common program groups from Start Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes items in the All Users profile from the Programs menu on the Start menu.*

*By default, the Programs menu contains items from the All Users profile and items from the user's profile. If you enable this policy, only items in the user's profile appear in the Programs menu.*

*Tip: To see the Program menu items in the All Users profile, on the system drive, go to Documents and Settings\All Users (WINNT)\Start Menu\Programs.*

- Remove Documents menu from Start Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Documents menu from the Start menu.*

*The Documents menu contains links to the non-program files that users have most recently opened. It appears so that users can easily reopen the documents.*

*You can use this policy, in coordination with the "Do not keep history of recently opened documents" and "Clear history of recently opened documents on exit" policies in this folder, to customize your policy for managing access to recently opened files.*

*Also, see the Maximum number of Recent documents" policy located in User Configuration\Administrative Templates\Windows Components\Windows Explorer.*

- Disable programs on Settings menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents Control Panel, Printers, and Network and Dial-up Connections from running.*

*This policy removes the Control Panel, Printers, and Network and Dial-up Connection folders from Settings on the Start menu, and from My Computer and Windows Explorer. It also prevents the programs represented by these folders (such as Control.exe) from running.*

*However, users can still start Control Panel items by using other methods, such as right-clicking the desktop to start Display or right-clicking My Computer to start System.*

*Also, see the "Disable Control Panel," "Disable Display in Control Panel," and "Remove Network and Dial-up Connections from Start Menu" policies.*

- Remove Network & Dial-up Connections from Start Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from running Network and Dial-up Connections.*

*This policy prevents the Network and Dial-up Connections folder from opening. This policy also removes Network and Dial-up Connections from Settings on the Start menu.*

*Network and Dial-up Connections still appears in Control Panel and in Windows Explorer, but if users try to start it, a message appears explaining that a policy prevents the action.*

*Also, see the "Disable programs on Settings menu" and "Disable Control Panel" policies and the policies in the Network and Dial-up Connections folder (Computer Configuration and User Configuration\Administrative Templates\Network\Network and Dial-up Connections).*

- Remove Favorites menu from Start Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from adding the Favorites menu to the Start menu.*

*The Favorites menu does not appear on the Start menu by default. To display the Favorites menu, click Start, point to Settings, click Taskbar & Start Menu, click the Start Menu Options tab, and then, under Start Menu Settings, select Display Favorites. If you enable this policy, the Display Favorites item does not appear in the Start Menu Settings box.*

*The items that appear in the Favorites menu when you install Windows are preconfigured by the system to appeal to most users. However, users can add and remove items from this menu, and system administrators can create a customized Favorites menu for a user group.*

*This policy only affects the Start menu. The Favorites item still appears in Windows Explorer and in Internet Explorer.*

- Remove Search menu from Start Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Search item from the Start Menu and disables some Windows Explorer search elements.*

*This policy removes the Search item from the Start menu and from the context menu that appears when you right-click the Start menu. Also, the system does not respond when users press the Application key (the key with the Windows logo)+ F.*

*In Windows Explorer, the Search item still appears on the Standard buttons toolbar, but the system does not respond when the user presses Ctrl + F. Also, Search does not appear in the context menu when you right-click an icon representing a drive or a folder.*

*This policy affects the specified user interface elements only. It does not affect Internet Explorer and does not prevent the user from using other methods to search.*

*Also, see the "Remove Search button from Windows Explorer" policy in User Configuration\Administrative Templates\Windows Components\Windows Explorer.*

- Remove Help menu from Start Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Help command from the Start menu.*

*This policy only affects the Start menu. It does not remove the Help menu from Windows Explorer and does not prevent users from running Windows 2000 Help.*

- Remove Run menu from Start Menu

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Removes the Run command from the Start menu and removes the New Task (Run) command from Task Manager. Also, users with extended keyboards can no longer display the Run dialog box by pressing Application key (the key with the Windows logo) + R.*
>
> *This policy affects the specified interface only. It does not prevents users from using other methods to run programs.*

- Add Logoff to the Start Menu

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Adds the "Log Off <username>" item to the Start menu and prevents users from removing it.*
>
> *If you enable this policy, the Log Off <username> item appears in the Start menu. This policy also removes the Display Logoff item from Start Menu Options. As a result, users cannot remove the Log Off <username> item from the Start Menu.*
>
> *If you disable this policy or do not configure it, users can use the Display Logoff item to add and remove the Log Off item.*
>
> *This policy affects the Start menu only. It does not affect the Log Off item on the Windows Security dialog box that appears when you press Ctrl+Alt+Del.*
>
> *Tip: To add or remove the Log Off item on a computer, click Start, click Settings, click Taskbar & Start Menu, click the Start Menu Options tab and, in the Start Menu Settings box, click Display Logoff.*
>
> *See also: "Disable Logoff" in User Configuration\Administrative Templates\System\Logon/Logoff.*

- Disable Logoff on the Start Menu

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Removes the "Log Off <username>" item from the Start menu and prevents users from restoring it.*
>
> *If you enable this policy, the Log Off <username> item does not appear in the Start menu. This policy also removes the Display Logoff item from Start Menu Options. As a result, users cannot restore the Log Off <username> item to the Start Menu.*
>
> *If you disable this policy or do not configure it, users can use the Display Logoff item to add and remove the Log Off item.*
>
> *This policy affects the Start menu only. It does not affect the Log Off item on the Windows Security dialog box that appears when you press Ctrl+Alt+Del, and it does not prevent users from using other methods to log off.*
>
> *Tip: To add or remove the Log Off item on a computer, click Start, click Settings, click Taskbar & Start Menu, click the Start Menu Options tab and, in the Start Menu Settings box, click Display Logoff.*
>
> *See also: "Disable Logoff" in User Configuration\Administrative Templates\System\Logon/Logoff.*

- Disable and remove the Shut Down command

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from shutting down or restarting Windows.*
>
> *This policy removes the Shut Down option from the Start menu and disables the Shut Down button on the Windows Security dialog box, which appears when you press CTRL+ALT+DEL.*
>
> *This policy prevents users from using the Windows user interface to shut down the system, although it does not prevent them from running programs that shut down Windows.*
>
> *If you disable this policy or do not configure it, the Shut Down menu option appears, and the Shut Down button is enabled.*

- Disable drag-and-drop context menu on the Start Menu

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from using the drag-and-drop method to reorder or remove items on the Start menu. Also, it removes context menus from the Start menu.*
>
> *If you disable this policy or do not configure it, users can remove or reorder Start menu items by dragging and dropping the item. They can display context menus by right-clicking a Start menu item.*
>
> *This policy does not prevent users from using other methods of customizing the Start menu or performing the tasks available from the context menus.*
>
> *Also, see the "Disable changes to Taskbar and Start Menu Settings" and the "Disable context menu for taskbar" policies.*
>
> *Disable changes to Taskbar and Start Menu Settings*
>
> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Removes the Taskbar & Start Menu item from Settings on the Start menu. This policy also prevents the user from opening the Taskbar Properties dialog box.*
>
> *If the user right-clicks the taskbar and then clicks Properties, a message appears explaining that a policy prevents the action.*

- Disable context menus for the taskbar

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Hides the menus that appear when you right-click the taskbar and items on the taskbar, such as the Start button, the clock, and the taskbar buttons.*
>
> *This policy does not prevent users from using other methods to issue the commands that appear on these menus.*

- Do not keep history of recently opened documents

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents the system from saving shortcuts to documents the user has most recently opened.*

*By default, the system saves a shortcut to each of the non-program files the user most recently opened and displays the shortcuts on the Start menu under Documents. The shortcuts let users easily review and restart recently used documents.*

*If you enable this policy, the system does not save shortcuts to the Documents menu.*

*You can use this policy, in coordination with the "Remove Documents menu from Start Menu" and "Clear history of recently opened documents on exit" policies in this folder, to customize your policy for managing access to recently opened files.*

*If you enable this policy and do not select the "Remove Documents menu from Start Menu" policy, the Documents menu appears on the Start menu, but it is empty.*

*Also, see also the "Maximum number of Recent documents" policy located in UserConfiguration\Administrative Templates\Windows Components\Windows Explorer).*

- Clear history of recently opened documents on exit

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Directs the system to delete the contents of the Documents menu on the Start menu when the user logs off.*

*The Documents menu contains shortcuts to the non-program files the user opened most recently.*

*If you enable this policy, the Documents menu is always empty when the user logs on. Otherwise, when the user logs on again, the Documents menu appears just as it did when the user logged off.*

*You can use this policy, in coordination with the "Remove Documents menu from Start Menu" and "Do not keep history of recently opened documents" policies in this folder to customize your policy for managing access to recently opened files. The system uses this policy only when neither of these related policies are selected.*

- Disable personalized menus

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables personalized menus.*

*Windows 2000 personalizes long menus by moving recently used items to the top of the menu and hiding items that have not been used recently. Users can display the hidden items by clicking an arrow to extend the menu.*

*If you enable this policy, the system does not personalize menus. All menu items appear and remain in standard order. Also, this policy removes the "Use Personalized Menus" option so users do not try to change the setting while a policy is in effect.*

*Note: Personalized menus require user tracking. If you enable the "Disable user tracking" policy, the system disables user tracking and personalized menus, and ignores this policy.*

*Tip: To disable personalized menus without setting a policy, click Start, click Settings, click Taskbar & Start Menu, and, on the General tab, clear the "Use Personalized Menus" option.*

- Disable user tracking

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Disables user tracking.*
>
> *This policy prevents the system from tracking the programs users run, the paths they navigate, and the documents they open. The system uses this information to customize Windows features, such as personalized menus.*
>
> *If you enable this policy, the system does not track these user actions. The system disables customized features that require user tracking information, including personalized menus.*
>
> *Also, see the "Disable personalized menus" policy.*

- Add “Run in Separate Memory Space” check box to Run dialog box

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Lets users run a 16-bit program in a dedicated (not shared) Virtual DOS Machine (VDM) process.*
>
> *All DOS and 16-bit programs run on Windows 2000 in the Windows Virtual DOS Machine program. VDM simulates a 16-bit environment, complete with the DLLs required by 16-bit programs. By default, all 16-bit programs run as threads in a single, shared VDM process. As such, they share the memory space allocated to the VDM process and cannot run simultaneously.*
>
> *Enabling this policy adds a check box to the Run dialog box, giving users the option of running a 16-bit program in its own dedicated NTVDM process. The additional check box is enabled only when a user enters a 16-bit program in the Run dialog box.*

- Do not use the search-based method when resolving shell shortcuts

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents the system from conducting a comprehensive search of the target drive to resolve a shortcut.*
>
> *By default, when the system cannot find the target file for a shortcut (.lnk), it searches all paths associated with the shortcut. If the target file is located on an NTFS partition, the system then uses the target's file ID to find a path. If the resulting path is not correct, it conducts a comprehensive search of the target drive in an attempt to find the file.*
>
> *If you enable this policy, the system does not conduct the final drive search. It just displays a message explaining that the file is not found.*
>
> *Note: This policy only applies to target files on NTFS partitions. FAT partitions do not have this ID tracking and search capability.*
>
> *Also, see the "Do not track Shell shortcuts during roaming" and the "Do not use the tracking-based method when resolving shell shortcuts" policies.*

- Do not use the tracking-based method when resolving shell shortcuts

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents the system from using NTFS tracking features to resolve a shortcut.*

*By default, when the system cannot find the target file for a shortcut (.lnk), it searches all paths associated with the shortcut. If the target file is located on an NTFS partition, the system then uses the target's file ID to find a path. If the resulting path is not correct, it conducts a comprehensive search of the target drive in an attempt to find the file.*

*If you enable this policy, the system does not try to locate the file by using its file ID. It skips this step and begins a comprehensive search of the drive specified in the target path.*

*Note: This policy only applies to target files on NTFS partitions. FAT partitions do not have this ID tracking and search capability.*

*Also, see the "Do not track Shell shortcuts during roaming" and the "Do not use the search-based method when resolving shell shortcuts" policies.*

- Gray unavailable Windows Installer programs Start Menu shortcuts

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Displays Start menu shortcuts to partially installed programs in gray text.*

*This policy makes it easier for users to distinguish between programs that are fully installed and those that are only partially installed.*

*Partially installed programs include those that a system administrator assigns using Windows Installer and those that users have configured for full installation upon first use.*

*If you disable this policy or do not configure it, all Start menu shortcuts appear as black text.*

*Note: Enabling this policy can make the Start menu slow to open.*

## Desktop

- Hide all icons on Desktop

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, My Computer, and My Network Places.*

*Removing icons and shortcuts does not prevent the user from using another method to start the programs or opening the items they represent.*

- Remove My Documents icon from desktop

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes most occurrences of the My Documents icon.*

*This policy removes the My Documents icon from the desktop, from Windows Explorer, from programs that use the Windows Explorer windows, and from the standard Open dialog box.*

*This policy does not prevent the user from using other methods to gain access to the contents of the My Documents folder.*

*This policy does not remove the My Documents icon from the Start Menu. To do so, use the "Remove My Documents icon from Start Menu" policy.*

*Note: To make changes to this policy effective, you must log off of and log back on to Windows 2000.*

- Remove My Documents icon from Start Menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the My Documents icon from the Start Menu and its submenus.*

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

*Note: To make changes to this policy effective, you must log off of and log back on to Windows 2000.*

*Also, see the "Remove My Documents icon from desktop" policy.*

- Hide My Network Places icon on desktop

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the My Network Places icon from the desktop.*

*This policy only affects the desktop icon. It does not prevent users from connecting to the network or browsing for shared computers on the network.*

- Hide Internet Explorer icon on desktop

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Internet Explorer icon from the desktop and from the Quick Launch bar on the taskbar.*

*This policy does not prevent the user from starting Internet Explorer by using other methods.*

- Do not add shares of recently opened documents to My Network Places

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Remote shared folders are not added to My Network Places whenever you open a document in the shared folder.*

*If you disable this policy or do not configure it, then when you open a document in a remote shared folder, the system adds a connection to the shared folder to My Network Places.*

*If you enable this policy, shared folders are not added to My Network Places automatically when you open a document in the shared folder.*

- Prohibit user from changing My Documents path

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from changing the path to the My Documents folder.*
>
> *By default, a user can change the location of the My Documents folder by typing a new path in the Target box of the My Documents Properties dialog box. If you enable this policy, when users type a new path in the Target box, a message appears explaining that a policy prevents the action.*

- Disable adding, dragging, dropping, and closing the Taskbar's toolbars

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from manipulating desktop toolbars.*
>
> *If you enable this policy, users cannot add or remove toolbars from the desktop. Also, users cannot drag toolbars onto or off of docked toolbars.*
>
> *Note: If users have added or removed toolbars, this policy prevents them from restoring the default configuration.*
>
> *Tip: To view the toolbars that can be added to the desktop, right-click a docked toolbar (such as the taskbar beside the Start button), and point to "Toolbars."*
>
> *Also, see the "Disable adjusting desktop toolbars" policy.*

- Disable adjusting desktop toolbars

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from adjusting the length of desktop toolbars. Also, users cannot reposition items or toolbars on docked toolbars.*
>
> *This policy does not prevent users from adding or removing toolbars on the desktop.*
>
> *Note: If users have adjusted their toolbars, this policy prevents them from restoring the default configuration.*
>
> *Also see the "Disable adding, dragging, dropping and closing the Taskbar's toolbars" policy.*

- Don't save settings at exit

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from saving certain changes to the desktop.*
>
> *If you enable this policy, users can change the desktop, but some changes, such as the position of open windows or the size and position of the taskbar, are not saved when users log off. However, shortcuts placed on the desktop are always saved.*

### Active Desktop

- Enable Active Desktop

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Enables Active Desktop and prevents users from disabling it.*
>
> *This policy also removes the Active Desktop item from the context menu that appears when you right-click the desktop; it removes the Web tab from Display in Control Panel; and it disables the "Use Windows classic desktop" item on the General tab of the Folder Options dialog box. This prevents users from trying to enable or disable Active Desktop while a policy controls it.*
>
> *If you disable this policy or do not configure it, Active Desktop is disabled by default, but users can enable it.*
>
> *Note: If both the "Enable Active Desktop" policy and the "Disable Active Desktop" policy are enabled, the "Disable Active Desktop" policy is ignored. If the "Enable Classic Shell" policy (in User Configuration\Administrative Templates\Windows Components\Windows Explorer) is enabled, then Active Desktop is disabled and both of these policies are ignored.*
>
> *Tip: To enable Active Desktop without setting a policy, right-click the desktop, point to "Active Desktop," and then click "Show Web Content."*
>
> *Also, see the "Remove the Folder Options menu item from the Tools menu" policy in User Configuration\Administrative Templates\Windows Components\Windows Explorer.*

- Disable Active Desktop

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Disables Active Desktop and prevents users from enabling it.*
>
> *This policy also removes the Active Desktop item from the context menu that appears when you right-click the desktop; it removes the Web tab from Display in Control Panel; and it disables the "Enable Web content on my desktop" item on the General tab of the Folder Options dialog box. This prevents users from trying to enable or disable Active Desktop while a policy controls it. If you disable this policy or do not configure it, Active Desktop is disabled by default, but users can enable it.*
>
> *Note: If both the "Enable Active Desktop" policy and the "Disable Active Desktop" policy are enabled, the "Disable Active Desktop" policy is ignored. If the "Enable Classic Shell" policy (in User Configuration\Administrative Templates\Windows Components\Windows Explorer) is enabled, then Active Desktop is disabled and both of these policies are ignored.*
>
> *Tip: To disable Active Desktop without setting a policy, right-click the desktop, point to "Active Desktop" and then turn off "Show Web Content."*
>
> *Also, see the "Remove the Folder Options menu item from the Tools menu" policy in User Configuration\Administrative Templates\Windows Components\Windows Explorer.*

- Disable all items

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Removes Active Desktop content and prevents users from adding Active Desktop content.*

*This policy removes all Active Desktop items from the desktop. It also removes the Web tab from Display in Control Panel and removes the "New Desktop Item" command from the Active Desktop menu. As a result, users cannot add Web pages or pictures from the Internet or an intranet to the desktop.*

*This policy does not disable Active Desktop. Users can still use image formats, such as JPEG and GIF, for their desktop wallpaper.*

*Also, see the "Prohibit Adding Items" policy.*

- Prohibit changes

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents the user from enabling or disabling Active Desktop or changing the Active Desktop configuration.*

*This is a comprehensive policy that locks down the configuration you establish by using other policies in this folder.*

*This policy removes the Web tab from Display in Control Panel and removes the Active Desktop item from menu that appears when you right-click the desktop. As a result, users cannot enable or disable Active Desktop. If Active Desktop is already enabled, users cannot add, remove, or edit Web content or disable, lock, or synchronize Active Desktop components.*

- Prohibit adding items

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from adding Web content to their Active Desktop.*

*This policy removes the "New" button from Web tab in Display in Control Panel. It also removes the "New Desktop Item" command from the Active Desktop menu. As a result, users cannot add Web pages or pictures from the Internet or an intranet to the desktop.*

*This policy does not remove existing Web content from their Active Desktop, or prevent users from removing existing Web content.*

*Also, see the "Disable all items" policy.*

- Prohibit deleting items

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from deleting Web content from their Active Desktop.*

*This policy removes the Delete button from the Web tab in Display in Control Panel. As a result, users can temporarily remove, but not delete, Web content from their Active Desktop.*

*This policy does not prevent users from adding Web content to their Active Desktop.*

*Also, see the "Prohibit closing components" and "Disable all items" policies.*

- Prohibit editing items

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from changing the properties of Web content items on their Active Desktop.*

*This policy disables the Properties button on the Web tab in Display in Control Panel. Also, it removes the Properties item from the menu for each item on the Active Desktop. As a result, users can change the properties of an item, such as its synchronization schedule, password, or display characteristics.*

- Prohibit closing items

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from removing Web content from their Active Desktop.*

*In Active Desktop, you can add items to the desktop, but close them so they are not displayed. If you enable this policy, items added to the desktop cannot be closed; they always appear on the desktop.*

*This policy removes the list of the Active Desktop items from the Active Desktop menu. (To see this list, right-click the desktop and point to Active Desktop. The list appears at the bottom of the menu.) Also, it removes the check boxes from items on the Web tab in Display in Control Panel.*

*This policy does not prevent users from deleting items from their Active Desktop.*

- Add/Delete items

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must enter URL(s) of desktop item(s) to Add and enter the URL(s) of desktop item(s) to Delete.*

*Adds and deletes specified Web content items.*

*You can use the "Add" box in this policy to add particular Web-based items or shortcuts to users' desktops. Users can close or delete the items (if policies allow), but the items are added again each time the policy is refreshed.*

*You can also use this policy to delete particular Web-based items from users' desktops. Users can add the item again (if policies allow), but the item is deleted each time the policy is refreshed.*

*Note: Removing an item from the "Add" list for this policy is not the same as deleting it. Items removed from the add list are not removed from the desktop. They are just not added again.*

- Active Desktop Wallpaper

*Default Setting: Not configured*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must specify location and name of the wallpaper. The default setting for wallpaper style is: Center. The administrator may choose from among the following: Center, Stretch, Tile.*

*Specifies the desktop background ("wallpaper") displayed on all users' desktops.*

*This policy lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp), JPEG (*.jpg), or HTML (*.htm, *.html) file.*

*To use this policy, type the fully-qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Winnt\Logo.bmp or a UNC path, such as \\Server\Share\Logo.bmp.*

*If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternate wallpaper.*

*You can also use this policy to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.*

*If you disable this policy or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice.*

*Note: This policy requires that Active Desktop be enabled. By default, Active Desktop is disabled. To use a policy to enable Active Desktop, use the "Enable Active Desktop" policy.*

*Also, see the "Allow only bitmapped wallpaper" and the "Disable changing wallpaper" policies.*

- Allow only bitmapped wallpaper

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Permits only bitmap images for wallpaper.*

*This policy limits the desktop background ("wallpaper") to bitmap (.bmp) files. If users select files with other image formats, such as JPEG, GIF, PNG, or HTML, the wallpaper does not load.*

*This policy is designed to avoid the Active Desktop prompt. When users select a wallpaper with an alternate image format, the system prompts them to enable Active Desktop. By limiting users to bitmapped files, the prompt is avoided.*

*Also, see the "Active Desktop Wallpaper" and the "Disable changing wallpaper" (in User Configuration\Administrative Templates\Control Panel\Display) policies.*

### Active Directory

- Maximum size of Active Directory searches

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 10000. The minimum value is 0. The maximum value is somewhere around 4.2 billion.*

*Specifies the maximum number of objects the system displays in response to a command to browse or search Active Directory. This policy affects all browse displays associated with Active Directory, such as those in Local Users and Groups, Active Directory Users & Computers, and dialog boxes used to set permissions for user or group objects in Active Directory.*

*If you enable this policy, you can use the "Number of objects returned" box to limit returns from an Active Directory search.*

*If you disable this policy or do not configure it, the system displays up to 10,000 objects. This consumes approximately 2 MB of memory or disk space.*

*This policy is designed to protect the network and the domain controller from the effect of expansive searches.*

- Enable filter in Find dialog box

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Displays the filter bar above the results of an Active Directory search. The filter bar consists of buttons for applying additional filters to search results.*
>
> *If you enable this policy, the filter bar appears when the Active Directory Find dialog box opens, but users can hide it.*
>
> *If you disable this policy or do not configure it, the filter bar does not appear, but users can display it by selecting "Filter" from the "View" menu.*
>
> *To see the filter bar, open My Network Places, click Entire Network, and then click Directory. Right-click the name of a Windows 2000 domain, and click Find. Type the name of an object in the directory, such as "Administrator." If the filter bar does not appear above the resulting display then, from the View menu, click Filter.*

- Hide Active Directory folder

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Hides the Active Directory folder in My Network Places.*
>
> *The Active Directory folder displays Active Directory objects in a browse window.*
>
> *If you enable this policy, the Active Directory folder does not appear in the My Network Places folder.*
>
> *If you disable this policy or do not configure it, the Active Directory folder appears in the My Network Places folder.*
>
> *This policy is designed to let users search Active Directory, but not tempt them to casually browse Active Directory.*

## Control Panel

- Disable Control Panel

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Disables all Control Panel programs.*
>
> *This policy prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot start Control Panel or run any Control Panel items.*
>
> *This policy also removes Control Panel from the Start menu. (To open Control Panel, click Start, point to Settings, and then click Control Panel.) This policy also removes the Control Panel folder from Windows Explorer.*
>
> *If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a policy prevents the action.*
>
> *Also, see the "Disable Display in Control Panel" and "Disable programs on Settings menu" policies.*

- Hide specified control panel applets

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the administrator create a list of disallowed control panel applets.*
>
> *Hides specified Control Panel items and folders.*
>
> *This policy removes Control Panel items (such as Display) and folders (such as Fonts) from the Control Panel window and the Start menu. It can remove Control Panel items you have added to your system, as well Control Panel items included in Windows 2000.*
>
> *To hide a Control Panel item, type the file name of the item, such as Ncpa.cpl (for Network). To hide a folder, type the folder name, such as Fonts.*
>
> *This policy affects the Start menu and Control Panel window only. It does not prevent users from running Control Panel items.*
>
> *Also, see the "Disable Display in Control Panel" policy in User Configuration\Administrative Templates\Control Panel\Display.*
>
> *If both the "Hide specified control panel applets" policy and the "Show only specified control panel applets" policy are enabled, and the same item appears in both lists, the "Show only specified control panel applets" policy is ignored.*
>
> *Tip: To find the file name of a Control Panel item, search for files with the .cpl file name extension in the %Systemroot%\System32 directory.*

- Show only specified control panel applets

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the administrator must create a list of allowed control panel applets.*
>
> *Hides all Control Panel items and folders except those specified in this policy.*
>
> *This policy removes all Control Panel items (such as Network) and folders (such as Fonts) from the Control Panel window and the Start menu. It removes Control Panel items you have added to your system, as well the Control Panel items included in Windows 2000. The only items displayed in Control Panel are those you specify in this policy.*
>
> *To display a Control Panel item, type the file name of the item, such as Ncpa.cpl (for Network). To display a folder, type the folder name, such as Fonts. If you do not specify any items or folders, the Control Panel window is empty.*
>
> *This policy affects the Start menu and Control Panel window only. It does not prevent users from running any Control Panel items.*
>
> *Also, see the "Disable Display in Control Panel" policy in User Configuration\Administrative Templates\Control Panel\Display.*
>
> *If both the "Hide specified control panel applets" policy and the "Show only specified control panel applets" policy are enabled, the "Show only specified control panel applets" policy is ignored.*
>
> *Tip: To find the file name of a Control Panel item, search for files with the .cpl file name extension in the %Systemroot%\System32 directory.*

### Add/Remove Programs

- Disable Add/Remove Programs

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from using Add/Remove Programs.*
>
> *This policy removes Add/Remove Programs from Control Panel and removes the Add/Remove Programs item from menus.*
>
> *Add/Remove Programs lets users install, uninstall, repair, add, and remove features and components of Windows 2000 and a wide variety of Windows programs. Programs published or assigned to the user appear in Add/Remove Programs.*
>
> *If you disable this policy or do not configure it, Add/Remove Programs is available to all users.*
>
> *When enabled, this policy takes precedence over the other policies in this folder.*
>
> *This policy does not prevent users from using other tools and methods to install or uninstall programs.*

- Hide Change or Remove Programs page

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Removes the Change or Remove Programs button from the Add/Remove Programs bar. As a result, users cannot view or change the attached page.*
>
> *The Change or Remove Programs button lets users uninstall, repair, add, or remove features of installed programs.*
>
> *If you disable this policy or do not configure it, the Change or Remove Programs page is available to all users.*
>
> *This policy does not prevent users from using other tools and methods to delete or uninstall programs.*

- Hide Add New Programs page

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Removes the Add New Programs button from the Add/Remove Programs bar. As a result, users cannot view or change the attached page.*
>
> *The Add New Programs button lets users install programs published or assigned by a system administrator.*
>
> *If you disable this policy or do not configure it, the Add New Programs button is available to all users.*
>
> *This policy does not prevent users from using other tools and methods to install programs.*

- Hide Add/Remove Windows Components page

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Add/Remove Windows Components button from the Add/Remove Programs bar. As a result, users cannot view or change the associated page.*

*The Add/Remove Windows Components button lets users configure installed services and use the Windows Component wizard to add, remove, and configure components of Windows 2000 from the installation files.*

*If you disable this policy or do not configure it, the Add/Remove Windows Components button is available to all users.*

*This policy does not prevent users from using other tools and methods to configure services or add or remove program components. However, this policy blocks user access to the Windows Component wizard.*

- Hide the “Add a program from CD-ROM or floppy disk” option

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Add a program from CD-ROM or floppy disk section from the Add New Programs page. This prevents users from using Add/Remove Programs to install programs from removable media.*

*If you disable this policy or do not configure it, the Add a program from CD-ROM or floppy disk option is available to all users.*

*This policy does not prevent users from using other tools and methods to add or remove program components.*

*Note: If the "Hide Add New Programs page" policy is enabled, this policy is ignored. Also, if the "Disable media source for any install" policy (located in Computer Configuration\Administrative Templates\Windows Components\Windows Installer) is enabled, users cannot add programs from removable media, regardless of the setting of this policy.*

- Hide the “Add programs from Microsoft” option

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Add programs from Microsoft section from the Add New Programs page. This policy prevents users from using Add/Remove Programs to connect to Windows Update.*

*If you disable this policy or do not configure it, Add programs from Microsoft is available to all users.*

*This policy does not prevent users from using other tools and methods to connect to Windows Update.*

*Note: If the "Hide Add New Programs page" policy is enabled, this policy is ignored.*

- Hide the “Add programs from your network” option

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from viewing or installing published programs.*

*This policy removes the Add programs from your network section from the Add New Programs page. The Add programs from your network section lists published programs and provides an easy way to install them.*

*Published programs are those that the system administrator has explicitly made available to the user with a tool such as Windows Installer. Typically, system administrators publish programs to notify users that the programs are available, to recommend their use, or to enable users to install them without having to search for installation files.*

*If you enable this policy, users cannot tell which programs have been published by the system administrator, and they cannot use Add/Remove Programs to install published programs. However, they can still install programs by using other methods, and they can view and install assigned (partially installed) programs that are offered on the desktop or on the Start menu.*

*If you disable this policy or do not configure it, Add programs from your network is available to all users.*

*Note: If the "Hide Add New Programs page" policy is enabled, this policy is ignored.*

- Go directly to Components wizard

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from using Add/Remove Programs to configure installed services.*

*This policy removes the Set up services section of the Add/Remove Windows Components page. The Set up services section lists system services that have not been configured and offers users easy access to the configuration tools.*

*If you disable this policy or do not configure it, Set up services appears only when there are unconfigured system services. If you enable this policy, Set up services never appears.*

*This policy does not prevent users from using other methods to configure services.*

*Note: When Set up services does not appear, clicking the Add/Remove Windows Components button starts the Windows Component wizard immediately. Because the only remaining option on the Add/Remove Windows Components page starts the wizard, that option is selected automatically, and the page is bypassed.*

*To remove Set up services and prevent the Windows Component wizard from starting, enable the "Hide Add/Remove Windows Components page" policy. If the "Hide Add/Remove Windows Components page" policy is enabled, this policy is ignored.*

- Disable Support Information

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes links to the Support Info dialog box from programs on the Change or Remove Programs page.*

*Programs listed on the Change or Remove Programs page can include a "Click here for support information" hyperlink. When clicked, the hyperlink opens a dialog box that displays troubleshooting information, including a link to the installation files and data that users need to obtain product support, such as the Product ID and version number of the program. The dialog box also includes a hyperlink to support information on the Internet, such as the Microsoft Product Support Services Web page.*

*If you disable this policy or do not configure it, the Support Info hyperlink appears.*

*Note: Not all programs provide a support information hyperlink.*

- Specify default category for Add New Programs

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Specifies the category of programs that appears when users open the "Add New Programs" page.*
>
> *If you enable this policy, then only the programs in the category you specify are displayed when the "Add New Programs" page opens. Users can use the Category box on the "Add New Programs" page to display programs in other categories.*
>
> *To use this policy, type the name of a category in the Category box for this policy. You must enter a category that is already defined in Add/Remove Programs. To define a category, use Software Installation.*
>
> *If you disable this policy or do not configure it, all programs (Category: All) are displayed when the "Add New Programs" page opens.*
>
> *You can use this policy to direct users to the programs they are most likely to need.*
>
> *Note: This policy is ignored if either the "Disable Add/Remove Programs" policy or the "Hide Add New Programs page" policy is enabled.*

Display

- Disable Display in Control Panel

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Disables Display in Control Panel.*
>
> *If you enable this policy, Display in Control Panel does not run. When users try to start Display, a message appears explaining that a policy prevents the action.*
>
> *Also, see the "Disable Control Panel" and "Disable programs on Settings menu" policies.*

- Hide Background tab

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Removes the Background tab from Display in Control Panel.*
>
> *This policy prevents users from using Control Panel to change the pattern and wallpaper on the desktop.*

- Disable changing wallpaper

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from adding or changing the background design of the desktop.*
>
> *By default, users can use the Background tab of Display in Control Panel to add a background design (wallpaper) to their desktop. If you enable this policy, the Background tab still appears, but all options on the tab are disabled.*
>
> *To remove the Background tab, use the "Hide Background tab" policy.*

*To specify wallpaper for a group use the "Active Desktop Wallpaper" policy.*

*Also, see the "Allow only bitmapped wallpaper" policy.*

- Hide Appearance tab

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Appearance tab from Display in Control Panel.*

*This policy prevents users from using Control Panel to change the colors or color scheme of the desktop and windows.*

- Hide Settings tab

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Settings tab from Display in Control Panel.*

*This policy prevents users from using Control Panel to add, configure, or change the display settings on the computer.*

- Hide Screen Saver tab

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Removes the Screen Saver tab from Display in Control Panel.*

*This policy prevents users from using Control Panel to add, configure, or change the screen saver on the computer.*

- No screen saver

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables all desktop screen savers.*

*If you enable this policy, screen savers do not run. Also, this policy disables the Screen Saver section of the Screen Saver tab in Display in Control Panel. As a result, users cannot change the screen saver options.*

*If you disable this policy or do not configure it, this policy has no effect on the system.*

*Note: This policy takes precedence over the "Screen saver executable name" policy. If both are enabled, the "Screen saver executable name" policy is ignored and no screen savers run.*

*Also, see the "Hide Screen Saver tab" policy.*

- Screen saver executable name

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must enter the screen saver executable name.*

*Specifies the screen saver for the user's desktop.*

*If you enable this policy, the system displays the specified screen saver on the user's desktop. Also, this policy disables the drop-down list of screen savers on the Screen Saver tab in Display in Control Panel, preventing users from changing the screen saver.*

*If you disable this policy, or do not configure it, users can select any screen saver.*

*To use this policy, type the name of the file that contains the screen saver, including the .scr file name extension. If the screen saver file is not in the %Systemroot%\System32 directory, enter the fully qualified path to the file.*

*If the specified screen saver is not installed on a computer to which this policy applies, the policy is ignored.*

*Note: This policy can be superceded by the "No screen saver" policy. If both are enabled, this policy is ignored and screen savers do not run.*

- Password protect the screen saver

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether screen savers used on the computer are password protected.*

*If you enable this policy, all screen savers are password protected. If you disable this policy, password protection cannot be set on any screen saver.*

*This policy also disables the "Password protected" check box on the Screen Saver tab in Display in Control Panel, preventing users from changing the password protection setting.*

*If you do not configure this policy, users can choose whether or not to set password protection on each screen saver.*

*This policy is used only when a screen saver is specified for the computer. To specify a screen saver on a computer, in Control Panel, double-click Display, and then click the Screen Saver tab. To specify a screen saver in a policy, use the "Screen saver executable name" policy.*

*Note: To remove the Screen Saver tab, use the "Hide Screen Saver tab" policy.*

### Printers

- Disable deletion of printers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from deleting local and network printers.*

*If a user tries to delete a printer, such as by using the Delete option in Printers in Control Panel, a message appears explaining that a policy prevents the action.*

*This policy does not prevent users from running other programs to delete a printer.*

- Disable addition of printers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from using familiar methods to add local and network printers.*

*This policy removes the Add Printer option from the Start menu. (To find the Add Printer option, click Start, click Printers, and then click Add Printer.) This policy also removes Add Printer from the Printers folder in Control Panel.*

*Also, users cannot add printers by dragging a printer icon into the Printers folder. If they try, a message appears explaining that the a policy prevents the action.*

*However, this policy does not prevent users from using the Add Hardware wizard to add a printer. Nor does it prevent users from running other programs to add printers.*

*This policy does not delete printers that users have already added. However, if users have not added a printer when this policy is applied, they can't print.*

*Note: You can use printer permissions to restrict the use of printers without setting a policy. In the Printers folder, right-click a printer, click Properties, and then click the Security tab.*

- Browse the network to find printers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disable this option to remove the network printer browse page from within the Add Printer wizard. Use this policy to disallow users from browsing the network for printers. By removing the browse option users are encouraged to find printers in the Active Directory if one is available.*

*Lets users use the Add Printer wizard to search the network for shared printers.*

*If you enable this policy or do not configure it, then when users click "Add a network printer," but do not type the name of a particular printer, the Add Printer wizard displays a list of all shared printers on the network and invites users to choose a printer from among them.*

*If you disable this policy, users cannot search the network; they must type a printer name first.*

*This policy affects the Add Printer wizard only. It does not prevent users from using other programs to search for shared printers or to connect to network printers.*

- Default Active Directory path when searching for printers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must enter a default Active Directory path where users start their search for printers. This setting affects the printer search dialog when started from the Add Printer wizard (e.g. To start search in domain1.mycompany.com enter path as LDAP://DC=Domain1, DC=MyCompany,DC=com.)*

*Specifies the Active Directory location where searches for printers begin.*

*The Add Printer wizard gives users the option of searching Active Directory for a shared printer. If you enable this policy, these searches begin at the location you specify in the "Default Active Directory path" box. Otherwise, searches begin at the root of Active Directory.*

*This policy only provides a starting point for Active Directory searches for printers. It does not restrict user searches through the Active Directory.*

- Browse a common web site to find printers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may use this option to add a browse button for Internet printers in the Add Printer wizard. Use this policy to allow users browsing the company's Intranet for printers.*

*Adds a link to an Internet or intranet Web page to the Add Printer wizard.*

*You can use this policy to direct users to a Web page from which they can install printers.*

*If you enable this policy and type an Internet or intranet address in the text box, the system adds a Browse button to the "Locate Your Printer" page in the Add Printer wizard. The Browse button appears beside the "Connect to a printer on the Internet or your intranet" option. When users click Browse, the system opens an Internet browser and navigates to the specified URL address to display the available printers.*

*This policy makes it easy for users to find the printers you want them to add.*

*Also, see the "Custom support URL in the Printers folder's left pane" and "Web-based printing" policies in Computer Configuration\Administrative Templates\Printers.*

### Regional Options

- Restrict selection of Windows 2000 menus and dialogs language

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: English. The administrator may choose from all supported languages.*

*This policy restricts users to the specified language, by disabling the menus and dialogs control in the Regional Options control panel. If the specified language is not installed on the target computer, the language selection will default to English.*

## Network

### Offline Files

- Disable user configuration of Offline Files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from enabling, disabling, or changing the configuration of Offline Files.*

*This policy removes the Offline Files tab from the Folder Options dialog box. It also removes the Settings item from the Offline Files context menu and disables the Settings button on the Offline Files Status dialog box. As a result, users cannot view or change the options on the Offline Files tab or Offline Files dialog box.*

*This is a comprehensive policy that locks down the configuration you establish by using other policies in this folder.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: This policy provides a quick method for locking down the default settings for Offline Files. To accept the defaults, just enable this policy. You do not have to disable any other policies in this folder.*

- Synchronize all offline files before logging off

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Determines whether offline files are fully synchronized when users log off.*
>
> *This policy also disables the "Synchronize all offline files before logging off" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*
>
> *If you enable this policy, offline files are fully synchronized. Full synchronization ensures that offline files are complete and current.*
>
> *If you disable this policy, the system only performs a quick synchronization. Quick synchronization ensures that files are complete, but does not ensure that they are current.*
>
> *If you do not configure this policy, the system performs a quick synchronization by default, but users can change this option.*
>
> *This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*
>
> *Tip: To change the synchronization method without setting a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then select the "Synchronize all offline files before logging off" option.*

- Action on server disconnect

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the default setting is: Work offline. The administrator may choose from among the following:*
>
> *Never go offline = server's files are unavailable to local computer.*
>
> *Work offline = server's files are available to local computer.*
>
> *Determines whether network files remain available if the computer is suddenly disconnected from the server hosting the files.*
>
> *This policy also disables the "When a network connection is lost" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*
>
> *If you enable this policy, you can use the "Action" box to specify how computers in the group respond.*
>
> *-- "Work offline" indicates that the computer can use local copies of network files while the server is inaccessible.*
>
> *-- "Never go offline" indicates that network files are not available while the server is inaccessible.*
>
> *If you disable this policy or select the "Work offline" option, users can work offline if disconnected.*
>
> *If you do not configure this policy, users can work offline by default, but they can change this option.*
>
> *This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To configure this setting without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, click Advanced, and then select an option in the "When a network connection is lost" section.*

*Also, see the "Non-default server disconnect actions" policy.*

- Non-default server disconnect actions

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must specify non-default actions for servers that become unavailable. The administrator must enter a server name paired with an action value. Action values are:*

*0 = Work offline. Server's files are available to local computer.*

*1 = Never go offline. Server's files are unavailable to local computer.*

*Determines how computers respond when they are disconnected from particular offline file servers. This policy overrides the default response, a user-specified response, and the response specified in the "Action on server disconnect" policy.*

*This policy also disables the "Exception list" section on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*

*To use this policy, click Show, and then click Add. In the "Type the name of the item to be added" box, type the server's computer name. Then, in the "Type the value of the item to be added" box, type "0" if users can work offline when they are disconnected from this server, or type "1" if they cannot.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To configure this setting without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click Advanced. This policy corresponds to the settings in the "Exception list" section.*

- Disable 'Make Available Offline'

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prevents users from making network files and folders available offline.*

*This policy removes the "Make Available Offline" option from the File menu and from all context menus in Windows Explorer. As a result, users cannot designate files to be saved on their computer for offline use.*

*However, this policy does not prevent the system from saving local copies of files that reside on network shares designated for automatic caching.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Prevent use of Offline Files folder

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the Offline Files folder.*

*This policy disables the "View Files" button on the Offline Files tab. As a result, users cannot use the Offline Files folder to view or open copies of network files stored on their computer. Also, they cannot use the folder to view characteristics of offline files, such as their server status, type, or location.*

*This policy does not prevent users from working offline or from saving local copies of files available offline. Also, it does not prevent them from using other programs, such as Windows Explorer, to view their offline files.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To view the Offline Files Folder, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click "View Files."*

- Administratively assigned offline files

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must specify network files and folders that are always available offline. The administrator must enter the fully-qualified UNC path for each file or folder.*

*Lists network files and folders that are always available for offline use. This policy makes the specified files and folders available offline to users of the computer.*

*To assign a folder, click Show and then click Add. In the "Type the name of the item to be added" box, type the fully qualified UNC path to the file or folder. Leave the "Enter the value of the item to be added" field blank.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Disable reminder balloons

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Hides or displays reminder balloons, and prevents users from changing the setting.*

*Reminder balloons appear above the Offline Files icon in the status area to notify users when they have lost the connection to a networked file and are working on a local copy of the file. Users can then decide how to proceed.*

*If you enable this policy, the system hides the reminder balloons, and prevents users from displaying them.*

*If you disable the policy, the system displays the reminder balloons, and prevents users from hiding them.*

*If this policy is not configured, reminder balloons are displayed by default when you enable offline files, but users can change the setting.*

*To prevent users from changing the setting while a policy is in effect, the system disables the "Enable reminders" option on the Offline Files tab*

*This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To display or hide reminder balloons without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This policy corresponds to the "Enable reminders" check box.*

- Reminder balloon frequency

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 60 minutes.*

*Determines how often reminder balloon updates appear.*

*This policy also removes the "Display reminder balloon every ... minutes" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.*

*Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the update interval.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To set reminder balloon frequency without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This policy corresponds to the "Display reminder balloons every ... minutes" option.*

- Initial reminder balloon lifetime

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 30 seconds.*

*Determines how long the first reminder balloon for a network status change is displayed.*

*Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the duration of the first reminder.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Reminder balloon lifetime

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 15 seconds.*

*Determines how long updated reminder balloons are displayed.*

*Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the duration of the update reminder.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Event logging level

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 0. The administrator may choose from among the following:*

*0 = Cache data corrupted.*

*1 = Log 'server offline'*

*2 = Level 1 + log 'net stopped' and 'net started'*

*3 = Level 2 + log 'server available for reconnection'*

*Determines which events the Offline Files feature records in the event log.*

*Offline Files records events in the Application log in Event Viewer when it detects errors. By default, Offline Files records an event only when the offline files storage cache is corrupted. However, you can use this policy to specify additional events you want Offline Files to record.*

*To use this policy, from the "Enter" box, select the number corresponding to the events you want the system to log. The levels are cumulative; that is, each level includes the events in all preceding levels.*

*"0" records an error when the offline storage cache is corrupted.*

*"1" also records an event when the server hosting the offline file is disconnected from the network.*

*"2" also records events when the local computer is connected and disconnected from the network.*

*"3" also records an event when the server hosting the offline file is reconnected to the network.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

### Network and Dial-up Connections

- Prohibit deletion of RAS connections

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can delete their private dial-up (RAS) connections.*

*Private connections are those that are available only to one user. To create a private connection, on the Connection Availability page in the Network Connections wizard, click the "Only for myself" option.*

*If you enable this policy, users (including administrators) cannot delete any RAS connections. This setting also disables the "Delete" option on the context menu for a RAS connection and on the File menu in Network and Dial-up Connections.*

*If you disable this policy or do not configure it, users can delete their private RAS connections. Private connections are those that are available only to one user. (By default, only administrators can delete connections available to all users, but you can change the default by using the "Prohibit deletion of RAS connections available to all users" policy.)*

*Important: When enabled, this policy takes precedence over the "Prohibit deletion of RAS connections available to all users" policy. Users cannot delete any RAS connections and the "Prohibit deletion of RAS connections available to all users" policy is ignored.*

*Note: LAN connections are created and deleted automatically when a LAN adapter is installed or removed. You cannot use Network and Dial-up Connections to create or delete a local area connection.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to bypass this policy.*

- Prohibit deletion of RAS connections available to all users

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Prohibits users from deleting shared dial-up (RAS) connections. Shared connections are available to all users of the computer.*

*Shared connections are those that are available to all users. To create a shared dial-up (RAS) connection, on the Connection Availability page in the Network Connections wizard, click the "For all users" option.*

*If you enable this policy or do not configure it, only administrators can delete shared RAS connections. (By default, users can still delete their private connections, but you can change the default by using the "Prohibit deletion of RAS connections" policy.)*

*If you disable this policy, users can delete shared RAS connections. Additionally, if your file system is NTFS users need to have write access to Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk to delete a shared RAS Connection.*

*Important: When enabled, the "Prohibit deletion of RAS connections" policy takes precedence over this policy. Users (including administrators) cannot delete any RAS connections and this policy is ignored.*

*Note: LAN connections are created and deleted automatically by the system when a LAN adapter is installed or removed. You cannot use Network and Dial-up Connections to create or delete a local area connection.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to bypass this policy.*

- Prohibit connecting and disconnecting a RAS connection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can connect and disconnect dial-up connections.*

*If you enable this policy, then double-clicking the icon has no effect, and the Connect and Disconnect menu items are disabled.*

*If you disable this policy, the Connect and Disconnect options for dial-up connections are available to all users. Users can connect or disconnect a dial-up connection by double-clicking the icon representing the connection, by right-clicking it, or by using the File menu.*

*Note: Users can still connect and disconnect from the Status page for a connection. To prevent users from displaying the Status page, enable the "Prohibit viewing of status statistics for an active connection" policy.*



- Prohibit enabling/disabling a LAN connection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can Enable/Disable local area connections.*

*If you enable this policy, then double-clicking the icon has no effect, and the Enable and Disable menu items are disabled.*

*If you disable this policy, the Enable and Disable options for local area connections are available to users in the group. Users can Enable/Disable a local area connection by double-clicking the icon representing the connection, by right-clicking it, or by using the File menu.*

*Note: Administrators can still Enable/Disable local area connections from Device Manager.*

- Prohibit access to properties of a LAN connection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether administrators can view and change the properties of a local area connection.*

*This policy determines whether the Properties menu item is enabled, and thus, whether the Local Area Connection Properties dialog box is available to administrators.*

*If you enable this policy, the Properties menu items are disabled, and administrators cannot open the Local Area Connection Properties dialog box.*

*If you disable this policy, a Properties menu item appears when administrators right-click the icon representing a local area connection. Also, when administrators select the connection, Properties is enabled on the File menu.*

*Note: This policy supersedes policies that remove or disable parts of the Local Area Connection Properties dialog box, such as those that hide tabs, remove the check boxes for enabling or disabling components, or disable Properties button for components that a connection uses. If you enable this policy, then the policies that disable parts of the Local Area Connection Properties dialog box are ignored.*

*Note: Non-administrators are already denied access to properties regardless of policies.*

- Prohibit access to current user's RAS connection properties

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can view and change the properties of their private dial-up (RAS) connections.*

*Private connections are those that are available only to one user. To create a private connection, on the Connection Availability page in the Network Connections wizard, click the "Only for myself" option.*

*This policy determines whether the Properties menu item is enabled, and thus, whether the Dial-up Connection Properties dialog box is available to users.*

*If you enable this policy, the Properties menu items are disabled, and users cannot open the Dial-up Connection Properties dialog box.*

*If you disable this policy, a Properties menu item appears when users right-click the icon representing a dial-up connection. Also, when users select the connection, Properties appears on the File menu.*

*Note: This policy supersedes policies that remove or disable parts of the Dial-up Connection Properties dialog box, such as those that hide tabs, remove the check boxes for enabling or disabling components, or disable the Properties button for components that a connection uses. If you enable this policy, it overrides these subsidiary policies.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to bypass this policy.*

- Prohibit access to properties of RAS connections available to all users

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether a user can view and change the properties of dial-up connections that are available to all users of the computer.*

*Shared connections are those that are available to all users. To create a shared dial-up (RAS) connection, on the Connection Availability page in the Network Connections wizard, click the "For all users" option.*

*This policy determines whether the Properties menu item is enabled, and thus, whether the Dial-up Connection Properties dialog box is available to users.*

*If you enable this policy, the Properties menu items are disabled, and users cannot open the Dial-up Connection Properties dialog box.*

*If you disable this policy, a Properties menu item appears when users right-click the icon for a dial-up connection. Also, when users select the connection, Properties appears on the File menu.*

*Note: This policy supersedes policies that remove or disable parts of the Dial-up Connection Properties dialog box, such as those that hide tabs, remove the check boxes for enabling or disabling components, or disable the Properties button for components that a connection uses. If you enable this policy, it overrides these subsidiary policies.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to bypass this policy.*

- Prohibit renaming LAN connections or RAS connections available to all users

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can rename dial-up (RAS) and local area connections.*

*Private RAS connections can be renamed regardless of this setting.*

*If you enable this policy, the Rename option is disabled.*

*If you disable this policy, the Rename option is enabled. Users can rename connections by clicking the icon representing a connection or by using the File menu.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to rename RAS connections.*

- Prohibit renaming of RAS connections belonging to current user

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can rename their private dial-up (RAS) connections.*

*Private connections are those that are available only to one user. To create a private connection, on the Connection Availability page in the Network Connections wizard, click the "Only for myself" option.*

*If you enable this policy, the Rename option is disabled.*

*If you disable this policy, the Rename option is enabled for users' private dial-up connections. Users can rename their private connection by clicking an icon representing the connection or by using the File menu.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to bypass this policy.*

- Prohibit adding and removing components for a LAN or RAS connection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether administrators can add and remove network components. This policy has no effect on non-administrators.*

*If you enable this policy, the Install and Uninstall buttons for components of connections are disabled and users are not permitted access to network components in the Windows Components wizard.*

*If you disable this policy, the Install and Uninstall buttons for components of connections in Network and Dial-up Connections are enabled. Also, users can gain access to network components in the Windows Components wizard.*

*The Install button opens the dialog boxes used to add network components. Clicking the Uninstall button removes the selected component in the components list (above the button).*

*The Install and Uninstall buttons appear when users right-click a connection and click Properties. These buttons are on the General tab for LAN connections and on the Networking tab for dial-up connections.*

*The Windows Components wizard permits users to add and remove components. To use the wizard, double-click Add/Remove Programs in Control Panel. To go directly to the network components in the Windows Components wizard, click the Advanced menu in Network and Dial-up Connections, and then click "Optional Networking Components."*

*Note: Non-administrators are already prohibited from adding or removing components for a LAN or RAS connection regardless of this policy.*

- Prohibit enabling/disabling components of a LAN connection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether administrators can enable and disable the components used by local area connections.*

*Enabling this policy removes the check boxes for enabling and disabling components. As a result, administrators cannot enable or disable the components that a connection uses.*

*If you disable this policy, the Properties dialog box for a connection includes a check box beside the name of each component that the connection uses. Selecting the check box enables the component, and clearing the check box disables the component.*

*Note: Non-administrators are already prohibited from enabling or disabling components for a LAN connection regardless of this policy.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to enable/disable connection components.*

- Prohibit access to properties of components of a LAN connection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether administrators can change the properties of components used by a local area connection.*

*This policy determines whether the Properties button for components of a local area connection is enabled.*

*If you enable this policy, the Properties button is disabled.*

*If you disable this policy or do not configure it, the Properties button is enabled.*

*The Local Area Connection Properties dialog box includes a list of the network components that the connection uses. To view or change the properties of a component, click the name of the component, and then click the Properties button beneath the component list.*

*Note: Not all network components have configurable properties. For components that are not configurable, the Properties button is always disabled.*

*Note: Non-administrators are already prohibited from accessing properties of components for a LAN connection regardless of this policy.*

- Prohibit access to properties of components of a RAS connection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can view and change the properties of components used by a dial-up connection.*

*This policy determines whether the Properties button for components used by a RAS connection is enabled.*

*If you enable this policy, the Properties button is disabled.*

*If you disable this policy, the Properties button is enabled.*

*The Networking tab of the Dial-up Connection Properties dialog box includes a list of the network components that the connection uses. To view or change the properties of a component, click the name of the component, and then click the Properties button beneath the component list.*

*Note: Not all network components have configurable properties. For components that are not configurable, the Properties button is always disabled.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to bypass this policy.*



- Prohibit access to the Network Connection wizard

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can use the Network Connection wizard, which creates new network connections.*

*If you enable this policy, the Make New Connection icon does not appear in the Start Menu on in the Network and Dial-up Connections folder. As a result, users cannot start the Network Connection wizard.*

*If you disable this policy, the Make New Connection icon appears in the start menu and in the Network and Dial-up Connections folder. Clicking Make New Connection starts the Network Connection wizard.*

*Note: Changing this policy from Enabled to Not Configured does not restore the Make New Connection icon until the user logs off.*

*Note: This policy does not prevent users from using other programs such Internet Explorer to bypass this policy.*

- Prohibit viewing of status statistics for an action connection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can view the Status page for an active connection.*

*The Status page displays information about the connection and its activity. It also provides buttons to disconnect and to configure the properties of the connection.*

*If you enable this policy, the Status option is disabled, and the Status page doesn't appear.*

*If you disable this policy, the Status page appears when users double-click an active connection. Also, an option to display the Status page appears on a menu when users right-click the icon for an active connection, and the option appears on the File menu when users select an active connection.*

*Note: Even when this policy is enabled, some connection statistics can be viewed by hovering with the mouse pointer over the connection icon (in the system tray).*

- Prohibit access to Dial-up Preferences item on the Advanced menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether the "Dial-up Preferences" item on the Advanced menu in Network and Dial-up Connections is enabled.*

*The Dial-up Preferences item lets users create and change connections before logon and configure automatic dialing and callback features.*

*If you enable this policy, the Dial-up Preferences item is disabled.*

*If you disable this policy, the Dial-up Preferences item is enabled.*

- Prohibit access to Advanced Settings item on the Advanced menu

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether the Advanced Settings item on the Advanced menu in Network and Dial-up Connections is enabled for administrators.*

*The Advanced Settings item lets users view and change bindings and view and change the order in which the computer accesses connections, network providers, and print providers.*

*If you enable this policy, the Advanced Settings item is disabled.*

*If you disable this policy, the Advanced Settings item is enabled.*

*Note: Non-administrators are already prohibited from accessing the Advanced Settings dialog box regardless of policies.*

- Prohibit configuration of connection sharing

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether administrators can enable, disable, and configure the Connection Sharing feature of LAN or RAS connections.*

*If you enable this policy, the system removes the Sharing tab from the Properties dialog box for a LAN or RAS connection. On Windows 2000 Server, it also removes the Internet Connection Sharing page from the Network Connection wizard.*

*If you disable this policy, the Sharing tab and Internet Connection Sharing wizard page are displayed.*

*Connection Sharing lets users configure their system as an Internet gateway for a small network. It provides network services, such as name resolution, to the network.*

*By default, Connection Sharing is disabled when you create a dial-up connection, but administrators can use the Sharing tab and Internet Connection Sharing wizard page to enable it.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Note: LAN Connection Sharing is only available when two or more network interfaces are present.*

*Note: Non-administrators are already prohibited from configuring Connection Sharing regardless of this policy.*

- Prohibit TCP/IP advanced configuration

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Determines whether users can use Network and Dial-up Connections to configure TCP/IP, DNS, and WINS settings.*

*If you enable this policy, the Advanced button on the Internet Protocol (TCP/IP) Properties dialog box is disabled. As a result, users cannot open the Advanced TCP/IP Settings Properties page and modify IP settings, such as DNS and WINS server information.*

*If you disable this policy, the Advanced button is enabled and the users can open the Advanced TCP/IP Setting dialog box.*

*Note: This policy is superceded by policies that prohibit access to properties of connections or connection components. When these polices are enabled users cannot gain access to the Advanced button.*

*Tip: To open the Advanced TCP/IP Setting dialog box, in Network and Dial-up Connections, right-click a connection icon, and click Properties. For RAS connections select the Networking tab. In the "Components checked are used by this connection" box, click Internet Protocol (TCP/IP), click the Properties button, and then click the Advanced button.*

*Note: Changing this policy from Enabled to Not Configured does not enable the Advanced button until the user logs off.*

## System

- Don't display welcome screen at logon

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Suppresses the "Getting Started with Windows 2000" welcome screen.*

*This policy hides the welcome screen that is displayed on Windows 2000 Professional each time the user logs on.*

*Users can still display the "Getting Started with Windows 2000" welcome screen by selecting it from the Start menu or by typing "Welcome" in the Run dialog box.*

*This policy applies only to Windows 2000 Professional. It does not affect the "Configure Your Server on a Windows 2000 Server" screen on Windows 2000 Server.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

*Tip: To display the welcome screen, click Start, point to Programs, point to Accessories, point to System Tools, and then click "Getting Started." To suppress the welcome screen without setting a policy, clear the "Show this screen at startup" check box on the welcome screen.*

- Century interpretation for Year 2000

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may specify the maximum year for which two digit years are interpreted as being the 21st century.*

*The default year is: 2029.*

*Determines how programs interpret two-digit years.*

*This policy specifies the largest two-digit year interpreted as being preceded by 20. All numbers less than or equal to the specified value are interpreted as being preceded by 20. All numbers greater than the specified value are interpreted as being preceded by 19.*

*For example, the default value, 2029, specifies that all two-digit years less than or equal to 29 (00 to 29) are interpreted as being preceded by 20, that is 2000 to 2029. Conversely, all two-digit years greater than 29 (30 to 99) are interpreted as being preceded by 19, that is, 1930 to 1999.*

*This policy only affects the programs that use this Windows feature to interpret two-digit years. If a program does not interpret two-digit years correctly, consult the documentation or manufacturer of the program.*

- Code signing for device drivers

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default response is: Warn. The administrator may choose from among the following: Ignore, Warn, Block.*

*Determines how the system responds when a user tries to install device driver files that are not digitally signed.*

*This policy establishes the least secure response permitted on the systems of users in the group. Users can use System in Control Panel to select a more secure setting, but when this policy is enabled, the system does not implement any setting less secure than the one the policy established.*

*When you enable this policy, use the drop-down box to specify the desired response.*

*-- "Ignore" directs the system to proceed with the installation even if it includes unsigned files.*

*-- "Warn" notifies the user that files are not digitally signed and lets the user decide whether to stop or to proceed with the installation and whether to permit unsigned files to be installed. "Warn" is the default.*

*-- "Block" directs the system to refuse to install unsigned files. As a result, the installation stops, and none of the files in the driver package is installed.*

*To change driver file security without setting a policy, use System in Control Panel. Right-click My Computer, click Properties, click the Hardware tab, and then click the Driver Signing button.*

- Custom user interface

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must enter the interface name.*

*Specifies an alternate user interface for Windows 2000.*

*The Explorer program (Explorer.exe) creates the familiar Windows interface, but you can use this policy to specify an alternate interface. If you enable this policy, the system starts the interface you specify instead of Explorer.exe.*

*To use this policy, copy your interface program to a network share or to your system drive. Then, enable this policy, and type the name of the interface program, including the file name extension, in the Shell name text box. If the interface program file is not located in a folder specified in the Path environment variable for your system, enter the fully qualified path to the file.*

*If you disable this policy or do not configure it, the policy is ignored and the system displays the Explorer interface.*

*Tip: To find the folders indicated by the Path environment variable, click System Properties in Control Panel, click the Advanced tab, click the Environment Variables button, and then, in the System variables box, click Path.*



- Disable the command prompt

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: No. The administrator may choose from among the following: Yes, and No.*

*Prevents users from running the interactive command prompt, Cmd.exe. This policy also determines whether batch files (.cmd and .bat) can run on the computer.*

*If you enable this policy and the user tries to open a command window, the system displays a message explaining that a policy prevents the action.*

*Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Terminal Services.*

- Disable registry editing tools

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Disables the Windows registry editors, Regedt32.exe and Regedit.exe.*

*If this policy is enabled and the user tries to start a registry editor, a message appears explaining that a policy prevents the action.*

*To prevent users from using other administrative tools, use the "Run only allowed Windows applications" policy.*

- Run only allowed Windows applications

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must enter a list of allowed applications by the executable name (e.g. Winword.exe, Poledit.exe, Powerpnt.exe).*

*Limits the Windows programs that users have permission to run on the computer.*

*If you enable this policy, users can only run programs that you add to the List of Allowed Applications.*

*This policy only prevents users from running programs that are started by the Windows Explorer process. It does not prevent users from running programs such as Task Manager, which are started by the system process or by other processes. Also, if users have access to the command prompt, Cmd.exe, this policy does not prevent them from starting programs in the command window that they are not permitted to start by using Windows Explorer.*

- Don’t run specified Windows applications

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator must enter a list of disallowed applications by executable name (e.g. Winword.exe, Poledit.exe, Powerpnt.exe).*

*Prevents Windows from running the programs you specify in this policy.*

*If you enable this policy, users cannot run programs that you add to the List of disallowed applications.*

*This policy only prevents users from running programs that are started by the Windows Explorer process. It does not prevent users from running programs, such as Task Manager, that are started by the system process or by other processes. Also, if you permit users to gain access to the command prompt, Cmd.exe, this policy does not prevent them from starting programs in the command window that they are not permitted to start by using Windows Explorer.*

- Disable Autoplay

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: CD-ROM drives. The administrator may choose from among the following: All drives and CD-ROM drives.*

*Disables the Autoplay feature.*

*Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media starts immediately.*

*By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.*

*If you enable this policy, you can also disable Autoplay on CD-ROM drives, or disable Autoplay on all drives.*

*This policy disables Autoplay on additional types of drives. You cannot use this policy to enable Autoplay on drives on which it is disabled by default.*

*Note: This policy appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

- Download missing COM components

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Directs the system to search Active Directory for missing Component Object Model (COM) components that a program requires.*

*Many Windows programs, such as the MMC snap-ins, use the interfaces provided by the COM. These programs cannot perform all of their functions unless Windows 2000 has internally registered the required components.*

*If you enable this policy and a component registration is missing, the system searches for it in Active Directory and if it is found, downloads it. The resulting searches might make some programs start or run slowly.*

*If you disable this policy or do not configure it, the program continues without the registration. As a result, the program might not perform all of its functions, or it might stop.*

*This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*

### Logon/Logoff

- Disable Task Manager

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from starting Task Manager (Taskmgr.exe).*
>
> *If this policy is enabled and users try to start Task Manager, a message appears explaining that a policy prevents the action.*
>
> *Task Manager lets users start and stop programs; monitor the performance of their computers; view and monitor all programs running on their computers, including system services; find the executable names of programs; and change the priority of the process in which programs run.*

- Disable Lock Computer

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from locking the system.*
>
> *While locked, the desktop is hidden and the system cannot be used. Only the user who locked the system or the system administrator can unlock it.*
>
> *Tip:To lock a computer without configuring a policy, press Ctrl+Alt+Delete, and then click "Lock Computer."*

- Disable Change Password

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents users from changing their Windows password on demand.*
>
> *This policy disables the "Change Password" button on the Windows Security dialog box (which appears when you press Ctrl+Alt+Del).*
>
> *However, users are still able to change their password when prompted by the system. The system prompts users for a new password when an administrator requires a new password or their password is expiring.*

- Disable Logoff

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents the user from logging off of Windows 2000.*
>
> *This policy does not let the user log off of the system by using any method, including programs run from the command line, such as scripts. It also disables or removes all menu items and buttons that log the user off of the system.*
>
> *Also, see the "Disable Logoff on the Start Menu" policy.*

- Run logon scripts synchronously

> *Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Directs the system to wait for the logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop.*

*If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.*

*If you disable this policy or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously.*

*This policy appears in the Computer Configuration and User Configuration folders. The policy set in Computer Configuration takes precedence over the policy set in User Configuration.*

- Run legacy logon scripts hidden

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Hides the instructions in logon scripts written for Windows NT 4.0 and earlier.*

*Logon scripts are batch files of instructions that run when the user logs on. By default, Windows 2000 displays the instructions in logon scripts written for Windows NT 4.0 and earlier in a command window as they run, although it does not display logon scripts written for Windows 2000.*

*If you enable this policy, Windows 2000 does not display logon scripts written for Windows NT 4.0 and earlier.*

*Also, see the "Run Logon Scripts Visible" policy.*

- Run logon scripts visible

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Displays the instructions in logon scripts as they run.*

*Logon scripts are batch files of instructions that run when the user logs on. By default, the system does not display the instructions in the logon script.*

*If you enable this policy, the system displays each instruction in the logon script as it runs. The instructions appear in a command window. This setting is designed for advanced users.*

*If you disable this policy or do not configure it, the instructions are suppressed.*

- Run logoff scripts visible

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Displays the instructions in logoff scripts as they run.*

*Logoff scripts are batch files of instructions that run when the user logs off. By default, the system does not display the instructions in the logoff script.*

*If you enable this policy, the system displays each instruction in the logoff script as it runs. The instructions appear in a command window. This setting is designed for advanced users.*

*If you disable this policy or do not configure it, the instructions are suppressed.*

- Connect home directory to root of the share

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Restores the definitions of the %HOMESHARE% and %HOMEPATH% environment variables to those used in Windows NT 4.0 and earlier.*
>
> *If you enable this policy, the system uses the Windows NT 4.0 definitions. If you disable this policy or do not configure it, the system uses the new definitions designed for Windows 2000.*
>
> *Along with %HOMEDRIVE%, these variables define the home directory of a user profile. The home directory is a persistent mapping of a drive letter on the local computer to a local or remote directory.*
>
> *By default, in Windows 2000, %HOMESHARE% stores the fully qualified path to the home directory (such as \\server\share\dir1\dir2\homedir). Users can access the home directory and any of its subdirectories from the home drive letter, but they cannot see or access its parent directories. %HOMEPATH% stores a final backslash and is included for compatibility with earlier systems.*
>
> *On Windows NT 4.0 and earlier, %HOMESHARE% stores only the network share (such as \\server\share). %HOMEPATH% stores the remainder of the fully qualified path to the home directory (such as \dir1\dir2\homedir). As a result, users can access any directory on the home share by using the home directory drive letter.*
>
> *Tip: To specify a home directory in Windows 2000, in Active Directory Users and Computers or Local Users and Groups, right-click the name of a user account, click Properties, click the Profile tab, and in the "Home folder" section, select the "Connect" option and select a drive letter and home directory.*
>
> *Example: Drive Z is mapped to \\server\share\dir1\dir2\homedir.*
>
> *If this policy is disabled or not configured (Windows 2000 behavior):*
>
> *-- %HOMEDRIVE% = Z: (mapped to \\server\share\dir1\dir2\homedir)*
>
> *-- %HOMESHARE% = \\server\share\dir1\dir2\homedir*
>
> *-- %HOMEPATH% = *
>
> *If the policy is enabled (Windows NT 4.0 behavior):*
>
> *-- %HOMEDRIVE% = Z: (mapped to \\server\share)*
>
> *-- %HOMESHARE% = \\server\share*
>
> *-- %HOMEPATH% = \dir1\dir2\homedir*

- Limit profile size

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *When enabled, the default maximum profile size is: 30000 KB. The default reminder is every 15 minutes. The default message is: 'You have exceeded your profile storage space. Before you can log off, you need to move some items from your profile to network or local storage.*
>
> *The administrator may also choose to include registry in the file list, and to be notified when profile storage space is exceeded.*
>
> *Sets the maximum size of each roaming user profile and determines the system's response when a roaming user profile reaches the maximum size.*

*If you disable this policy or do not configure it, the system does not limit the size of roaming user profiles.*

*If you enable this policy, you can do the following:*

*-- Set a maximum permitted roaming profile size;*

*-- Determine whether the registry files are included in the calculation of the profile size;*

*-- Determine whether users are notified when the profile exceeds the permitted maximum size;*

*-- Specify a customized message notifying users of the oversized profile;*

*-- Determine how often the customized message is displayed.*

- Exclude directories in roaming profile

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: Local Settings; Temporary Internet Files; History, and Temp.*

*The administrator may enter multiple directory names, semi-colon separated, all relative to the root of the user's profile.*

*Lets you add to the list of folders excluded from the user's roaming profile.*

*This policy lets you exclude folders that are normally included in the user's profile. As a result, these folders need not be stored by the network server on which the profile resides, and do not follow users to other computers.*

*By default, the History, Local Settings, Temp, and Temporary Internet Files folders are excluded from the user's roaming profile.*

*If you enable this policy, you can exclude additional folders.*

*If you disable this policy or do not configure it, then only the default folders are excluded.*

*Note: You cannot use this policy to include the default folders in a roaming user profile.*

- Run these programs at user logon

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the administrator may enter the items to run at logon.*

*Specifies additional programs or documents that Windows starts automatically when a user logs on to the system.*

*To use this policy, click Show, click Add and, in the text box, type the name of the executable program (.exe) file or document file. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file.*

*Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the system starts the programs specified in the Computer Configuration policy just before it starts the programs specified in the User Configuration policy.*

*Also, see the "Disable legacy run list" and the "Disable the run once list" policies.*

- Disable the run once list

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Ignores customized run-once lists.*
>
> *You can create a customized list of additional programs and documents that are started automatically the next time the system starts (but not thereafter). These programs are added to the standard list of programs and services that the system starts.*
>
> *If you enable this policy, the system ignores the run-once list.*
>
> *If you disable this policy, or do not configure it, the system runs the programs in the run-once list.*
>
> *This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*
>
> *Tip: Customized run-once lists are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce.*
>
> *Also, see the "Disable legacy run list" policy.*

- Disable legacy run list

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Ignores the customized run list for Windows NT 4.0 and earlier.*
>
> *On Windows 2000 and Windows NT 4.0 and earlier, you can create a customized list of additional programs and documents that the system starts automatically when it starts. These programs are added to the standard run list of programs and services that the system starts.*
>
> *If you disable this policy, or do not configure it, Windows 2000 adds any customized run list configured for Windows NT 4.0 and earlier to its run list.*
>
> *If you enable this policy, the system ignores the run list for Windows NT 4.0 and earlier.*
>
> *This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.*
>
> *Tip: To create a customized run list by using a policy, use the "Run these applications at startup" policy.*
>
> *The customized run lists for Windows NT 4.0 and earlier are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run and HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run. They can be configured by using the "Run" policy in System Policy Editor for Windows NT 4.0 and earlier.*
>
> *Also, see the "Disable the run once list" policy.*

### Group Policy

- Group Policy refresh interval for users

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: 90 minutes. The random time added to the refresh interval to prevent all clients from requesting Group Policy at the same time is: 30 minutes.*

*Specifies how often Group Policy for users is updated while the computer is in use (in the background). This policy specifies a background update rate only for the Group Policies in the User Configuration folder.*

*In addition to background updates, Group Policy for users is always updated when they log on.*

*By default, user Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes.*

*You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update user Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.*

*If you disable this policy, user Group Policy is updated every 90 minutes (the default). To specify that Group Policy for users should never be updated while the computer is in use, select the "Disable background refresh of Group Policy" policy.*

*This policy also lets you specify how much the actual update interval varies. To prevent clients with the same update interval from requesting updates simultaneously, the system varies the update interval for each client by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that client requests overlap. However, updates might be delayed significantly.*

*Important: If the "Disable background refresh of Group Policy" policy is enabled, this policy is ignored.*

*Note: This policy establishes the update rate for user Group Policies. To set an update rate for computer Group Policies, use the "Group Policy refresh interval for computers" policy (located in Computer Configuration\Administrative Templates\System\Group Policy).*

*Tip: Consider notifying users that their policy is updated periodically so that they recognize the signs of a policy update. When Group Policy is updated, the Windows desktop is refreshed; it flickers briefly and closes open menus. Also, restrictions imposed by Group Policies, such as those that limit the programs a user can run, might interfere with tasks in progress.*

- Group Policy slow link detection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting for a slow connection is: 500 Kbps. Connections below this speed are considered slow and connections above this speed are considered fast.*

*Defines a slow connection for purposes of applying and updating Group Policy.*

*If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this policy, the system considers the connection to be slow.*

*The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, the policy processing policies in this folder let you override the programs' specified responses to slow links.*

*To use this policy, in the "Connection speed" box, type a decimal number between 0 and 4,294,967,200 (0xFFFFFFA0), indicating a transfer rate in kilobits per second. Any connection*

*slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast.*

*If you disable this policy or do not configure it, the system uses the default value of 500 kilobits per second.*

*This policy appears in the Computer Configuration and User Configuration folders. The policy in Computer Configuration defines a slow link for policies in the Computer Configuration folder. The policy in User Configuration defines a slow link for policies in the User Configuration folder.*

*Also, see the "Automatically detect slow network connections" and related policies in Computer Configuration\Administrative Templates\System\Logon.*

- Group Policy domain controller selection

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*When enabled, the default setting is: Use the Primary Domain Controller. The administrator may choose from among the following:*

*- Use the Primary Domain Controller*

*- Inherit from the Active Directory Snap-ins*

*- Use any available domain controller*

*Determines which domain controller the Group Policy snap-in uses.*

*-- "Use the Primary Domain Controller" indicates that the Group Policy snap-in reads and writes changes to the domain controller designated as the PDC Operations Master for the domain.*

*-- "Inherit from the Active Directory Snap-ins" indicates that the Group Policy snap-in reads and writes changes to the domain controller that Active Directory Users and Computers or Active Directory Sites and Services snap-ins use.*

*-- "Use any available domain controller" indicates that the Group Policy snap-in can read and write changes to any available domain controller.*

*If you disable this policy or do not configure it, the Group Policy snap-in uses the domain controller designated as the PDC Operations Master for the domain.*

*Tip: To change the PDC Operations Master for a domain, in Active Directory Users and Computers, right-click a domain, and then click "Operations Masters."*

- Create new Group Policy Object links disabled by default Properties

*Default Setting: Not configured.*

*Administrator may choose from among the following: Not configured, Enabled, and Disabled.*

*Creates new Group Policy object links in the disabled state.*

*This policy creates all new Group Policy object links in the disabled state by default. After you configure and test the new object links, either by using Active Directory Users and Computers or Active Directory Sites and Services, you can enable the object links for use on the system.*

*If you disable this policy or do not configure it, new Group Policy object links are created in the enabled state. If you don't want them to be effective until they are configured and tested, you must disable the object link.*

- Enforce Show Policies Only

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents administrators from viewing or using Group Policy preferences.*
>
> *A Group Policy administration (.adm) file can contain both true policies and preferences. True policies, which are fully supported by Group Policy, must use registry entries in the Software\Policies or Software\Microsoft\Windows\CurrentVersion\Policies registry subkeys. Preferences, which are not fully supported, use registry entries in other subkeys.*
>
> *If you enable this policy, the "Show Policies Only" command is turned on, and administrators cannot turn it off. As a result, Group Policy displays only true policies; preferences do not appear.*
>
> *If you disable this policy or do not configure it, the "Show Policies Only" command is turned on by default, but administrators can view preferences by turning off the "Show Policies Only" command.*
>
> *Tip: To find the "Show Policies Only" command, in Group Policy, click the Administrative Templates folder (either one), then right-click the same folder, and then point to "View."*
>
> *In Group Policy, preferences have a red icon to distinguish them from true policies, which have a blue icon.*

- Disable automatic update of ADM files

> *Default Setting: Not configured.*
>
> *Administrator may choose from among the following: Not configured, Enabled, and Disabled.*
>
> *Prevents the system from updating the Administrative Templates source files automatically when you open Group Policy.*
>
> *By default, when you start Group Policy, the system loads the most recently revised copies of the Administrative Templates source files (.adm) that it finds in the %Systemroot%\inf directory. The .adm files create the list of policies that appear under Administrative Templates in Group Policy.*
>
> *If you enable this policy, the system loads the .adm files you used the last time you ran Group Policy. Thereafter, you must update the .adm files manually.*
>
> *Note: Upgrading your .adm files does not overwrite your policy configuration settings. The settings are stored in Active Directory, not in the .adm files.*
>
> *Tip: To upgrade your .adm files manually, in Group Policy, right-click Administrative Templates (either instance), and then click Add/Remove Templates*

This Page Intentionally Left Blank

# Index

Access this computer from the network, 6
account
  Rename administrator account, 14
  Rename guest account, 15
Account lockout
  duration, 4
  reset counter, 4
  threshold, 4
Account Lockout Policy, 4
Act as part of the operating system, 6
Active Desktop, 177
  Add/Delete items, 180
  Allow only bitmapped wallpaper, 181
  Disable Active Desktop, 178
  Disable all items, 178
  Enable Active Desktop, 177
  Prohibit adding items, 179
  Prohibit changes, 179
  Prohibit closing items, 180
  Prohibit deleting items, 179
  Prohibit editing items, 179
  Wallpaper, 180
Active Directory, 181
  default path when searching for printers, 191
  Enalbe filter in Find dialog box, 182
  Hide Active Directory folder, 182
  Maximum size of Active Directory searches, 181
Active Directory Domains and Trusts, 129
Active Directory Sites and Services, 130
Active Directory Users and Computers, 129
Add workstations to domain, 7
Add/Remove Programs, 184
  Disable, 184
  Disable Support Information, 186
  Go directory to Components wizard, 186
  Hide Add New Programs page, 184
  Hide Change or Remove Programs page, 184
  Hide the 'Add a program from CD-ROM or floppy disk' option, 185
  Hide the 'Add programs from Microsoft' option, 185
  Hide the 'Add programs from your network' option, 186
  Hide Windows Components page, 185
  Specify default category for Add New Programs, 187
Additional restrictions for anonymous connections, 11
Administrative Templates, 83
  Windows Components, 28
Administrative Templates (Computers) Group Policy snap-in, 157
Administrative Templates (Users) Group Policy snap-in, 158
Allow
  admin to install from Terminal Services session (Windows Installer), 37
  bitmapped wallpaper only (Active Desktop), 181
anonymous connections
  additional restrictions, 11
AppleTalk Routing (MMC extension snap-in), 143
application log, 17
  Restrict guest access, 17
  Retain, 18
  Retention method, 18
assign an application, 2, 78
Audit
  access of global system objects, 11
  account logon events, 5
  account management, 5
  directory service access, 6
  logon events, 6
  object access, 6
  policy change, 6
  privilege use, 6
  process tracking, 6
  Shut down system immediately if unable to log security audits, 16
  Shut down the computer when the security audit log is full, 19
  system events, 6
  use of Backup and Restore privilege, 12
Audit Policy, 5
Automatic Certificate Request Settings, 23
Back up files and directories, 7
Browser User Interface, 78
Bypass traverse checking, 7
Cache transforms in secure location on workstation, 38
Carpoint, 118
Certificates (MMC snap-in), 130
certification authority, 23

Certification Authority (MMC extension snap-in), 144
Change the system time, 7
Clear virtual memory pagefile when system shuts down, 12
COM
  Download missing COM components, 42
Component Services (MMC snap-in), 131
Computer Management (MMC snap-in), 131
Control Panel, 182
  Disable Control Panel, 182
  Hide specified control panel applets, 183
  Show only specified control panel applets, 183
Create a pagefile, 7
Create a token object, 7
Create permanent shared objects, 7
CTRL+ALT+DEL requirement for logon
  Diable, 13
Custom user interface, 206
DCOM Configuration Extension (MMC extension snap-in), 145
Debug programs, 7
delegation
  enable computer and user accounts to be trusted, 8
delete an assigned application, 2
Deny
  access to this computer from the network, 8
  logon as a batch job, 8
  logon as a service, 8
  logon locally, 8
Desktop, 175
  Disable adding, dragging, dropping, and closing the Taskbar's toolbars, 177
  Disable adjusting desktop toolbars, 177
  Do not add shares of recently opened documents to My Network Places, 176
  Don't save settings at exit, 177
  Hide all icons on Desktop, 175
  Hide Internet Explorer icon on desktop, 176
  Hide My Network Places icon on desktop, 176
  Prohibit user from changing My Document path, 176
  Remove My Documents icon from desktop, 175
  Remove My Documents icon from Start Menu, 175
Desktop Sharing
  Disable, 28
Device Manager (MMC extension snap-in), 145
Device Manager (MMC snap-in), 132
DHCP Relay Management (MMC extension snap-in), 146
DHTML Edit Control, 117
Digitally sign
  client communication (always), 12
  client communication (when possible), 12
  server communication (always), 12
  server communication (when possible), 13
Disable
  Active Desktop, 178
  Add/Remove Programs, 184
  adding channels (Internet Explorer), 102
  adding schedules for offline pages (Internet Explorer), 103
  addition of printers, 190
  adjusting desktop toolbars, 177
  Advanced Calling button (NetMeeting), 88
  Advanced Menu (Task Scheduler), 33, 164
  Advanced page (Internet Explorer), 102
  all items (Active Desktop), 178
  all scheduled offlien pages (Internet Explorer), 105
  Application Sharing (NetMeeting), 86
  Audio (NetMeeting), 87
  AutoComplete for forms (Internet Explorer), 97
  Automatic Install of Internet Explorer, 30
  automatic update of ADM files (Group Policy), 216
  Autoplay, 40
  Autoplay (System), 208
  background refresh of Group Policy, 52
  Boot/Shutdown/Logon/Logoff status messages, 39
  browse dialog box for new source (Windows Installers), 35
  caching of Auto-Proxy scripts, 91
  Change Password (Logon/Logoff), 209
  changes to Taskbar and Start Menu Settings, 171
  changing accessibility settings, 94
  changing Advanced homepage settings (Internet Explorer), 90
  changing Automatic Configuration settings, 96
  changing Calendar and Contact settings, 98
  changing certificate settings (Internet Explorer), 96
  changing color settings (Internet Explorer), 93
  changing connection settings (Internet Explorer), 95
  changing font settings (Internet Explorer), 93
  changing history settings, 92
  changing home page settings (Internet Explorer), 91

changing language settings (Internet Explorer), 94
changing link color settings (Internet Explorer), 93
changing Messaging settings, 98
changing Profile Assistant settings, 97
changing proxy settings (Internet Explorer), 95
changing rating settings (Internet Explorer), 96
changing Temporary Internet files settings, 92
changing wallpaper (Display), 188
channel user interface completely (Internet Explorer), 105
Chat (NetMeeting), 85
closing the browser and Explorer windows (Internet Explorer), 108
command prompt (System), 207
Connections page (Internet Explorer), 101
Content page (Internet Explorer), 101
Context menu (Internet Explorer), 111
context menus for the taskbar, 172
Control Panel, 182
CTRL+ALT+DEL requirement for logon, 13
customizing browser toolbar buttons (Internet Explorer), 112
customizing browser toolbars (Internet Explorer), 112
default browser check (Internet Explorer), 99
default context menu (Windows Explorer), 121
deletion of printers, 190
DFS tab (Windows Explorer), 124
Directory Services (NetMeeting), 84
Display in Control Panel, 187
downloading of site subscription content, 105
Drag-and-Drop, 32
Drag-and-Drop (Task Scheduler), 163
drag-and-drop context menu on the Start Menu, 171
editing and creating of schedule groups (Internet Explorer), 106
editing schedules for offline pages (Internet Explorer), 103
external branding of Internet Explorer, 90
Find Files via F3 within the browser (Internet Explorer), 89
full duplex Audio (NetMeeting), 88
Full Screen menu option (Internet Explorer), 109
General page (Internet Explorer), 100
IE Security prompt for Windows Installer scripts, 35
importing and exporting favorites (Internet Explorer), 90
Internet Connection wizard, 94
Internet Options menu option (Internet Explorer), 110
legacy run list, 41
legacy run list (Logon/Logoff), 213
links to Windows Update, 167
Lock Computer (Logon/Logoff), 209
Logoff (Logon/Logoff), 209
Logoff on the Start Menu, 170
Make Available Offline (Network), 194
media source for any install (Windows Installer User Configuration), 166
NetMeeting 2.x Whiteboard, 86
New menu option (Internet Explorer), 107
New Task Creation, 32
New Task Creation (Task Scheduler), 163
offline page hit logging (Internet Explorer), 104
Open in New Window menu option (Internet Explorer), 111
Open menu option (Internet Explorer), 108
patching (Windows Installer), 35
Periodic Check for Internet Explorer software updates, 30
personalized menus (Start Menu), 173
programs on Settings menu (Start Menu & Taskbar), 168
Programs page (Internet Explorer), 102
registry editing tools (System), 207
reminder balloons (Network), 195
reminder balloons (Offline files), 64
remote Desktop Sharing, 28
Remove 'Tip of the Day' menu option (Internet Explorer), 110
removing channels (Internet Explorer), 103
removing schedules for offline pages (Internet Explorer), 104
Reset Web Settings feature (Internet Explorer), 99
rollback, 34
rollback (Windows Installer User Configuration), 166
run once list, 41
Save As Web Page Complete (Internet Explorer), 108
Save As...menu option (Internet Explorer), 107
Save this program to disk option (Internet Explorer), 112
Search Customication (Internet Explorer), 89
Security page (Internet Explorer), 100
showing the splash screen, 31
Shut Down command (Start Menu), 171

software update shell notifications on program launch, 30
Source menu option (Internet Explorer), 109
Support Information (Add/Remove Programs), 186
Task Deletion, 32
Task Deletion (Task Scheduler), 164
Task Manager (Logon/Logoff), 209
the run once list (Logon/Logoff), 213
UI to change keyboard navigation indicator settings (Windows Explorer), 124
UI to change menu animation settings, 124
user configuration of Offlien Files (Network), 192
user configuration of Offline files, 64
user tracking (Start Menu), 173
Whiteboard (NetMeeting), 86
Windows Installer, 33
Disable application Sharing
Application Sharing
Disable application sharing, 86
Disable the General page
Internet Control Panel
Disable the General page, 100
disconnecting session
Amount of idle time required before disconnecting session, 11
Disk Defragmenter (MMC snap-in), 133
Disk Management (MMC snap-in), 132
disk quota
Apply policy to removable media, 50
Default quota limit and warning level, 49
Enforce limit, 48
Log even when quota warning level exceeded, 50
Log event when quota limit exceeded, 50
policy processing (Group Policy), 52
Disk Quotas, 48
Display, 187
Disable changing wallpaper, 188
Disable Display in Control Panel, 187
Hide Apperance tab, 188
Hide Background tab, 187
Hide Screen Saver tab, 188
Hide Settings tab, 188
No Screen Saver, 188
Password protect the screen saver, 189
Screen saver executabe name, 189
Distributed File System (MMC snap-in), 133
DNS
Primary DNS Suffix, 51
DNS Client, 51
EFS
recovery policy processing (Group Policy), 53
eject removable NTFS media
Allow, 11
elevated privileges, 34
Windows Installer (User Configuration), 165
Enable
Active Desktop, 177
Automatic Configuration (NetMeeting), 83
Classic Shell, 120
computer and user accounts to be trusted for delegation, 8
disk quotas, 48
filter in Find dialog box, 182
Offline Files, 65
user control over installs, 36
user to browse for source while elevated (Windows Installer), 36
user to patch elevated products (Windows Installer), 37
user to use media source while elevated (Windows Installer), 37
encrypt
Do not automatically encrypt files moved to encrypted folders, 42
Encrypted Data Recovery Agents, 22
Enforce
disk quota limit, 48
user logon restrictions, 4
Enterprise Trust, 24
Event Log, 17
Settings, 17
Event Viewer (MMC extension snap-in), 146
Event Viewer (MMC snap-in), 134
FAX Service (MMC snap-in), 134
File System, 20
Folder Redirection, 83
policy processing (Group Policy), 53
Folder Redirection Group Policy snap-in, 158
Force shutdown from a remote system, 8
Generate security audits, 8
Group Policy, 51, 214
Apply for computers asynchronously during startup, 51
Apply for users asynchronously during logon, 52
Create new GPO links disable by default Properties, 216
Disable automatic update of ADM files, 216
Disable background refresh of Group Policy, 52
Disk Quota policy processing, 52
domain controller selection, 215
EFS recovery policy processing, 53
Enforce Show Policies Only, 216
Folder Redirection policy processing, 53
Internet Explorer Maintenance policy processing, 57
IP Security policy processing, 56

loopback processing mode, 60
refresh interval for domain controllers, 55
refresh interval for omputers, 54
refresh interval for users, 214
Registry policy processing, 57
Scripts policy processing, 58
Security policy processing, 58
slow link detection, 55, 215
Group Policy snap-in. *See* Microsoft Management Console (MMC)
Hide Property Pages, 31
Hide Property Pages (Task Scheduler), 162
Hide the common dialog places bar
Common Open File Dialog
Hide the common dialog places bar, 127
history
Clear history of recently opened documents on exit (Start Menu), 172
Do not keep history of recently opened documents (Start Menu), 172
IAS Logging (MMC extension snap-in), 147
IGMP Routing (MMC extension snap-in), 147
Increase quotas, 8
Increase scheduling priority, 9
Indexing Service (MMC snap-in), 135
installing
Prevent users from installing printer drivers, 14
Internet Authentication Service (MMC snap-in), 135
Internet Explorer, 89
Administrator Approved Controls, 115
Browser Menu
File Menu
Disable New menu option, 107
Browser Menus, 107
Disable Context menu, 111
Disable Open in New Window menu option, 111
Disable Save this program to disk option, 112
File Menu
Disable closing the browser and Explorer windows, 108
Disable Open menu option, 108
Disable Save As Web Page Complete, 108
Disable Save As...menu option, 107
Help Menu
Disable Remove 'Tip of the Day' menu option, 110
Remove 'For Netscape Users' menu option, 110
Remove 'Send Feedback' menu option, 111
Remove 'Tour' menu option, 111
Hide Favorite menu, 109
Tools Menu
Disable Internet Options...menu option, 110
View Menu
Disable Full Screen menu option, 109
Disable Source menu option, 109
Connection, 79
Automatic Browser Configuration, 79
Connection Settings, 79
Proxy Settings, 80
User Agent String, 80
Disable AutoComplete for forms, 97
Disable Automatic Install of IE components, 30
Disable caching of Auto-Proxy scripts, 91
Disable changing accessibility settings, 94
Disable changing Advacned homepage settings, 90
Disable changing Automatic Configuration settings (Internet Explorer), 96
Disable changing Calendar and Contact settings (Internet Explorer), 98
Disable changing certificate settings, 96
Disable changing color settings, 93
Disable changing connection settings, 95
Disable changing default browser check, 99
Disable changing font settings, 93
Disable changing history settings, 92
Disable changing homepage settings, 91
Disable changing language settings, 94
Disable changing link color settings, 93
Disable changing Messaging settings, 98
Disable changing Profile Assistant settings, 97
Disable changing proxy settings, 95
Disable changing rating settings, 96
Disable changing Temporary Internet files settings, 92
Disable external branding, 90
Disable importing and exporting favorites, 90
Disable Internet Connection wizard, 94
Disable Periodic Check for IE software updates, 30
Disable the Reset Web Settings feature, 99
Display error message on proxy script download failure, 92
Do not allow AutoComplete to save passwords, 98
Hide Internet Explorer icon on desktop, 176
Identity Manager
prevent user from using Identities, 99
Internet Control Panel, 100
Disable the Advanced page, 102
Disable the Connections page, 101

Disable the Content page, 101
Disable the Programs page, 102
Disable the Security page, 100
Offline Pages, 102
Disable adding channels, 102
Disable adding schedules for offline pages, 103
Disable all scheduled offline pages, 105
Disable channel user interface completely, 105
Disable downloading of site subcription content, 105
Disable editing and creating of schedule groups, 106
Disable editing schedules for offline pages, 103
Disable offline page hit logging, 104
Disable removing channels, 103
Disable removing schedules for offline pages, 104
Subscription Limits, 106
Persistence Behavior, 113
File size limits for Internet zone, 114
File size limits for Intranet zone, 113
File size limits for Local Machine zone, 113
File size limits for Restricted Sites zone, 114
File size limits for Trusted Sites zone, 114
Programs, 81
Search
Disable Find Files via F3 within the browser, 89
Disable Search Customication, 89
Security, 80
Authenticode Settings, 81
Security Zones and Content Ratings, 80
Toolbars, 112
Configure Toolbar Buttons, 113
Disable customizing browser toolbar buttons, 112
Disable customizing browser toolbars, 112
URLs, 80
Channels, 80
Favorites and Links, 80
Important URLs, 80
Use Automatic Detection for dial-up connections, 91
User Interface
Animated Bitmaps, 79
Browser Title, 78
Browser Toolbar Buttons, 79
Custom Logo, 79
Internet Explorer Maintenance, 78
Internet Explorer Maintenance Group Policy snap-in, 159
Internet Information Services (MMC snap-in), 136
Investor, 118
IP Routing (MMC snap-in), 148
IP Security, 24
Client (Respond Only), 25
IP Sec policy processing (Group Policy), 56
IPSec, 24
Secure Server (Require Security), 26
Server (Request Security), 27
IP Security (MMC snap-in), 136
IPX RIP Routing (MMC extension snap-in), 148
IPX Routing (MMC extension snap-in), 149
IPX SAP Routing (MMC extension snap-in), 149
ISAKMP/Oakley, 28
LAN Manager Authentication Level, 13
last user name in logon screen
Do not display, 13
LDAP, 78
Load and unload device drivers, 9
Local Policies, 5
Local Users and Groups (MMC snap-in), 137
Lock pages in memory, 9
log on, 43
Apply Group Policy for users asynchronously during logon, 52
Delete cached copies of roaming profiles, 44
Do not detect slow network connections, 45
Don't display welcome screen, 40, 205
Maximum wait time for Group Policy scripts, 44
Message text for users, 13
Message title for users, 13
Number of previous logons to cache, 14
Prompt user when slow link is detected, 46
Recovery Console
Allow automatic administrative logon, 14
Run logon scripts synchronously, 43
Run shutdown scripts visible, 44
Run startup scripts asynchronously, 43
Run startup scripts visible, 43
Run these programs at user logon, 41
slow network connection timeout for user profiles, 45
Timeout for dialog boxes, 47
Wait for remote user profile, 46
Log on
as a batch job, 9
as a service, 9
locally, 9
log size

Maximum application log size, 17
Maximum security log size, 17
Maximum system log size, 17
logging
Event logging level (Network, Offline Files), 196
Event logging level (Offline Files), 65
Logging (Windows Installer), 38
Logical and Mapped Drives (MMC extension snap-in), 150
logon time expires
Automatically logoff users, 12
logon time expires (local)
Automatically log off users, 12
Logon/Logoff, 209
Connect home directory to root of the share, 211
Disable Change Password, 209
Disable legacy run list, 213
Disable Lock Computer, 209
Disable Logoff, 209
Disable Task Manager, 209
Disable the run once list, 213
Exclude directories in roaming profile, 212
Limit profile size, 212
Run legacy logon scripts hidden, 210
Run logoff scripts visible, 211
Run logon scripts hidden, 210
Run logon scripts visible, 210
Run these programs at user logon, 213
Loopback
User Group Policy processing mode, 60
Manage auditing and security log, 9
Maximum
lifetime for service ticket, 4
lifetime for user ticket, 5
lifetime for user ticket renewal, 5
tolerance for computer clock synchronization, 5
Media Player, 115
Menu Controls, 115
Message text for users attempting to log on, 13
Message title for users attempting to log on, 13
Microsoft Agent, 116
Microsoft Chat, 116
Microsoft Management Console, 128
Microsoft Scriptlet Component, 118
Microsoft Survey Control, 117
Minimum
password length, 4
MMC, 128
Extension snap-ins, 143
AppleTalk Routing, 143
Certification Authority, 144
Connection Sharing (NAT), 144
DCOM Configuration Extension, 145
Device Manager, 145
DHCP Relay Management, 146
Event Viewer, 146
IAS Logging, 147
IGMP Routing, 147
IP Routing, 148
IPX RIP Routing, 148
IPX Routing, 149
IPX SAP Routing, 149
Logical and Mapped Drives, 150
OSPF Routing, 150
Public Key Policies, 151
RAS Dialin - User Mode, 151
Remote Access, 152
Removable Storage, 152
RIP Routing, 153
Routing, 153
Send Console Message, 154
Service Dependencies, 154
SMTP Protocol, 155
SNMP, 155
System Properties, 156
Group Policy snap-in, 156
Administrative Templates (Computers), 157
Administrative Templates (Users), 158
Folder Redirection, 158
Group Policy Tab for Active Directory Tools, 157
Internet Explorer Maintenance, 159
Remote Installation Services, 159
Scripts (Logon/Logoff), 160
Scripts (Startup/Shutdown), 160
Security Settings, 161
Software Installation (Computers), 161
Software Installation (Users), 162
Restrict the user from entering authormode, 128
Restrict users to the explicitly permitted use of snap-ins, 128
Restricted/Permitted snap-ins, 128
Active Directory Domains and Trusts, 129
Active Directory Sites and Services, 130
Active Directory Users and Computers, 129
Certificates, 130
Component Services, 131
Computer Management, 131
Device Manager, 132
Disk Defragmenter, 133
Disk Management, 132
Distributed File System, 133
Event Viewer, 134
FAX Service, 134

Indexing Service, 135
Internet Authentication Service (IAS), 135
Internet Information Services, 136
IP Security, 136
Local Users and Groups, 137
Performance Logs and Alerts, 137
QoS Admission Control, 138
Removable Storage Management, 138
Routing and Remote Access, 139
Security Configruation and Analysis, 139
Security Templates, 140
Services, 140
Shared Folders, 141
System Information, 141
Telephony, 142
Terminal Services Configuration, 142
WMI Control, 143
Modify firmware environment values, 9
MSNBC, 119
My Computer
Hide specified drives, 122
My Documents
Prohibit user from changing path, 176
Remove icon from desktop, 175
Remove icon from Start Menu, 175
My Network Places
Do not add shares of recently opened documents, 176
Hide icon on desktop, 176
No 'Computers Near Me', 125
No 'Entire Network', 125
NetMeeting, 28, 83
Application Sharing, 86
Prevent Application Sharing in true color, 87
Prevent Control, 87
Prevent Desktop Sharing, 86
Prevent Sharing, 86
Prevent Sharing Command Prompts, 86
Prevent Sharing Explorer windows, 87
Audio & Video, 87
Disable Audio, 87
Disable full duplex Audio, 88
Limit the bandwidth of Audio and Video, 87
Prevent changing DirectSound Audio setting, 88
Prevent receiving Video, 88
Prevent sending Video, 88
Disable Chat, 85
Disable Directory Services, 84
Disable NetMeeting 2.x Whiteboard, 86
Disable Whiteboard, 86
Enable Automatic Configuration, 83
Limit the size of sent files, 85
Options Page, 88
Disable the Advanced Calling button, 88
Hide the Audio page, 89
Hide the General page, 88
Hide the Security page, 89
Hide the Video page, 89
Prevent adding Directory Servers, 84
Prevent automatic acceptance of Calls, 85
Prevent changing Call placement method, 85
Prevent receiving files, 85
Prevent sending files, 85
Prevent viewing Web Directory, 84
Set Call Security options, 84
Set the intranet support Web page, 84
NetShow File Transfer Control, 117
Network, 62, 192
Offline Files, 192
Action on server disconnect, 193
Adminsitratively assigned offline files, 195
Disable 'Make Available Offline', 194
Disable reminder balloons, 195
Disable user configuration of Offline Files, 192
Event logging level, 196
Initial reminder balloon lifetime, 196
Non-default server disconnect actions, 193
Prevent use of Offline Files folder, 194
Reminder balloon frequency, 195
Reminder balloon lifetime, 196
Synchronize all offline files before logging off, 192
Network and Dial-up Connections, 69, 197
Allow configuration of connection sharing, 69
NTLM, 13
Offline files
Action on server disconnect, 62
Administratively assigned, 62
At logoff, delete loxal copy of user's offline files, 63
Default cache size, 63
Disable 'Make Available Offline', 64
Disable reminder balloons, 64
Disable user configuration of, 64
Enabled, 65
Event logging level, 65
Files not cached, 66
Initial reminder balloon lifetime, 66
Non-default server disconnect actions, 67
Prevent use, 67
Reminder balloon frequency, 68
Reminder balloon lifetime, 68
Subfolders available offline, 68
synchronize all offline files before logging off, 69

Offline Files, 62
OSPF Routing (MMC extension snap-in), 150
password
  complexity requirements, 4
  Disable Change Password (Logon/Logoff), 209
  minimum length, 4
  Prevent system maintenance of computer account password, 14
  Prompt user to change password before expiration, 14
  screen saver, 189
  send unencrpted password to connect to third-party SMB servers, 16
  store using reversible encryption, 4
passwords
  Do not allow AutoComplete to save (Internet Explorer), 98
Performance Logs and Alerts (MMC snap-in), 137
permissions
  Strengthen default permissions of global system objects, 16
Prevent
  access to drives from My Computer, 123
  adding Directory Servers (NetMeeting), 84
  Application Sharing in true color (NetMeeting), 87
  automatic acceptance of Calls (NetMeeting), 85
  changing Call placement method, 85
  changing DirectSound Audio setting (NetMeeting), 88
  Control (NetMeeting), 87
  Desktop Sharing (NetMeeting), 86
  receiving files (NetMeeting), 85
  receiving Video (NetMeeting), 88
  sending files (NetMeeting), 85
  sending Video (NetMeeting), 88
  Sharing (NetMeeting), 86
  Sharing Command Prompts (NetMeeting), 86
  Sharing Explorer windows (NetMeeting), 87
  Task Run or End, 31
  Task Run or End (Task Scheduler), 163
  user from using Identities (Internet Explorer), 99
  user of Offline Files folder (Network), 194
  viewing Web Directory (NetMeeting), 84
Printer
  browsing, 74
Printers, 70, 190
  Allow printers to be published, 70
  Allow pruning of published printers, 70
  Automatically publish new printers in Active Directory, 70
  Browse a common web site to find printers, 191
  Browse the network to find printers, 190
  Check published state, 71
  Computer location, 71
  Custom support URL, 71
  Default Active Directory path when searching for printers, 191
  Directory pruning interval, 72
  Directory pruning priority, 73
  Directory pruning retry, 73
  Disable addition of printers, 190
  Disable deletion of printers, 190
  Pre-populate printer search location text, 74
  Prune printers that are not automatically republished, 75
  Web-based printing, 75
Profile single process, 10
Profile system performance, 10
program launch
  Disable software update shell notifications, 30
Prohibit
  adding items (Active Desktop), 179
  Browse (from Task Scheduler), 33
  Browse (Task Scheduler), 164
  changes (Active Desktop), 179
  closing items (Active Desktop), 180
  deleting items (Active Desktop), 179
  editing items (Active Desktop), 179
  user from changing My Documents path, 176
proxy settings
  per-machine, 29
Public Key Policies, 21
Public Key Policies (MMC extension snap-in), 151
publish an application, 2, 78
QoS Admission Control (MMC snap-in), 138
RAS Dialin – User Mode (MMMC extension snap-in), 151
recent documents, 125
Recovery Console
  Allow automatic administrative logon, 14
  Allow floppy copy and access to all drives and all folders, 14
*recovery policy*, 22
**Recovery-agent policy**, 23
Regional Options, 191
  Restrict selection of Windows 2000 menus and dialogs language, 191
Registry, 20
  Disable registry editing tools (System), 207
  policy processing (Group Policy), 57
Remote Access (MMC extension snap-in), 152
Remote Installation Services, 82

Remote Installation Services Group Policy snap-in, 159
Removable Storage (MMC extension snap-in), 152
Removable Storage Management (MMC snap-in), 138
Remove
  common program groups from Start Menu, 167
  Disconnect item from Start Menu (Terminal Services Only), 39
  Documents menu from Start Menu, 168
  Favorites menu from Start Menu, 169
  File menu from Windows Explorer, 120
  Folder Options menu item from the Tool menu, 120
  For Netscape Users menu option (Internet Explorer), 110
  Help menu from Start Menu, 169
  links to Windows Update, 167
  Map Network Drive and Disconnect Network Drive (Windows Explorer), 120
  My Documents icon from Start Menu, 175
  My Documents icon from the desktop, 175
  Network & Dial-up Connections from Start Menu, 168
  Run menu from Start Menu, 170
  Search button from Windows Explorer, 121
  Search menu from Start Menu, 169
  Security option from Start Menu (Terminal Services Only), 39
  Send Feedback menu option, 111
  Shut Down command (Start Menu), 171
  Tour menu option (Internet Explorer), 111
  user's folder from the Start Menu, 167
Remove computer from docking station, 10
Rename administrator account, 14
Rename guest account, 15
Replace a process level token, 10
Restore files and directories, 10
Restrict
  CD-ROM access to locally logged-on users only, 15
  floppy access to locally logged-on user only, 15
  selection of Windows 2000 menus and dialogs language, 191
  user from entering authormode (MMC), 128
  users to the explicitly permitted use of snap-ins (MMC), 128
Restricted Groups, 19
RIP Routing (MMC extension snap-in), 153
roaming profile
  Exclude directories, 212
  Log users off when roaming profile fails, 47
  Wait for remote user profile, 46
roaming profiles
  Delete cached copies, 44
Routing (MMC extension snap-in), 153
Routing and Remote Access (MMC snap-in), 139
schedule tasks (domain controllers only)
  Allow server operators, 11
scripts
  Disable caching of Auto-Proxy scripts (Internet Explorer), 91
  Display error message on proxy script download failure (Internet Explorer), 92
  Group Policy snap-in, 160
  logon/logoff, 81
  Maximum wait time for Group Policy scripts, 44
  policy processing (Group Policy), 58
  Run legacy logon scripts hidden (Logon/Logoff), 210
  Run logoff scripts visible (Logon/Logoff), 211
  Run logon scripts synchronously, 43
  Run logon scripts synchronously (Logon/Logoff), 210
  Run logon scripts visible (Logon/Logoff), 210
  Run shutdown scripts visible, 44
  Run start up scripts visible, 43
  Run startup scripts asynchronously, 43
  Startup/Shutdown Group Policy snap-in, 160
Scripts (Logon/Logoff) Group Policy snap-in, 160
Scripts (Startup/Shutdown) Group Policy snap-in, 160
Secure Channel
  Digitally encrypt secure channel data (always), 15
  Digitally encrypt secure channel data (when possible), 15
  Reguire strong session key (Windows 2000 or later), 15
Secure system partition (for RISC platforms only), 16
Security
  Internet Explorer, 80
Security Configuration and Analysis (MMC snap-in), 139
security log, 17
  Restrict guest access, 17
  Retain, 18
  Retention method, 18
Security Options, 10
Security Settings, 81
Security Settings Group Policy snap-in, 161
Security Templates (MMC snap-in), 140

Security Zone
Use only machine settings, 28
Security Zones
Do not allow users to add/delete sites, 29
Security Zones and Content Ratings, 80
Send Console Message (MMC extension snap-in), 154
Service Dependencies (MMC extension snap-in), 154
Services (MMC snap-in), 140
Setting for Event Logs, 17
Seucurity Zones
Do not allow users to change policies, 29
Shared Folders (MMC snap-in), 141
Shockwave Flash, 117
Shut down
computer when the security audit log is full, 19
immediately if unable to log security audits, 16
Shut down the system, 10
shut down without having to log on
Allow, 11
slow network connection
Group Policy slow link detection, 55
Prompt user when slow link is detected, 46
timeout for user profiles, 45
slow network connections
Do not detect, 45
Smart card
removal behavior, 16
SMTP Protocol (MMC extension snap-in), 155
SNMP (MMC extension snap-in), 155
Software Installation, 77
policy processing (Group Policy), 59
Software Installation (Computers) Group Policy snap-in, 161
Software Installation (Users) Group Policy snap-in, 162
Software Settings, 77
splash screen
Disable, 31
Start Menu
Remove Disconnect (Terminal Services Only), 39
Remove Security Option (Terminal Services Only), 39
Start Menu & Taksbar
Do not keep history of recently opened documents, 172
Start Menu & Taskbar, 167
Add Logoff to the Start Menu, 170
Add 'Run in Separate Memory Space' check box to Run dialog box, 173
Clear history of recently opened documents on exit, 172
Disable and remove links to Windows Update, 167
Disable and remove the Shut Down command, 171
Disable changes to Taskbar and Start Menu Settings, 171
Disable context menus for the taskbar, 172
Disable drag-and-drop context menu on the Start Menu, 171
Disable Logoff on the Start Menu, 170
Disable personalized menus, 173
Disable programs on Settings menu, 168
Disable user tracking, 173
Do not use the search based method when resolving shell shortcuts, 174
Do not use the tracking based method when resolving shell shortcuts, 174
Gray unavailable Windows Installer programs Start Menu shortcuts, 174
Remove common program groups from Start Menu, 167
Remove Documents menu from Start Menu, 168
Remove Favorites menu from Start Menu, 169
Remove Help menu from Start Menu, 169
Remove Network & Dial-up Connections from Start Menu, 168
Remove Run menu from Start Menu, 170
Remove Search menu from Start Menu, 169
Remove user's folder from the Start Menu, 167
startup
Apply Group Policy for computers asynchronously during startup, 51
status messages
Disable Boot/Shutdown/Logon/Logoff status messages, 39
Verbose vs. normal, 40
Synchronize directory service data, 10
System, 39, 205
Century interpretation for Year 2000, 205
Code signing for device drivers, 206
Custom user interface, 206
Disable Autoplay, 208
Disable registry editing tools, 207
Disable the command prompt, 207
Don't display welcome screen at logon, 205
Don't run specified Windows applications, 207
Downloading missing COM components, 208
Run only allowed Windows applications, 207
System Information (MMC snap-in), 141
system log, 17

Restrict guest access, 17
Retain, 18
Retention method, 18
System Properties (MMC extension snap-ins), 156
System Services, 19
system shuts down
Clear virtual memory pagefile, 12
Take ownership of files or other objects, 10
Task Scheduler, 31, 162
Disable Advanced Menu, 164
Disable Drag-and-Drop, 163
Disable New Task Creation, 163
Disable Task Deletion, 164
Hide Property Pages, 162
Prevent Task Run or End, 163
Prohibit Browse, 164
Telephony (MMC snap-in), 142
Terminal Services Configuration (MMC snap-in), 142
Trusted Root Certification Authorities, 24
Unsigned driver installation behavior, 16
Unsigned non-driver installation behavior, 17
user profile
Maximum retries to unload and update, 47
User Rights Assignment, 6
Access this computer from the network, 6
Act a part of the operating system, 6
Add workstations to domain, 7
Back up files and directories, 7
Bypass traverse checking, 7
Change the system time, 7
Create a pagefile, 7
Create a token object, 7
Create permanent shared objects, 7
Debug programs, 7
Deny access to this computer from the network, 8
Deny logon as a batch job, 8
Deny logon as a service, 8
Deny logon locally, 8
Enable computer and user accounts to be trusted for delegation, 8
Force shutdown from a remote system, 8
Generate security audits, 8
Increase quotas, 8
Increase scheduling priority, 9
Load and unload device drivers, 9
Lockpages in memory, 9
Log on as a batch job, 9
Log on as a service, 9
Log on locally, 9
Manage auditing and security log, 9
Modify firmware environment values, 9
Profile single process, 10
Profile system performance, 10
Remove computer from docking station, 10
Replace a process level token, 10
Restor files and directories, 10
Shut down the system, 10
Synchronize directory service data, 10
Take ownership of files and other objects, 10
Windows Components, 83
Windows Explorer, 120
Common Open File Dialog, 127
Hide the common dialog back button, 127
Hide the dropdown list of recent files, 127
Disable default context menu, 121
Disable DFS tab, 124
Disable UI to change keyboard navigation indicator settings, 124
Disable UI to change menu animation settings (Windows Explorer), 124
Do not requrest alternate credentials, 126
Do not track Shell shortcuts during roaming, 122
Enable Classic Shell, 120
Hide Hardware tab, 124
Hide the Manage item on the Windows Explorer context menu, 121
Hide these specified drives in My Computer, 122
Maximum number of recent documents, 125
No 'Computers Near Me' in My Network Places, 125
No 'Entire Network' in My Network Places, 125
Only allow approved Shell extensions, 122
Prevent access to drives from My Computer, 123
Remove "Map Network Drive" and "Disconnet Network Drive", 120
Remove File menu, 120
Remove Search button, 121
Remove the Folder Options menu item from the Tool menu, 120
Request credentials for network installations, 126
Windows File Protection, 60
Hide the file scan progress window, 60
Limit cache size, 60
Set scanning, 61
Specify cache location, 61
Windows Installer, 33, 165
Alwyas install with elevated privileges, 165
Disable media source for any install, 166
Disable rollback, 166
Search order, 165
Windows Script Host, 3
Windows Settings, 78
WMI Control (MMC snap-in), 143