Windows XP Professional Resource Kit

Managing Desktops

Published: November 3, 2005

Deploying standard desktop configurations and managing users' computers and settings reduces the time required to support computer users in an organization. Microsoft Windows XP Professional includes desktop management technologies—collectively known as Microsoft IntelliMirror—that allow you to centrally manage the privileges, permissions, and capabilities of users and client computers and ensure that users' data, software, and settings are available to them when they move from one computer to another. Most IntelliMirror features rely on Group Policy, which requires the Microsoft Active Directory directory service, which is included with Microsoft Windows 2000 Server or Microsoft Windows Server™ 2003. Several of these desktop management tools and features can also be used to manage desktop computers in non–Active Directory environments.

For information on how to obtain the Windows XP Professional Resource Kit in its entirety, please see http://www.microsoft.com/mspress/books/6795.asp.

On This Page

Managing Desktops in Various Network Environments

Desktop Management tools and features available for managing Windows XP Professional–based clients differ depending upon whether the Windows XP Professional desktop operates exclusively in an Active Directory environment or in other network environments. IntelliMirror management technologies rely on Group Policy and most also require Active Directory; both are available in Windows 2000 Server and Windows Server 2003 environments. Group Policy requires Active Directory.

In an environment without Active Directory, you can use a variety of tools, such as Systems Management Server (SMS) for managing software distribution, the Internet Explorer Administration Kit for managing Internet Explorer settings, and System Policy for managing registry-based settings. In addition, each local computer has its own local Group Policy object (LGPO), regardless of whether it participates in a domain. While it is possible to set a variety of settings by using the LGPO, note that System Policy scales more easily to a large number of clients. The LGPO can be useful if you need to apply certain settings only to a small number of Windows XP Professional–based clients in a Windows NT 4.0 or other domain.

"Group Policy" refers to policy that relies on a hierarchical targeting mechanism based on Active Directory. Group Policy does not include the local Group Policy object (LGPO), which is specific to each computer rather than to objects in

Active Directory. Because LGPOs cannot be managed through Active Directory, they must instead be managed on each computer.

For Windows XP Professional desktops operating in other environments, such as Microsoft Windows NT version 4.0, UNIX, or Novell, or in a mixed environment, many desktop management capabilities and tools differ. Table 5-1 summarizes the differences in desktop management tools and functionality between Active Directory and non–Active Directory environments.

Table 5-1 Desktop Management Tools and Features in Active Directory and Non– Active Directory Environments

Management Task	Active Directory	Non–Active Directory
Configure registry-based settings for computers and users.	Administrative Templates deployed using Group Policy. Administrative templates deployed using local Group Policy object (LGPO).	System Policy LGPO
Manage local, domain, and network security.	Security Settings deployed using Group Policy. Security Settings deployed using the LGPO.	LGPO
Centrally install, update, and remove software.	Systems Management Server (SMS). Group Policy–based software distribution.	SMS
Manage Internet Explorer configuration settings after deployment.	Internet Explorer Maintenance in the Group Policy MMC snap-in (called Group Policy Object Editor in Windows Server 2003). Internet Explorer Maintenance deployed using the LGPO. Internet Explorer Administration Kit (IEAK).	LGPO IEAK
Apply scripts during user logon/logoff and computer startup/shutdown.	Logon/logoff and startup/shutdown scripts can be centrally configured using Group Policy or independently through the LGPO.	LGPO
Centrally manage users' folders and files on the network.	Folder Redirection in conjunction with Offline Files and Folders.	System Policy Manipulation of registry settings
Centrally manage user settings on the network.	Roaming User Profiles.	Roaming User Profiles (for Windows domains)

- User Rights
- Tools for Troubleshooting
- Differences with Windows XP Home Edition
- Accessibility Tools

You can also manage Windows XP Professional desktops on UNIX and Novell networks by using standards-based protocols such as TCP/IP, Simple Network Management Protocol (SNMP), Telnet, and Internetwork Packet Exchange (IPX). To enable policy-based administration on UNIX and Novell networks, use a local Group Policy object or System Policy.

↑ Top of page

Managing Desktops in an Active Directory Environment

When you use Windows XP Professional or Windows 2000 Professional on networks with Active Directory installed, you can take full advantage of IntelliMirror and Group Policy management features. If you are managing Windows XP Professional or Windows 2000 Professional desktops on networks and Active Directory is not installed, see “Managing Desktops Without Active Directory” later in this chapter.

IntelliMirror allows you to centrally manage workstations, saving you significant time while improving manageability. IntelliMirror ensures that users’ data, software, and personal settings are available when they move from one computer to another, whether or not their computers are connected to the network.

IntelliMirror consists of four components: **user data management**, **user settings management**, **computer settings management**, and **Group Policy–based Software Installation and Maintenance**. The IntelliMirror components can help you to:

- Centrally create and manage the configuration of each user’s desktop.
- Enable users to access files from any location at any time by using Roaming User Profiles and Folder Redirection in combination with Offline Files.
- Manage how software is deployed and installed on computers to ensure that users have the software they need to perform their jobs. Large organizations that need advanced software distribution and inventory capabilities should consider using Microsoft Systems Management Server (SMS) 2.0 or SMS 2003.
- Manage and enforce centralized data storage, which helps administrators keep important corporate data backed up.
- Save time when replacing computers by using Remote Installation Services (RIS) and Group Policy–based software installation and maintenance to easily replace applications, Roaming User Profiles to recover user profiles, and Folder Redirection to centrally manage files.

For more information about implementing IntelliMirror features, see the Distributed Systems Guide of the Microsoft Windows 2000 Server Resource Kit. For more information about deploying IntelliMirror in an Active Directory environment, see the Change and Configuration Management Deployment Guide link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

Implementing IntelliMirror

Active Directory and Group Policy provide the foundation for implementing IntelliMirror. Without Active Directory, you cannot take full advantage of IntelliMirror for managing clients. Table 5-2 shows the streamlined management tasks you can perform in an Active Directory environment.

Table 5-2 Management Tasks That Use IntelliMirror

Management Task	**IntelliMirror Feature**
Configure registry-based Group Policy settings for computers and users.	Administrative Templates
Manage local, domain, and network security.	Security Settings
Centrally install, update, and remove software.	Group Policy–based software distribution
Manage Internet Explorer configuration settings after deployment.	Internet Explorer Maintenance
Apply scripts during user logon/logoff and computer startup/shutdown.	Scripts
Centrally manage users' folders and files on the network, and make shared files and folders available offline.	Folder Redirection Offline Files and Folders
Centrally manage user profiles.	Roaming User Profiles

You can also use Group Policy to manage Remote Installation Services (RIS) by centrally setting client configuration options. For more information about using RIS, see Chapter 2, "Automating and Customizing Installations."

Active Directory stores information about all physical and logical objects on the network. This information is automatically replicated across the network to simplify finding and managing data, no matter where the data is located in the organization. The Active Directory structure you create determines how you apply Group Policy settings. In an Active Directory environment, Group Policy allows you to define and control the state of computers and users in an organization. Group Policy allows you to control more than 1000 customizable settings that you can use to centrally configure and manage users and computers.

Depending on the size of your organization, managing desktops, users, and their permissions can be a very complex task, especially because changes constantly happen. For example, users join and leave organizations, get promoted and transferred, and regularly change offices. Similarly, printers, computers, and network file shares are frequently added, removed, and relocated. When implemented in an Active Directory infrastructure, Group Policy–based IntelliMirror features greatly simplify managing these ongoing changes. Once set, Group Policy automatically maintains the state you design without requiring further intervention.

You can associate or link a particular Group Policy object (GPO) to one or more sites, domains, or organizational units (OUs) in an Active Directory structure. When multiple GPOs are linked to a particular site, domain, or OU, you can prioritize the order in which the GPOs are applied by determining when in the processing order particular settings are processed.

By linking GPOs to sites, domains, and OUs, you can implement Group Policy settings as broadly or as narrowly in the organization as necessary. Consider the following when linking GPOs:

- A GPO linked to a site applies to all users and computers in the site.

- A GPO linked to a domain applies directly to all users and computers in the domain and by inheritance to all users and computers in all the OUs that are linked to that domain. Note that Group Policy is *not* inherited across domains.
- A GPO linked to an OU applies directly to all users and computers in the OU and by inheritance to all users and computers in child OUs.
- GPOs are stored in Active Directory by domain. You can, however, link a site, domain, or OU to a GPO in another trusted domain, but this is generally not recommended for performance reasons.

For detailed procedures for linking a GPO to a site, domain, or OU, see Windows 2000 Server or Windows Server 2003 Help. For complete technical information about Active Directory and Group Policy, see the *Distributed Systems Guide* of the Microsoft Windows 2000 Server Resource Kit. For information about planning and deploying an Active Directory structure, see "Designing the Active Directory Structure" in the *Deployment Planning Guide*. For examples of Active Directory deployment scenarios, see the Windows 2000 Server Deployment Lab Scenarios link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

Using IntelliMirror to Manage Desktops

Windows XP Professional, Windows 2000, and Windows Server 2003 include IntelliMirror management technologies, which are primarily enabled by Group Policy. IntelliMirror and Group Policy greatly streamline managing user data, managing user settings, managing computer settings, and installing and maintaining software.

User Data Management

Files that a user creates and uses are *user data*. Examples are word processing documents, spreadsheets, or graphics files. User data belongs to the user and is located on the user's computer or on a network share to which the user has permissions.

Less obvious forms of user data include Microsoft Internet Explorer cookies and Favorites and customized templates. User data is usually hard to re-create—for example, a template that has undergone extensive design work and customization. With IntelliMirror, users can transparently access their data from any Windows XP Professional–based or Windows 2000 Professional–based computer on the network, regardless of whether or not that computer is their primary computer.

IntelliMirror technologies that support user data management include:

- Folder Redirection
- Offline Files and Synchronization Manager
- Roaming User Profiles

You can ensure that users' data is always available to them in the following ways.

Protecting user data by using Folder Redirection

You can redirect user data to a network share, where it can be backed up as part of routine system maintenance. This can be done so that the process is transparent to the user. It is recommended that users be trained to store all user data in My Documents (in the built-in subfolders My Pictures, My Music, and My Videos, and in any subfolders they create to organize their data). The My Documents folder is then redirected to a network share. This capability helps to enforce corporate directives such as storing business-critical data on servers that are centrally managed by the IT staff. If users are in the habit of storing files on their desktops, you should also consider redirecting the desktop.

Although the Application Data folder can be redirected using Folder Redirection, this is generally recommended only in the following cases:

- To reduce the size of the profile—thereby decreasing logon time—on multi-user computers where you have enabled a Group Policy setting to delete cached profiles. This gives users access to their application data, but without the need to download possibly large files every time they log on.
- To reduce the size of the profile in situations where keeping initial logon time short is a top priority, such as on terminals.
- For Terminal Services clients.

Providing users access to their data even when they are disconnected from the network
By using Offline Files and Synchronization Manager, administrators can ensure that the most up-to-date versions of a user's data reside on both the local computer and on the server. You can use Offline Files in conjunction with Folder Redirection to make available offline those folders that have been redirected to a server. Users can manually configure which files and folders are available offline, or administrators can configure them through Group Policy. The file is stored on a server, and the file on the local computer is synchronized with the network copy. Changes made while offline are synchronized with the server when the user reconnects to the network. Offline Files now supports Distributed File System (DFS) and Encrypting File System (EFS).

Enabling roaming user profiles
Although profiles are commonly used as a method of managing user settings (such as a user's shortcuts and other customizations of their environment), the profile also contains user data, including Favorites and Cookies. When roaming user profiles are enabled, users can access this data when they log on to any computer on the network. Windows XP Professional Group Policy settings allow the profile to roam correctly and free up system memory.

User Settings Management

With the user settings management tools in Windows XP Professional, you can centrally define computing environments for groups of users, and grant or deny users the ability to further customize their environments.

By managing user settings, you can:

- Reduce support calls by providing a preconfigured desktop environment appropriate for the user's job.
- Save time and costs when replacing computers by automatically restoring the user's settings.
- Help users be more efficient by automatically providing their desktop environment, no matter where they work.

The primary IntelliMirror technologies that support user settings management is Roaming User Profiles and Administrative Templates. The policy settings in Administrative Templates can control the desktop with predefined configurations; for more information, see the "Administrative Templates" section, later in this chapter.

A user profile contains:

- The portion of the registry that stores settings such as Windows Explorer settings, persistent network connections, taskbar settings, network printer connections, and user-defined settings made from Control Panel, Accessories, and application settings.

- A set of profile folders that store information such as shortcut links, desktop icons, and startup applications.

User profiles are located by default on the local computer; one profile is created for each user who has logged on interactively to that computer. By configuring user profiles to roam, you can ensure that the settings in a user's profile are copied to a network server when the user logs off from the computer and are available to the user no matter where he or she next logs on to the network.

While useful for roaming users, roaming user profiles are also beneficial for users who always use the same computer. For these users, roaming user profiles provide a transparent way to back up their profile to a network server, protecting the information from individual system failure. If a user's primary workstation needs to be replaced, the new computer receives the user's profile from the server as soon as the user logs on.

Some folders in a user profile cannot be configured to roam; these are found in the Local Settings folder and include the subfolders Application Data (not to be confused with the "other" Application Data folder that is a peer of Local settings, which *does* roam), History, Temp, and Temporary Internet Files. These folders contain application data that is not required to roam with the user, such as temporary files, noncritical settings, and data too large to roam effectively. This data is not copied to and from the server when a user logs on or logs off.

As an illustration of using roaming and nonroaming folders, you might configure Internet Explorer to store a user's Favorites in the roaming portion of the user profile and store the temporary Internet files in the local, nonroaming portion of the user profile. By default, the History, Local Settings, Temp, and Temporary Internet Files folders are excluded from the roaming user profile. You can configure additional folders to not roam by specifying them in the Group Policy snap-in, at User Configuration\Administrative Templates\System\User Profiles\Exclude directories in roaming profile.

Computer Settings Management

Group Policy settings also allow you to define how desktop computers are customized and restricted on your network. For optimal control of workstations, use Group Policy objects in an Active Directory environment to centralize computer management. However, if Active Directory is not deployed, you can control security on a computer-by-computer basis by using the local Group Policy object. Each computer has one LGPO that can be used to manage the computer outside of an Active Directory environment. If you configure desktop security this way, make sure to set workstation security to match corporate security standards.

The Computer Configuration tree in the Group Policy Microsoft Management Console (MMC) snap-in includes the local computer-related Group Policy settings that specify operating system behavior, desktop behavior, application settings, security settings, computer-assigned application options, and computer startup and shutdown scripts. Computer-related Group Policy settings are applied when the operating system starts up and during periodic refresh cycles. See "Using Group Policy to Manage Desktops," later in this chapter for more information.

You can also customize computer configuration settings by using the Group Policy MMC snap-in, thus simplifying individual computer setup.

Group Policy–Based Software Distribution

While the advanced software deployment and management features of

Systems Management Server 2.0 (SMS) or SMS 2003 offer distinct advantages in enterprise-sized organizations—such as inventory, diagnosis, and monitoring—Group Policy provides some ability to deploy software to workstations and servers running Windows 2000 or later. With Group Policy–based software deployment, you can target groups of users and computers based on their location in the Active Directory. Group Policy–based software deployment uses Windows Installer as the installation engine on the local computer.

The Software Installation and Maintenance component of Group Policy allows you to efficiently deploy, patch, upgrade, and remove software applications without visiting each desktop. This gives users reliable access to the applications that they need to perform their jobs, no matter which computer they are using.

Group Policy–based software distribution enables you to:

- Centrally deploy new software, upgrade applications, deploy patches and operating system upgrades, and remove previously deployed applications that are no longer required.
- Ensure that users have the software they need to be productive without an Information Technology (IT) administrator or technical support person having to visit each computer.
- Create a standard desktop operating environment that results in uninterrupted user productivity and straightforward administration.
- Maintain version control of software for all desktop computers in the organization.
- Identify and diagnose Group Policy setting failures by using Resultant Set of Policy (RSoP) in logging mode.
- Deploy, in combination with Windows Installer, 64-bit applications as well as 32-bit applications.

Using the Software Installation extension of the Group Policy MMC snap-in, you can centrally manage the installation of software on a client computer, either by assigning applications to users or computers or by publishing applications for users. As Table 5-3 describes, you can:

- **Assign software to users.** As an administrator, you can install applications assigned to users the first time they log on after deployment, or you can have the application and its components install on demand as the user invokes that functionality.
- **Assign software to computers.** When you assign an application to a computer, the installation occurs the next time the computer starts up, and the application is available for all the users on that computer.
- **Publish software for users.** You can publish applications for users only. Those users can choose to install the software from a list of published applications located in **Add or Remove Programs** in Control Panel. **Add or Remove Programs** includes an active Web link that is associated with each application that provides users with the support information they need to install certain applications. For example, the default support link for Microsoft Office is http://www.microsoft.com/office. Administrators can overwrite this default by using the Software Installation extension of the Group Policy snap-in.

Table 5-3 Approaches to Assigning and Publishing Software

Situation or Condition	**Publish**	**Assign to User (Install on Demand)**	**Assign to User (Full Install)**	**Assign to Computer**
Once the administrator deploys the software, it is available for installation:	The next time the user, to whom this application's Group Policy setting applies, logs on. It is also immediately visible in Add or Remove Programs.	The next time the user, to whom this application's Group Policy setting applies, logs on. It is also immediately visible in Add or Remove Programs.	The next time the user logs on. It is also immediately visible in Add or Remove Programs.	The next time the computer is started.
The software is installed:	By the user from Add or Remove Programs or, optionally, by opening an associated document (for applications deployed to auto-install).	By the user from the Start menu or a desktop shortcut or by opening an associated document.	Automatically when the user logs on.	Automatically when the computer is started.
The software is not installed and the user opens a file associated with the software:	The software installs only if Auto-Install is selected.	The software installs.	Does not apply. The software is already installed.	Does not apply. The software is already installed.
The user wants to remove the software by using Add or Remove Programs:	The user can uninstall the software, and subsequently choose to install it again by using Add or Remove Programs.	The user can uninstall the software, but it is re-assigned the next time the user logs on. It is available for installation again from the typical software distribution points.	The user can uninstall the software, but it is re-assigned the next time the user logs on. It is available for installation again from the typical installation points.	Only the local administrator and the network administrator can remove the software.

Using Group Policy to Manage Desktops

Group Policy is the primary tool for defining and controlling how programs, network resources, and Windows XP Professional and Windows 2000 Professional behave for users and computers in an organization. Similar to the way in which information is stored in Microsoft Word .doc files, Group Policy settings are contained in Group Policy objects (GPOs) created by using the Group Policy MMC snap-in.

Using Group Policy in an Active Directory environment, you can specify a user or computer configuration once, and then rely on the Windows XP Professional or Windows 2000 operating system to enforce that configuration on all affected client computers until you change it. After you apply Group Policy, the system maintains the state without further intervention.

You can define configurations by implementing Group Policy settings from a central location for hundreds or even thousands of users or computers at one time. For example, you might use Group Policy to implement the following rules:

- Install Microsoft Office XP or Microsoft Office 2003 on all computers used by members of the Sales Department.
- Prevent temporary personnel from accessing Control Panel.
- Manage access to adding or removing hardware.

Note Do not confuse Group Policy settings with preferences. Group Policy settings are created by an administrator and enforced automatically. Preferences are system settings and configuration options, such as a screen saver or the view in My Documents that users set and alter without an administrator’s intervention. Group Policy settings take precedence over preferences.

Group Policy Objects

Each combination of Group Policy settings that you configure is called a *Group Policy object (GPO)*. You can link GPOs to computers and users based on their location in an Active Directory structure. That is, you can link a GPO to a site, domain, or organizational unit (OU). Each GPO is applied as part of the startup process or when a user logs on to a workstation. The settings within the GPOs are evaluated by the affected clients, using the hierarchical nature of Active Directory, as described in “GPO Processing Order,” later in this section.

Note Every computer has one LGPO, which is stored on the local computer itself. Because LGPOs must be set and modified individually on every client computer, it is recommended that you use LGPOs to manage clients only if Active Directory is not deployed in your environment, and only if you are not using the Windows XP Professional or Windows 2000 Group Policy Administrative Templates with Windows NT 4.0 System Policy.

To create, edit, and manage a GPO, use the Group Policy MMC snap-in, either as a stand-alone tool or as an extension to an Active Directory snap-in (such as the Active Directory Users and Computers snap-in or the Active Directory Sites and Services snap-in). When working in an Active Directory environment, the preferred method is to use the Group Policy snap-in as an extension to an Active Directory snap-in. This allows you to browse Active Directory for the correct Active Directory container, and then define Group Policy based on the selected scope. To access Group Policy from either the Active Directory Users and Computers snap-in or in the Active Directory Sites and Services snap-in, select the **Group Policy** tab from the **Properties** page of a site, domain, or organizational unit.

Tip An alternative to using the standard Group Policy tools to create and manage Group Policy is to use the Group Policy Management Console (GPMC). GPMC simplifies the management of Group Policy by making it easier to understand, deploy, manage, and troubleshoot Group Policy implementations and also enables automation of Group Policy operations via scripting. GPMC runs on Windows Server 2003 computers and on Windows XP Professional SP1 with the .NET Framework installed, and it can manage Group Policy in either Windows 2000 or Windows Server 2003 domains. For more information about the GPMC, search the Microsoft Download Center (http://www.microsoft.com/downloads) for "Group Policy Management Console."

When you create a GPO, start with a template that contains all the Group Policy settings available for you to configure. Because Group Policy settings apply to either computers or users, GPOs contain trees for each:

- **Computer Configuration.** All computer-related Group Policy settings that specify operating system behavior, desktop behavior, security settings, computer startup and shutdown scripts, computer-assigned applications, and any settings provided by applications.
- **User Configuration.** All user-related Group Policy settings that specify operating system behavior, desktop settings, security settings, user-assigned and user-published application options, folder redirection options, user logon and logoff scripts, and any Group Policy settings provided by applications.

  Warning If an Active Directory domain contains both Windows 2000 Professional–based and Windows XP Professional–based clients, any new Group Policy settings specific to Windows XP Professional that you configure do not apply to the Windows 2000–based clients. See Group Policy Help or the Extended view in the Group Policy snap-in for the desktop operating system required for each setting to apply.

GPO Processing Order

The computer policy portion of Group Policy is applied during the startup process and periodic refresh cycles. The user policy portion of Group Policy is applied when the user logs on to the computer and during the periodic refresh cycle. When a computer starts, computer policy is applied during the boot process. Then, when a user logs on, user policy is applied in the following order: local GPO, GPOs linked to sites, GPOs linked to domains, and GPOs linked to organizational units (OUs). In the case of nested OUs, GPOs associated with parent OUs are processed prior to GPOs associated with child OUs. Keep this processing order in mind when configuring multiple GPOs to centrally manage desktops in your network environment.

Note If a setting in a later-applied GPO is not configured, it does not overwrite settings configured in earlier-applied GPOs.

This order of application is the default behavior. You can modify the default processing order by using the **No Override**, **Block Policy Inheritance**, or **Loopback** Group Policy settings. These allow you to modify the rules of inheritance, either by forcing GPOs to affect groups of users or computers or by preventing higher-level GPOs from affecting groups of users or computers.

Resultant Set of Policy

The biggest change in Group Policy for Windows XP Professional is the introduction of the Resultant Set of Policy (RSoP) MMC snap-in. RSoP gives administrators a powerful and flexible tool for troubleshooting Group Policy. RSoP allows you to see the aggregate effect of Group Policy on a target user or computer, including which settings take precedence over others.

RSoP is enabled by Windows Management Instrumentation (WMI) by leveraging the capability of WMI to extract data from the registry, drivers, the file system, Active Directory, Simple Network Management Protocol (SNMP), Windows Installer, Microsoft SQL Server™, various networking features, and Microsoft Exchange Server.

Use Logging mode to determine which GPO settings are actually applied to a target user or computer. You can also use logging mode on a stand-alone computer.

For example, a help desk worker can connect to any Windows XP Professional–based computer on the network and run Logging mode if they have local administrator access on the target computer.

Warning The default configuration of Windows Firewall in Windows XP Service Pack 2 prevents you from remotely administering RSoP. For more information, see article 883611 in the Knowledge Base on Microsoft TechNet (http://support.microsoft.com/kb/883611).

Managing Users and Desktops by Using Group Policy Extensions

Group Policy provides several extensions you can use to configure GPOs that enable IntelliMirror features and manage users. These extensions include:

- Administrative Templates
- Security Settings
- Software Installation and Maintenance
- Scripts (computer startup and shutdown scripts, and user logon and logoff scripts)
- Folder Redirection
- Internet Explorer Maintenance
- Remote Installation Services

Note Folder Redirection, Software Installation and Maintenance, and RIS require Active Directory; they are not present on the local Group Policy object and cannot be managed by using the local Group Policy object. If Active Directory is not deployed on your network, use System Policy instead.

You can use any of these extensions to apply Group Policy to users or computers, although settings are different for users and computers. Use the Group Policy snap-in to access the extensions. By default, all the available extensions are loaded when you start the Group Policy snap-in. Different extensions are available depending on whether you are viewing the local Group Policy object or Active Directory domain–based Group Policy.

Administrative Templates

Administrative templates (.adm files) are *Unicode* files that you can use to configure the registry-based settings that govern the behavior of many services, applications, and operating system components such as the **Start** menu. By default, the Group Policy snap-in contains four .adm files that cumulatively contain almost 1400 settings for Windows XP Service Pack 2 machines. You can also access three additional .adm files that can be used with the Windows NT 4.0 System Policy Editor. The .adm files are described in Table 5-4.

Table 5-4 Administrative Template Files

.adm File	Use With	Description

System.adm	Windows XP Professional	Contains many settings that you can use to customize the user's operating environment
Inetres.adm	Windows XP Professional	Contains settings for Internet Explorer
Conf.adm	Windows XP Professional	Contains settings you can use to configure Microsoft NetMeeting
Winnt.adm	Windows NT 4.0 System Policy Editor, Poledit.exe	Contains policy for Windows NT 4.0–based clients
Wmplayer.adm	Windows XP Professional	Contains settings you can use to configure Windows Media Player
Common.adm	Windows NT 4.0 System Policy Editor, Poledit.exe	Contains policy for client computers running Windows NT 4.0, Microsoft Windows 95, and Microsoft Windows 98
Windows.adm	Windows NT 4.0 System Policy Editor, Poledit.exe	Contains policy for Windows 95–based and Windows 98–based clients
Wuau.adm	Windows XP Service Pack 1 and later	Contains policy for configuring Automatic Updates and Software Update Services (SUS) SP1 client functionality

An .adm file specifies a hierarchy of categories and subcategories that together define how the Group Policy snap-in displays the options. The file also indicates the registry locations where the settings are stored if a particular selection is made, specifies any options or restrictions in values that are associated with the selection, and might specify a default value if a selection is activated.

In Windows 2000 Professional and Windows XP Professional, all Group Policy settings set registry entries in either the \Software\Policies tree (the preferred location for all new policies) or the \Software\Microsoft\Windows\CurrentVersion\Policies tree, in either the HKEY_CURRENT_USER subtree or the HKEY_LOCAL_MACHINE subtree.

Policy settings that are stored in these registry subkeys are known as *true policy settings*. Storing settings here has the following advantages:

- These subkeys are secure and cannot be modified by a nonadministrator.
- When Group Policy changes for any reason, these subkeys are cleaned, and then the new Group Policy–related registry entries are rewritten.

This prevents Windows NT 4.0 behavior, where System Policy settings result in persistent settings in the registry. A policy remains in effect until the value of its corresponding registry entry is reversed, either by a counteracting policy or by editing the registry. These settings are stored outside the approved registry locations just mentioned and are known as *preferences*.

By default, only true policy settings are displayed in the Group Policy snap-in. Because they use registry entries in the Policies subkeys of the registry, they will *not* cause persistent settings in the registry when the GPO that applies them is no longer in effect. The following .adm files are displayed by default:

- System.adm, which contains operating system settings
- Inetres.adm, which contains Internet Explorer restrictions
- Conf.adm, which contains NetMeeting settings
- WMPlayer.adm, which contains Windows Media Player settings
- Wuau.adm, which contains Automatic Updates settings (found in Windows XP Service Pack 1 and later)

Administrators can add additional .adm files to the Group Policy snap-in that set registry values outside of the Group Policy subkeys. These settings are referred to as *preferences* because the user, application, or other parts of the system can also change the settings. By creating non–Group Policy .adm files, the administrator ensures that certain registry entries are set to specified values.

One useful feature of the Windows XP Professional Group Policy snap-in is view filtering. For example, you can hide settings that aren't configured or view only settings supported on a particular operating system platform.

To filter the view of the Group Policy snap-in

1. Click **View**, and then click **Filtering**.
2. Select the **Filter by requirements information** check box, and then in the list box select the check boxes for the categories that you want to make visible.
3. If you want to hide settings that are not configured, select the **Only show configured policy settings** check box. If you do this, only enabled or disabled settings will be visible.
4. If you want to hide Windows NT 4.0–style system policy settings, make sure that the **Only show policy settings that can be fully managed** check box is selected. This option is recommended, and it is enabled by default.

You can also prevent administrators from viewing or using non-policy settings by enabling the **Enforce Show Policies Only** Group Policy setting in **User Configuration\Administrative Templates\System\Group Policy**.

The icon for non-policy or preference settings is red. True policy settings have a blue icon.

Use of non–Group Policy settings within the Group Policy infrastructure is strongly discouraged because of the persistent nature of these registry-based settings. To set registry-based policy settings on client computers running Windows NT 4.0, Windows 95, and Windows 98, use the Windows NT 4.0 System Policy Editor tool, Poledit.exe, instead.

Extended view for the Group Policy snap-in now provides Explain text for the selected Group Policy setting without having to open a separate Help window. It also clearly shows which operating system client platform is required for the selected setting to apply. You can now more easily determine which settings will function depending on the existing desktop operating systems on your network.

A Group Policy settings spreadsheet is available on the Web for easy tracking of your configured Group Policy settings. See the Group Policy Object Settings spreadsheet link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

Security Settings

Use the Security Settings extension to set the security options for computers and users within the scope of a GPO. For information about defining security settings for the domain and network, see the *Distributed Systems Guide* of the Microsoft Windows 2000 Server Resource Kit.

The Security Settings extension of the Group Policy snap-in complements existing system security management features such as the Local Security Policy snap-in. You can continue to change specific settings as needed.

You can configure security for computers to include:

- **Account policies**, such as computer security settings for password policy, lockout policy, and Kerberos authentication protocol policy in Active Directory domains.

  Warning Security settings are applied only at the domain level. If configured at the OU level, they are neither processed nor applied.

- **Local policies**, including security settings for auditing, assigning user rights (such as who has network access to the computer), and security options (such as determining who can connect to a computer anonymously).
- **Event logging**, which controls settings such as the size and retention method for the Application, Security, and System event logs.
- **Restricted groups**, which allows administrators to control individual and group membership in security-sensitive groups. You can enforce a membership policy regarding sensitive groups, such as Enterprise Administrators or Payroll.
- **System services**, including services that control startup mode and access permissions for system services, such as who is allowed to stop and start the fax service.
- **Registry security**, which allows you to configure security settings for registry containers, including access control, audit, and ownership.
- **File system**, which configures security settings for file-system objects, including access control, audit, and ownership.
- **Public Key policies**, which control and manage certificate settings.
- **IP Security policies**, which propagates Internet Protocol security (IPSec) policy to any computer accounts affected by the GPO. For users, you can define IPSec security. This propagates IPSec policy to any user accounts affected by the GPO.

Incremental security templates
Windows XP Professional includes several incremental security templates. By default, these templates are stored in *systemroot*\Security\Templates. You can customize these predefined templates by using the Security Templates MMC snap-in or by importing them into the Security Settings extension of the Group Policy snap-in. These templates include:

- **Compatible.** The Compatible template (Compatws.inf) relaxes the default permissions for the Users group so that older applications written to less stringent security standards are more likely to run.
- **Secure.** Two templates, Securews.inf and Securedc.inf, work on workstations, servers, and domain controllers. These provide increased security compared to the access control permissions set by default when Windows XP Professional is installed. The Secure configuration includes increased security settings for Account Policy, Auditing, and some common security-related registry subkeys and entries.

  High Secure. The High Secure templates are Hisecws.inf and Hisecdc.inf.

- These provide increased security over the secure configuration, and they work on workstations, servers, and domain controllers. This configuration requires that all network communications be digitally signed and encrypted.
- **Root Directory Permissions.** The rootsec.inf template can be used to reapply the default root directory permissions for the root of the system volume if they are inadvertently altered. The template can also be used to apply the same root permissions to other volumes on the computer.
- **No Terminal Server user SID.** The Notssid.inf template is used only when Terminal Server is running in application compatibility mode.

In addition, the Setup security.inf template, which is not incremental, contains the default security settings applied to the computer during Setup, including the file permissions for the root of the system volume. This template, or portions of it, can be used for disaster recovery purposes, but this template should never be applied using Group Policy because it contains a large amount of data and can degrade performance when Group Policy is periodically refreshed. This template should be applied only to the local computer using the Security Configuration and Analysis snap-in because the Setup security.inf template is created during installation and is unique for each computer.

For more information about these templates, see Chapter 17, "Managing Authorization and Access Control."

Software Installation

Use the Software Installation extension of the Group Policy snap-in to centrally manage software in your organization. You can assign (make mandatory) or publish (make optionally available) software to users, and assign (but not publish) software to computers. For more information about using the Software Installation extension, see "Using IntelliMirror to Manage Desktops" earlier in this chapter.

Scripts

You can use Group Policy–based scripts to automate computer startup and shutdown, and user logon and logoff sessions. You can use any language supported by Windows Script Host (WSH), a language-independent scripting host for 32-bit Windows platforms. Your options include Microsoft Visual Basic Scripting Edition (VBScript), JavaScript, Perl, and batch files (with .bat and .cmd extensions) such as in Microsoft MS-DOS.

WSH is included in Windows XP Professional. With WSH, you can run scripts directly in Windows XP Professional by double-clicking a script file, or by typing the name of a script file at the command prompt.

You can use any WSH scripting tool, including the VBScript programming system and Microsoft JScript development software, to create scripts. Independent software vendors provide WSH support for other popular scripting languages. You can use Windows Script Host to run .vbs and .js scripts directly on the Windows desktop or command console, without having to embed the scripts in an HTML document. MS-DOS-type batch files (with .bat and .cmd extensions) also use WSH.

Windows XP Professional supports the following five scripts:

- Group Policy logon scripts
- Group Policy logoff scripts
- Group Policy startup scripts
- Group Policy shutdown scripts
-

Logon scripts set on the properties sheets for user accounts

Note Although Group Policy–based scripts are similar to logon scripts set on the user object, they often require multibranching logic to target a specific group of users. Using Group Policy, you can target the scripts by using OUs and security group filtering. For this reason, the Windows XP Professional scripting options are a more efficient choice.

Using the **Scripts** folder located under **Computer Configuration\Administrative Templates\ System** and **User Configuration\Configuration\Administrative Templates\System** in the Group Policy snap-in, you can specify when and how startup and shutdown scripts and logon and logoff scripts are run. See Table 5-6 later in this chapter for a partial list of script-related settings.

Folder Redirection
Use Folder Redirection to redirect certain Windows XP Professional folders from their default location in the user profile to an alternate location on an Active Directory network where you can centrally manage them and keep them secure. The Windows XP Professional folders that can be redirected include My Documents (and its subfolders My Pictures, My Music, and My Videos), Application Data, Desktop, and the Start menu.

Internet Explorer Maintenance
Using Internet Explorer Maintenance, you can administer and customize Internet Explorer on Windows XP Professional–based client computers by using Group Policy instead of using the Internet Explorer Administration Kit (IEAK). You can also export these settings to clients running earlier versions of Windows. For more information about managing Internet Explorer, see the Microsoft Internet Explorer Administration Kit (IEAK) link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources. For information about individual Internet Explorer Group Policy settings, see Group Policy Help or the Extended view in the Group Policy snap-in.

Refreshing Group Policy from the Command Line

A new command-line tool, GPUdate.exe, replaces the Secedit.exe tool to give administrators better control and flexibility in refreshing policy. Normally, Group Policy refreshes every 90 minutes for the computer and user. However, after you modify a GPO, you can use GPUpdate to refresh the GPO so that it takes effect immediately. GPUpdate replaces the Windows 2000 tool Secedit.exe and provides increased control and flexibility. The command-line parameters for this tool are described in Table 5-5.

Table 5-5 Command-Line Parameters for GPUdate.exe

Command-Line Parameter	Behavior
/target: {computer|user}	Specifies that only Computer or User policy settings are refreshed. By default, both Computer and User policy settings are refreshed.
/force	Reapplies all policy settings. By default, only policy settings that have changed are applied.
/wait:value	Sets the number of seconds to wait for policy processing to finish. The default is 600 seconds. The value "0" means not to wait. The value "-1" means to wait indefinitely. When the time limit is exceeded, the command prompt returns but policy processing continues.
/logoff	Causes a logoff after the Group Policy settings have

	been refreshed. This is required for Group Policy client-side extensions that do not process policy on a background refresh cycle but that do process policy when the user logs on. Examples include user-targeted Software Installation and Folder Redirection. This option has no effect if there are no extensions called that require the user to log off.
/boot	Causes a reboot after the Group Policy settings are refreshed. This is required for Group Policy client-side extensions that do not process policy on a background refresh cycle but that do process policy when the computer starts up, such as computer-targeted Software Installation. This option has no effect if there are no extensions called that require a reboot.
/sync	Causes the next foreground policy application to be processed synchronously. Foreground policy applications occur at computer boot and user logon. You can specify this for the user, computer, or both using the /target parameter. The /force and /wait parameters are ignored if specified.

Top of page

Managing Desktops Without Active Directory

On a network not running the Active Directory directory service, you can implement the following IntelliMirror and Group Policy features to manage Windows XP Professional and Windows 2000 desktops:

- Roaming User Profiles and logon scripts (Microsoft Windows NT version 4.0 domains)
- Folder Redirection (limited functionality only)
- Internet Explorer Maintenance
- System Policy
- Local Group Policy object

Roaming User Profiles and Logon Scripts

In a Windows NT 4.0 domain, both roaming user profiles and logon scripts are configured on the properties sheets for user accounts.

My Documents Redirection

On a Windows NT 4.0 Server network, you can redirect My Documents and its subfolders, Application Data, Desktop, and the Start menu to a local or network location by using the following methods:

- You can use System Policy to redirect these folders. This will provide only limited functionality compared with true Folder Redirection because you cannot actually move folder contents or set ACLs.
- Users can manually redirect the My Documents folder by changing the target folder location in the **My Documents** Properties page.
- Manipulation of registry settings.

Note that you cannot configure Folder Redirection by using an LGPO.

Internet Explorer Maintenance

Instead of using Group Policy to control Internet Explorer settings, you can use the Internet Explorer Administration Kit (IEAK) to apply settings to Internet Explorer clients by using auto-configuration packages. To download the IEAK, see the Microsoft Internet Explorer Administration Kit (IEAK) link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

System Policy

Like Active Directory–based Group Policy objects, System Policy can define a specific user's settings or the settings for a group of users. The resulting policy file contains the registry information for all users, groups, and computers that will use the policy file. Separate policy files for each user, group, or computer are not necessary.

Group Policy includes the functionality from Windows NT 4.0 System Policy. It also provides additional policy settings for scripts, Software Installation and Maintenance, security settings, Internet Explorer maintenance, and folder redirection. Table 5-6 provides an overall comparison of Group Policy and Windows NT 4.0 System Policy.

Table 5-6 Comparison of Group Policy and System Policy

Comparison	Group Policy	Windows NT 4.0 System Policy
Tool used:	Microsoft Management Console (MMC) Group Policy snap-in or Group Policy Management Console (GPMC).	System Policy Editor (Poledit.exe).
Number of settings:	More than 150 security-related settings and almost 1400 registry-based settings.	72 settings.
Applied to:	Users or computers in a specified Active Directory container (site, domain, or OU) or local computers and users.	Domains or local computers and users.
Security:	Secure.	Not secure.
Extensible by:	Using Microsoft Management Console (MMC) or .adm files.	Using .adm files.
Persistence:	Does not leave settings in the users' profiles when the effective policy is changed.	Persistent in users' profiles until the specified policy is reversed or until you edit the registry.
Defined by:	User or computer membership in security groups.	User membership in security groups.
Primary uses:	Implementing registry-based settings to control the desktop and user. Configuring many types of security settings. Applying logon, logoff, startup, and shutdown scripts.	Implementing registry-based settings that govern the behavior of applications and operating system components such as the Start Menu.

	Implementing IntelliMirror Software Installation and Maintenance. Implementing IntelliMirror data and user settings management. Optimizing and maintaining Internet Explorer.	

Warning System Policy settings applied to computers that have been upgraded to Windows XP Professional are persistent in the registry. Applying Group Policy to a computer with persistent registry-based System Policy settings might have unpredictable results. It is recommended that you remove these settings from computers before applying GPOs.

Windows XP Professional–based clients in an Active Directory domain can process Group Policy but cannot process Windows NT 4.0 System Policy. Windows NT 4.0 policies are persistent in user profiles. This means that after a registry-based setting is applied using Windows NT 4.0 System Policy, the setting persists until the specified policy is reversed or you edit the registry to remove the corresponding entry. The effect of persistent registry-based settings can cause conflicts when a user’s group membership changes. If the Windows XP Professional computer account object or user account object that you manage exists in a Windows NT 4.0 domain, you can still use certain System Policy tools to manage them.

Note You can use System Policy to deliver any of the registry-based policy settings (Administrative Templates) that are available in Windows XP Professional. The procedures described in the following subsections also work for providing System Policy from any Server Message Block (SMB)–enabled share or even from a local share.

To create a policy that is automatically downloaded from validating domain controllers, you must create a .pol file by using the System Policy Editor:

- For Windows NT 4.0 and later, the .pol file is named Ntconfig.pol and is created using the System Policy Editor for the specific operating system.
- For Windows 95, Windows 98, and Microsoft Windows Millennium Edition (Windows Me), the .pol file is named Config.pol and must be created by using the System Policy Editor for that operating system.

As system administrator, you can choose an alternate name for the .pol file and can direct the computer to update the policy from a path other than the Netlogon share. You can do this by using System Policy. The update path can even be a local path, so that each computer has its own policy file. However, you must make this change manually on each desktop. For more information about specifying a path to the policy file, see “Specifying a path to the policy file” later in this chapter.

Administrative templates

The System Policy Editor tool uses files called *administrative templates* (.adm files) to determine which registry settings you can modify and which settings display in the System Policy Editor.

In Windows XP Professional and Windows 2000, the Administrative Templates item in the Group Policy snap-in uses administrative templates (.adm files) to specify the registry settings that can be modified through the Group Policy snap-in. This includes Group Policy for the Windows XP Professional operating system and its components as well as for applications.

Policy settings are written to the following locations in the registry:

- HKEY_CURRENT_USER\Software\Policies (preferred location)
- HKEY_LOCAL_MACHINE\Software\Policies (preferred location)
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

Caution Do not edit the registry unless you have no alternative. The Registry Editor bypasses standard safeguards, allowing settings that can damage your system or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference in the *Microsoft Windows 2000 Server Resource Kit* at http://www.microsoft.com/windows/reskits/.
To configure or customize Group Policy, use the Group Policy snap-in whenever possible.

A client running Windows XP Professional or Windows 2000 Professional processes System Policy if the user or computer account, or both, are in a Windows NT 4.0 domain. The client looks for the Ntconfig.pol file used by Windows NT 4.0–style System Policy. By default, it looks for this file in the Netlogon share of the authenticating Windows NT 4.0 domain controller.

Warning It is possible for a computer account object to exist in a Windows NT 4.0 domain and a user account object for a user of that computer to exist in an Active Directory domain, or vice versa. However, operating in such a mixed environment makes the users and computers difficult to manage and might cause unpredictable behavior. For optimal central management, it is recommended that you move from a mixed environment to a pure Active Directory environment.

Setting registry-based policy in a Windows NT 4.0 domain

A Windows XP Professional–based client processes System Policy if either the user or computer account exists in a Windows NT 4.0 domain. When a user logs on to a Windows XP Professional–based client in a Windows NT 4.0 domain and the client is running in the default Automatic mode, it checks the Netlogon share on the validating domain controller for the Ntconfig.pol file. If the client finds the file, it downloads it, parses it for user, group, and computer policy data, and then applies the appropriate settings. If the client does not locate the policy file on its validating domain controller, it does not check elsewhere. It is therefore critically important that the Ntconfig.pol file is replicated among the domain controllers performing authentication.

Setting registry-based policy in a workgroup environment

In the absence of a Windows NT 4.0 domain, you can configure the client to look for the Ntconfig.pol file in a specific location on the local computer or on any SMB share location. For more information about specifying a path to the policy file, see “Specifying a path to the policy file” later in this chapter.

Creating Ntconfig.pol files based on Windows XP Professional .adm files

You can create Ntconfig.pol files based on the Windows XP Professional .adm files and apply these settings to Windows XP Professional–based clients. To do this, you need the Windows NT 4.0 System Policy Editor tool, Poledit.exe, which is installed with Windows 2000 Server and Advanced Server. You can install Poledit.exe on Windows XP Professional–based computers by installing the Administrative Tools package that is included on the Windows 2000 Server and Microsoft Windows 2000 Advanced Server operating system CDs.

To install Administrative Tools on a Windows XP Professional–based computer, open the **i386** folder on the applicable Windows 2000 Server disc, and then double-click the **Adminpak.msi** file. Follow the instructions that appear in the Administrative Tools setup wizard.

When you install the Administrative Tools package, Poledit.exe and its supporting .adm files (Winnt.adm, Windows.adm, and Common.adm) are installed into the root \System directory and the \Inf directory, as in Windows NT 4.0. Poledit.exe is not added to the Start menu, but it is accessible from the command line.

Use the following procedure to create an Ntconfig.pol file.

Note The System Policy Editor from Windows NT 4.0 or earlier cannot read the Unicode-formatted .adm files shipped in Windows 2000 or later. You must use the version of System Policy Editor that ships in Windows 2000 or later, which supports Unicode. Alternatively, if you resave the .adm files as .txt files without Unicode encoding, you can use an older version of Poledit.exe.

To create an Ntconfig.pol file

1. Using a text editor such as Notepad, remove all **#if version** and **#endif** statements from the following .adm files: System.adm, Inetres.adm, and Conf.adm, and then save the files. This prevents inadvertent loading of these files by Poledit.exe.

   For example, in the Inetres.adm file, remove these lines:

   ```
   #if version <= 2
   #endif
   ```

2. Open Poledit.exe.

3. In the **System Policy Editor** window, on the **Options** menu, click **Policy Template**.

4. In the **Policy Template Options** dialog box, click **Add**, select one of the .adm files that you modified in step 1 above, and then click **OK**.

5. Specify the appropriate policy settings, as documented in System Policy Editor Help.

6. Save the file as Ntconfig.pol to the NETLOGON share of the Windows NT 4.0 domain controller.

Specifying a path to the policy file

You can change the default behavior so that a Windows XP Professional–based client looks for the policy file in a different location than the Netlogon share. The **UpdateMode** registry entry forces the computer to retrieve the policy file from a specific location (expressed as a UNC path), regardless of which user logs on.

You can set **UpdateMode** by using the System Policy Editor and the System.adm file.

To retrieve the policy file from a specific location

1. Open Poledit.exe.

2. Click **Options**, click **Policy Template**, and then in the **Policy Template Options** dialog box, make sure that System.adm is listed in the Current Policy Template(s) list box. If it is not listed, click **Add** to add this file.

3. To open the Default Computer policy, on the **File** menu, click **New Policy**, and then double-click **Default Computer** from the **Policies for**

list.

– or –

To open the Local Computer policy, on the **File** menu, click **Open Registry**, and then double-click **Local Computer**.

4. In the **Properties** dialog box, expand **Network**, and then expand **System policies update** to display the Remote update option.
5. Select the **Remote update** box.
6. In the **Update mode** drop-down menu, select **Manual (use specific path)**.
7. In the **Path for manual update** text box, type the UNC path and file name for the policy file, and then click **OK** to save your changes.

The first time the Windows XP Professional–based client is modified locally by using the System Policy Editor or receives a default System Policy file from the NETLOGON share of a domain controller, this location is written to the registry. Thereafter, the Windows XP Professional–based client does *not* look at a domain controller again to find a policy file, and all policy updates use the location you specified manually. Note that this change is permanent until you edit the policy file to reset the option to **Automatic**.

Local Group Policy Object

In addition to setting System Policy, you can set settings in the local Group Policy object (LGPO) for any computer, whether or not it participates in an Active Directory domain. Although System Policy scales more easily to a large number of clients, the LGPO can be useful if you need to apply certain settings to only a small number of Windows XP Professional–based clients in a Windows NT 4.0 or other domain.

The LGPO is located at \systemroot\System32\GroupPolicy. Not all Group Policy extensions are available for the local GPO. Each Group Policy extension snap-in queries the Group Policy engine to get the GPO type, and then determines whether the GPO is to be displayed. To set the LGPO, use the Group Policy snap-in focused on the local computer.

Table 5-7 shows which Group Policy snap-in extensions open when the Group Policy snap-in is focused on an LGPO.

Table 5-7 Local Group Policy Object Extensions

Group Policy Snap-In Extension	Available in LGPO
Software Installation	No
Scripts	Yes
Security Settings	Yes
Administrative Templates	Yes
Folder Redirection	No
Internet Explorer Maintenance	Yes
RIS	No

You can access the Group Policy snap-in by using the following procedure.

To start the Group Policy snap-in on a Windows XP Professional–based client

1. In the MMC window, on the **File** menu, click **Add/Remove Snap-in**.

2. On the **Standalone** tab, click **Add**.

3. In the **Add Standalone Snap-in** dialog box, click **Group Policy**, and then click **Add**. The **Group Policy Wizard** appears.

4. Select **Local Computer** to edit the local GPO, or click **Browse** to select another computer.

5. Click **Finish**.

6. In the **Add Standalone Snap-in** dialog box, click **Close**.

7. In the **Add/Remove Snap-in** dialog box, click **OK**.

   The Group Policy snap-in opens with focus on the specified GPO. If you select **Local Computer**, you see Local Computer Policy. Expand the tree to see **Computer Configuration** and **User Configuration**.

Alternatively, to quickly access the local Group Policy object on the local computer, type **gpedit.msc** in the **Run** dialog box.

Note The Security Settings extension of the Group Policy snap-in does not support remote management for the local Group Policy object in Windows XP Professional.

Managing Desktops in UNIX and Novell Environments

You can use LGPOs and System Policy to manage Windows XP Professional Desktops in Novell and UNIX environments. For example, NTConfig.pol can exist on any network server. You can perform typical desktop-management tasks that are based on industry-standard protocols, such as Telnet and Simple Network Management Protocol (SNMP), a standards-based TCP/IP network management protocol that is implemented in many environments. For more information about using LGPOs and System Policy, see "Managing Desktops Without Active Directory" earlier in this chapter.

Standards-Based Management

Windows XP Professional provides full support for SNMP, allowing you to easily manage systems that run Windows XP Professional by using a UNIX-based SNMP management suite available from independent software vendors.

Telnet Client and Server

You can use Telnet to remotely log on to and execute commands on a Windows XP Professional–based or UNIX-based system. The Telnet client included with Windows XP Professional is character–based and console-based and is enhanced for advanced remote management capabilities.

The Windows XP Professional–based Telnet client also provides NTLM authentication support. With this feature, a Windows XP Professional Telnet client can log on to a Telnet server that uses NTLM authentication, such as the Telnet Server included with Windows 2000 Server and Windows Server 2003.

Novell NetWare IPX Network

Internetwork Packet Exchange (IPX) is the native NetWare protocol used on legacy Novell networks. You can integrate Network Connections clients into a NetWare IPX network, with the exception of clients running Microsoft Windows XP Professional x64 Edition.

The client must run a NetWare redirector to see a Novell NetWare network. This redirector is called Client Service for NetWare (CSNW).

A remote access server is also an IPX router and Service Advertising Protocol (SAP) agent. Once configured, remote access servers enable file and print services and the use of Windows Sockets programs over IPX on the NetWare network for Network Connections clients. Remote access servers and their Network Connections clients use the Point-to-Point (PPP) IPX Control Protocol (IPXCP), as defined in RFC 1552, "The PPP Internetwork Packet Exchange Control Protocol (IPXCP)," to configure the remote access line for IPX.

Network Connections clients are always provided an IPX address by the remote access server. The IPX network number is either generated automatically by the remote access server, or a static pool of network numbers is given to the remote access server for assignment to Network Connections.

For automatically generated IPX network numbers, the remote access server uses the NetWare Router Information Protocol (RIP) to determine an IPX network number that is not in use in the IPX network. The remote access server assigns that number to the connection.

Configure a connection by selecting **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol** on the **General** tab of **Local Area Connection Properties**.

Novell ZENworks

To use Novell ZENworks, you must register Windows XP Professional with ZENworks. A workstation record can then be imported into the Novell Directory Services (NDS) database of a Novell NetWare network. The workstation is registered by running Wsreg32.exe either from the command line or from a logon script. The following is an example of the logon script code that detects Windows XP Professional and runs the correct registry program:

```
IF " %PLATFORM" =" WINDOWS_NT" THEN BEGIN
#F:\PUBLIC\WSREG32.EXE
END
```

After the workstation is registered, you can import it into NDS by using Nnwadmn32.exe.

You can administer Windows XP Professional–based clients by using the standard ZENworks tools.

Top of page

Creating and Managing Standard Desktop Configurations

IntelliMirror and Group Policy allow you to manage desktops with great efficiency. To take full advantage of these benefits, it is recommended that you define and set up default user configurations.

A standard configuration must be carefully adapted to the target users' applications, tasks, and locations. It can also increase productivity by preventing users from making system changes that could cause downtime. Because standard configurations are easier to troubleshoot or replace, they can also reduce support costs.

IntelliMirror and Group Policy are designed for use in environments where administrators need to centralize tasks such as the following:

- Creating managed desktops
- Managing mobile users

- Managing new users
- Managing multi-user desktops
- Replacing computers

Creating Managed Desktops

The managed desktop contains settings that can lower the total cost of ownership (TCO) of a desktop for any level of user. This configuration can reduce help desk costs and user downtime by providing users with just the applications and tools they need to perform their jobs. The user is permitted to install approved applications and make extensive customizations of applications and the desktop environment. At the same time, the managed desktop configuration can keep users from making potentially harmful changes to configuration settings, such as adding or disabling hardware devices, or changing system or user environment settings, such as the location of the **My Documents** folder, and can restrict access to such features as the MMC administration snap-ins and some hardware-configuration items in **Control Panel**. The user for this configuration does not usually require access to **Network Connections**.

Table 5-8 shows the desktop management features used to create a typical managed desktop configuration.

Table 5-8 Features of a Managed Desktop Configuration

Feature	Specifics	Explanation
Multiple Users	Per-user logon accounts	Users might share this computer during different shifts. Each user has a unique logon account.
Roaming User Profiles	Yes	Makes user settings available from any computer and enables administrators to easily replace computers without losing user configuration.
Folder Redirection	My Documents folder	User data is saved on server shares and Group Policy prevents users from storing data locally.
Ability for User to Customize	Most	Allows users to personalize their work environment while preventing changes to critical system settings.
Assigned Applications	Multiple	Core applications are automatically installed before the user logs on.
Published Applications	Multiple	All required applications are available for users to install locally.
Group Policy Settings	Yes	Group Policy settings are used to create the managed environment.

Managing Mobile Users

Many organizations have mobile users—traveling employees who often use a portable computer. Mobile users have unique needs because, although these users usually log on to the same computer, they sometimes connect through a high-speed line and sometimes through a low-speed (or dialup) line, and some mobile users never have a fast connection. Such users fall into two main categories:

- Users who spend the majority of time away from the office or have no fixed office. Typically, these users connect by using slow links, although they might have occasional LAN access to their logon server, data servers, and application-delivery servers.
- Users who spend most of their time in an office but occasionally work at home or in another location. The majority of their network access is at LAN speed, but they occasionally use the Routing and Remote Access service or remote network links.

Despite the apparent differences between these two types of users, you can generally accommodate them with a single configuration. However, you might want to consider creating a slightly different GPO for users who spend the majority of their time out of the office.

Mobile users are often expected to provide much of their own computer support because on-site support is not available. For this reason, you might want to grant them more privileges than equivalent users on a desktop computer (for example, so they can install printers).

You might, however, decide to restrict mobile users from making system changes that might damage or disable their systems. For example, you might restrict mobile users from altering certain Internet Explorer settings or adding unapproved hardware devices. Although these users might need access to some of the MMC administration snap-ins, you can make available only a restricted set.

Mobile users expect transparent access to the most critical parts of their data and settings, regardless of whether the portable computer is connected to the network. They roam to desktop computers while their portable computer is in use, for example, to read mail while they are in a remote office. Finally, mobile users frequently disconnect their portable computer from the network without logging off and shutting down. This is more likely to happen with the hibernate and standby features of Windows XP Professional.

IntelliMirror provides several tools that greatly simplify managing mobile users. User data and settings management tools allow users to work on files offline and automatically update network versions of those files when they later reconnect to the network. The Offline Files feature allows users to work on network files when they are not actually connected to the network. Synchronization Manager coordinates synchronization of any changes between the offline version of a file and the network version.

Note If users are likely to disconnect from the network without logging off, it is recommended that you set Offline Files to periodically synchronize in the background. If Offline Files is set to synchronize only when users log off, users' files might not be up–to-date. You might also want to educate users to manually synchronize their data before disconnecting from the network to ensure all files are up–to-date.

Synchronization Manager also helps manage multi-user network files. If multiple users modify the same network file, Synchronization Manager notifies the users about the conflict and offers several resolution methods. The users can save the network version, their local version, or both versions. If both are to be kept, the user is asked for a new file name to store one of the versions so that uniqueness is maintained.

Software installation for the mobile user requires some additional planning. You can make sure that all important software components, defined by you or the user, are completely installed initially. This allows the user access to necessary software even when he or she is not connected to the network. That means that prior to these users leaving the office, you must ensure that all relevant features within the application are installed locally and are not just advertised. For example, make sure the spelling checker for Microsoft Office is locally installed so that the user does not trigger on-demand installation of this feature while offline.

It is not recommended that you publish software for mobile users who connect over slow links. Additionally, when mobile users connect over a slow link, user-assigned software effectively behaves the same as if you published it for these users. If you set the Group Policy slow-link detection setting to the default in the user interface, the software will not install on demand. However, you can define the connection speed that is considered to be a slow link in the Group Policy setting for slow-link detection.

Note It is recommended you treat any link that is slower than local area network (LAN) speed as a slow link, although a broadband Internet connection such as DSL or a wireless access point is usually sufficient for most software installation scenarios.

If you determine that it is appropriate for mobile users to download software from a remote location and they experience difficulty staying connected when downloading the software, you can verify that the connection speed and Group Policy settings are set appropriately in the **Group Policy slow link detection** setting in **Computer Configuration/Administrative Templates/System/Group Policy** or **User Configuration/Administrative Templates/System/Group Policy**.

Typically, a mobile user has a single portable computer and does not roam between portable computers (unless the computer is replaced). However, roaming user profiles are useful to give some measure of protection against mobile computer failure or loss and to allow roaming to desktop computers when the mobile user is often connected to a fast network. When the mobile user is *not* often connected to a fast network, it is best not to use roaming user profiles.

Data accessed by the mobile user often falls into one or more of the following categories:

- Data that resides on a network server and which users want to access while not connected to the network. Users typically own this data (for example, their home directory), but shared data can also be stored on the local computer.
- Data that resides only on the network server (either not needed offline or volatile shared data that is inappropriate for storing offline).
- Data that resides only on the portable computer local disk. Examples are policy manuals or other read-only items or large document sets that are needed offline by the user but the performance overhead of synchronizing precludes storing them on a file server. (In this case, a suitable backup mechanism is definitely needed.) Other examples might be large database files or other data items that have their own synchronization mechanism, such as the offline storage feature in Microsoft Outlook.

Table 5-9 summarizes desktop management features you can use to create a mobile user configuration.

Table 5-9 Features of a Mobile User Configuration

Feature	Specifics	Explanation
Number of Users	One	Each user has a local logon account.

Roaming User Profiles	Yes, depending on connection type and frequency	Provides centralized storage of user state to help administrators replace computers without losing user configuration. Also facilitates roaming.
Folder Redirection	My Documents folder	Allows users to access centrally stored data and documents from anywhere. Redirected folders are automatically made available offline to provide access when users are not connected to the network.
Ability for User to Customize	Within certain guidelines	Allows users to personalize their work environment while preventing changes to critical system settings.
Assigned Applications	Multiple	Core applications are installed on all laptops.
Published Applications	Multiple	Optional applications are available for users to install locally.
Group Policy Settings	Yes	Policy settings are used to create the managed environment.

For more information about configuring portable computers, see Chapter 7, “Supporting Mobile Users.”

Managing New Users

IntelliMirror, Group Policy, Windows Installer, and RIS greatly streamline adding new users and their computers to your network. You might use these technologies as follows to add a new managed user.

A new user logs on to a new computer and finds shortcuts to documents on the desktop. These shortcuts link to common files, data, and URLs, such as the employee handbook, the company intranet, and appropriate departmental guidelines and procedures. Desktop options, application configurations, Internet settings, and so on are configured to the corporate standard. As the user customizes his or her environment (within boundaries defined by the administrator), these changes are added to the initial environment. For example, the user might change the screen resolution for better visibility and might add shortcuts to the desktop.

In this situation, a default domain profile and Group Policy are used to configure the new user’s environment based on job requirements. The advantage of using a default domain profile is that all new users start from a common, administrator-defined configuration in an existing domain structure. You create a customized domain profile that applies to all new domain users the first time they log on, and they receive the customized settings from this profile. Then, as the user personalizes desktop settings and items, these settings are saved in the user’s profile that is stored locally, or in the case of a roaming user profile, in a predetermined location on the network. By implementing a default domain profile in conjunction with Roaming User Profiles, the administrator provides users with the necessary business information as a starting point and also allows them to access their settings whenever and wherever needed. Finally, the administrator uses Folder Redirection to redirect the user’s My Documents folder to a network location so that the user’s documents are safely stored on a network server and can be backed up regularly.

The administrator uses the Software Installation and Maintenance extension of

Group Policy to assign Microsoft Word to a user or a specific group of users. The new user logs on for the first time and sees that the software required to do his job is listed in the **Start** menu. When the user selects Microsoft Word from the **Start** menu or double-clicks on a Word document, Windows Installer checks to see whether the application is installed on the local computer. If it is not, Windows Installer downloads and installs the necessary files for Word to run and sets up the necessary local user and computer settings for an on-demand installation.

Managing Multi-User Desktops

A multi-user desktop is managed, but it allows users to configure parts of their own desktops. The multi-user desktop is ideal for public shared access computers, such as those in a library, university laboratory, or public computing center. The multi-user desktop experiences high traffic and must be reliable and unbreakable while being flexible enough to allow some customization.

Users can change their desktop wallpaper and color scheme. Because many people use the computers and security must be maintained, they cannot control or configure hardware or connection settings. The computers often require certain tools, such as word processing software, spreadsheet software, or a development studio. Students might need access to customized applications for instructional purposes, and they might need to be able to install applications that the network administrator has published.

With the multi-user desktop configuration, users can:

- Modify Internet Explorer and the desktop.
- Run assigned or published applications.
- Configure some Control Panel options.

However, users cannot:

- Use the Run command in the **Start** menu or at a command prompt.
- Add, remove, or modify hardware devices.

In the multi-user environment, turnover is high and a user is unlikely to return to the same computer. Therefore, local copies of roaming user profiles that are cached on the computer are removed after the user logs off if the roaming user profile settings were successfully synchronized back to the server. Roaming user profiles use the My Documents and Application Data folders that are redirected to a network folder. However, users can log on even if their network profile is not available. In this case, the user receives a new profile based on the default profile.

The multi-user computer is assigned a set of core applications that is available to all users who log on to that particular computer. In addition, a wide variety of applications are available by publishing for user or assigning to users. Due to security risks, users cannot install from a disk, CD-ROM, or Internet location. To conserve disk space on the workstation, most applications must be configured to run from a network server. **Start** menu shortcuts and registry-based settings are configured when the user selects an application to install, but most of the application’s files remain on the server. The shares that store the applications can be configured for automatic caching for programs so that application files are cached at the workstation on first use.

Table 5-10 shows the desktop management features used to create a multi-user computing environment.

Table 5-10 Features of a Multi-User Desktop Configuration

Feature	Specifics	Explanation
Multiple Users	Per-user logon accounts	Users share this computer during different shifts. Each user has a unique logon account.
Roaming User Profiles	Yes	Makes user settings available from any computer, and enables administrators to easily replace computers without losing their configuration. When the user logs off, the local cached version of the profile is removed to preserve disk space.
Folder Redirection	My Documents and Application Data	User data is saved on server shares, and Group Policy prevents users from storing data locally.
Ability for User to Customize	Some	Most of the system is locked down, but some personal settings are available.
Assigned Applications	Multiple	Core applications that are common to all users are assigned to the computer. Other applications are available for on-demand install by means of user assignment.
Published Applications	Multiple	Applications are available for users to install from Add or Remove Programs in Control Panel.
Group Policy Settings	Yes	Group Policy settings are used to create the managed environment.

Replacing Computers

When a user receives a new or different computer, it can cause a time-consuming interruption in productivity. It is extremely important that such users regain productivity in the shortest possible time and with a minimum of support. This can be accomplished by storing user data and settings independently of any specific computer. By using the Group Policy features Roaming User Profiles and Folder Redirection, you can assure that the user’s data, settings, and applications are available wherever the user logs on to the network.

To further simplify setting up a new managed computer on your network, use Remote Installation Services (RIS) to create standardized operating system configurations. RIS allows you to create a customized image of a Windows XP Professional or Windows 2000 Professional desktop from a source computer. Then you can save that desktop image to the RIS server. The image can include the operating system alone or a preconfigured desktop image, including the operating system and a standard, locally installed desktop application. You can use that preconfigured image to set up multiple desktops, saving valuable time. Create as many standard desktop images as you need to meet the needs of all types of users in your organization. For more information about using RIS, see Chapter 2, “Automating and Customizing Installations.”

These technologies might work together as outlined in the following paragraphs.

A user’s computer suddenly undergoes a complete hardware failure. The user calls the internal support line. Shortly, a new computer, loaded only with the Windows XP Professional operating system, arrives. Without waiting for technical assistance, the user plugs in the new computer, connects it to the network, starts it, and can immediately log on.

Because roaming user profiles are enabled, the user finds that the desktop takes on the same configuration as the computer it replaced: the same color scheme, screen saver, and all the application icons, shortcuts, and favorites are present. Because folder redirection and software installation are enabled, the user can seamlessly access data files on the server by using the necessary productivity applications once they automatically install.

⇡ Top of page

Additional Resources

These resources contain additional information related to this chapter.

Related Information

- The *Designing a Managed Environment* book in the Microsoft Windows Server 2003 Deployment Kit, for information about deploying Group Policy and security policies
- The Microsoft Windows Security Resource Kit, for information about implementing security for Windows-based client computers and servers
- The *Deployment Planning Guide* of the Windows 2000 Server Resource Kit, for information about deploying Group Policy and Active Directory
- The *Distributed Systems Guide* of the Microsoft Windows 2000 Server Resource Kit, for more information about implementing and troubleshooting IntelliMirror technologies
- Chapter 2, “Automating and Customizing Installations,” for more information about using Remote Installation Services (RIS)
- The Change and Configuration Management Guide link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources, for information about deploying IntelliMirror
- The Microsoft Internet Explorer Administration Kit (IEAK) at http://www.microsoft.com/technet/prodtechnol/ie/ieak/, for detailed information about managing Internet Explorer
- The “Group Policy Settings Reference for Windows XP Professional Service Pack 2” spreadsheet, which is available from the Microsoft Download Center (http://www.microsoft.com/downloads)
- The “Managing Windows XP Service Pack 2 Features Using Group Policy” document, which can be found at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpsp2/mngxpsp2.mspx

Related Help Topics

- “Tools for Troubleshooting” in Windows XP Professional Help and Support Center, for information about troubleshooting tools use and syntax
- Group Policy Help, for information about Group Policy

- “IntelliMirror” in Windows XP Professional Help and Support Center, for information about user data management, software installation and maintenance, user settings management, and Remote Installation Services (RIS)

⇡ Top of page ◀ 5 of 29 ▶

Manage Your Profile