Windows XP Professional

User Data and Settings Management

By Craig Marl

Microsoft Corporation

Published: March 2002

Abstract

This white paper explains the IntelliMirror® user data and settings management features in Microsoft® Windows® Server 2003. These key components of change and configuration management can help administrators reduce total cost of ownership (TCO).

Acknowledgements

Craig Marl, program manager, Microsoft Corporation.

John Kaiser, technical editor, Microsoft Corporation.

Introduction

User data includes the documents, images, spreadsheets, presentations and e-mail messages on a user's computer. User settings include application configurations, preferences, window sizes, toolbar settings and so forth on a user's computer.

With Microsoft® IntelliMirror® management technologies, administrators can manage user data and settings in ways that reduce the total cost of ownership (TCO) for the computing systems.

By using IntelliMirror on both the server and client, administrators can protect and manage user data and settings. Non-recoverable data from local workstations can be copied to servers, where it can be easily backed up and centrally managed. Personalized data, applications, and settings can follow each user to different computers throughout the network. Administrators can easily replace faulty computers and restore all user data and settings on a new computer.

When fully deployed, IntelliMirror uses the Active Directory® service and Group Policy for policy-based management of user desktops. A Windows 2000, Windows XP Professional or Windows Server 2003 computer can be automatically configured to meet specific requirements of a user's business roles, group memberships, and location. Group Policy and the Active Directory are not necessary for every IntelliMirror feature. Some of the features can be set on the local level or through local polices. An organization can tailor use of IntelliMirror to its needs.

This paper discusses two of the key components that provide user data and settings management in IntelliMirror—User Profiles and Folder Redirection. It also provides an architectural overview of these features, and presents sample scenarios showing how IntelliMirror is used throughout a computer's lifecycle.

User Profiles Overview

A user profile describes the desktop computing configuration for a specific user, including the user's environment and preference settings.

A profile is created the first time that a user logs on to a computer running Windows Server 2003, Windows XP, Windows 2000, or Windows NT® Workstation. A user profile is a group of settings and files that defines the environment that the system loads when a user logs on. It includes all the user-specific configuration settings, such as program items, screen colors, network connections, printer connections, mouse settings, and window size and position. Profiles are not user policies and the user has a profile even if you don't use Group Policy.

A user's data can be stored on the local hard disk drive, or IntelliMirror can be set so that the data roams with the user wherever he or she logs on. User data can include shortcuts to executable files, personal files, and user settings, such as a custom dictionary.

Depending on how you manage your network, you or a user can define the desktop settings.

The following user profiles are available in Windows Server 2003, Windows XP Professional, and Windows 2000 Professional:

- **Local User Profile.** Created the first time that a user logs on to a computer, the local user profile is stored on a computer's local hard disk. Any changes made to the local user profile are specific to the computer on which the changes are made.
- **Roaming User Profile.** A copy of the local profile is copied to, and stored on a server share. This profile is downloaded every time that a user logs on to any computer on the network, and any changes made to a roaming user profile are synchronized with the server copy upon logoff.
- **Mandatory User Profile.** A type of profile that administrators can use to specify particular settings for users. Only system administrators can make changes to mandatory user profiles. Changes made by the user to desktop settings are lost when the user logs off.

- **Temporary User Profile.** A temporary profile is issued any time that an error condition prevents the users profile from being loaded. Temporary profiles are deleted at the end of each session - changes made by the user to their desktop settings and files are lost when the user logs off.

Note If you need to provide managed desktop configurations for groups of users or computers, consider using Group Policy instead of mandatory profiles.

Advantages of User Profiles

A primary goal of user profiles is to separate each user's settings and data from that of other users and the local computer. Separating each user's state provides several advantages:

- It allows for "stateless" computers. An organization can configure computers to store all the key user settings and data away from the local computer. This allows for much easier computer replacement and backup. When a computer needs replacing, it can simply be swapped out—all of the user's state information is safely maintained separately on the network and is independent of a particular computer. When the user logs onto the new computer for the first time, the server copy of the user's state is copied to the new computer.
- It allows a user's system and desktop customizations to travel with the user from computer to computer, without requiring the user to reconfigure any settings. When a user logs on to any computer on the network that supports the roaming profile, the user's desktop appears—just as that user left it before logging off. With roaming user support, users can share computers, but each user has his or her personal desktop (both roaming and mandatory profiles support this functionality).

User Profile Structure

A user profile consists of:

- A registry hive. The registry is a database used to store computer- and user-specific settings. Portions of the registry can be saved as files, called hives. These hives can then be reloaded for use as necessary. User profiles take advantage of the hive feature to provide roaming profile functionality. The user profile registry hive is the NTuser.dat in file form, and is mapped to the HKEY_CURRENT_USER portion of the registry when the user logs on. The NTuser.dat hive maintains the user's environment preferences when the user is logged on. It stores those settings that maintain network connections, Control Panel configurations unique to the user (such as the desktop color and mouse), and application-specific settings. The majority of the settings stored in the registry are opaque to user profiles settings are owned and maintained by individual applications and OS components.
- A set of profile folders stored in the file system. User profile files are stored in the filesystem in the Documents and Settings directory, in a per user folder. The user profile folder is a container for applications and other OS components to populate with subfolders and per-user data, such as shortcut links, desktop icons, startup applications, documents, configuration files and so forth. Windows Explorer uses the user profile folders extensively for special folders such as the users desktop, start menu and my documents folder.

Together, these two components record user-configurable settings that can migrate from computer to computer.

The default location of user profiles was changed from the Windows NT 4.0 operating system to allow administrators to secure the operating system folders without adversely affecting user data. On a clean installed computer running Windows Server 2003, Windows XP or Windows 2000, profiles are stored in the %Systemdrive%\Documents and Settings folder. In contrast, on computers running Windows NT 4.0, profiles are stored inside the system directory, at %Systemroot%\profiles folder (typically WINNT\profiles).

Note if you upgrade a computer from Windows NT 4.0, the profile location remains %Systemroot%\profiles.

Table 1 below shows the location of user profiles for each of the possible installation scenarios:

Table 1 User Profile Locations

Operating system	Location of user profile
Windows Server 2003 clean installation (no previous operating system)	%SYSTEMDRIVE%\Documents and Settings; for example, C:\Documents and Settings
Windows Server 2003 upgrade of Windows 2000	SYSTEMDRIVE%\Documents and Settings; for example, C:\Documents and Settings
Windows Server 2003 upgrade of Windows NT 4.0	%SYSTEMROOT%\Profiles; for example, C:\WinNT\Profiles

Configuration Preferences Stored in the Registry Hive

The NTuser.dat file contains the following configuration settings:

- **Windows Explorer settings**. All user-definable settings for Windows Explorer, as well as persistent network connections.
- **Taskbar settings.**
- **Printer settings.** All network printer connections.
- **Control Panel.** All user-defined settings made in the Control Panel.
- **Accessories.** All user-specific application settings affecting the Windows environment, including: Calculator, Clock, Notepad, Paint, and HyperTerminal, among others.
- **Application Settings.** Many applications store some per user settings in the users' registry hive (HKEY_CURRENT_USER). An example of these types of settings would be Microsoft Word 2000's toolbar settings.

Configuration Preferences Stored in Profile Directories

Figure 1 below shows the structure of the user profile.

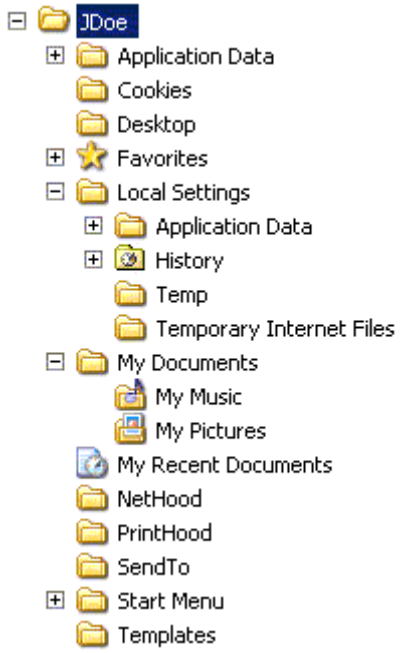

Figure 1 User Profile.

Each user's profile contains the following folders:

- *Application data**. Application-specific data, such as a custom dictionary for a word processing program. Application vendors decide what data to store in this directory.
- *Cookies*. Internet Explorer cookies.
- *Desktop.* Desktop items, including files and shortcuts.
- *Favorites.* Internet Explorer favorites
- *Local Settings**. Application settings and data that **do not roam** with the profile. Usually either machine specific, or too large to roam effectively.
  - *Application data*. Computer specific application data.
  - *History.* Internet Explorer history.
  - *Temp.* Temporary files.
  - *Temporary Internet Files.* Internet Explorer offline cache.
- *My Documents*. The new default location for any documents that the user creates. Applications should be written to save files here by default.
  - *My Pictures.* Default location for user's pictures.

- *My Music.* Default location for user's music.
- *NetHood**.* Shortcuts to Network Neighborhood items.
- *PrintHood**.* Shortcuts to printer folder items.
- *Recent*. Shortcuts to the most recently used documents.
- *SendTo*. Shortcuts to document storage locations and applications.
- *Start Menu*. Shortcuts to program items.
- *Templates**. Shortcuts to template items.

* These directories are hidden by default. To see these directories, change the View Options.

The Folder Redirection feature of IntelliMirror allows an administrator to redirect the location of certain folders in the user profile to a network location. When these redirected folders are accessed either by the operating system or by applications, the operating system automatically redirects to the location on a network share specified by the administrator. From a user perspective, this is similar to the roaming scenario because users have the same settings regardless of which computers they use. However unlike roaming, these settings actually remain on the network share. Folder redirection can be used with all types of user profiles: local, roaming, or mandatory.

Using Folder Redirection with local profiles can provide some of the benefits of roaming profiles (such as having a user's data available at any computer or maintaining data on the server) without the need to implement roaming profiles. Remember though, using Folder Redirection with a local profile would only result in the user's documents and files being available from all computers. To have settings and configurations move with the user, you would need to use roaming profiles.

Combining Folder Redirection with roaming profiles gives the benefit of roaming profiles, while minimizing network traffic caused by synchronization of the profile.

Folder redirection is accomplished using Group Policy. The use of Folder Redirection with roaming profiles is discussed later in this article.

Table 2 below lists the folders that roam with the profile by default and indicates whether they can be redirected using Group Policy.

Table 2 Folders that Roam with the Profile

Folder Name	Description	Roams with profile by default	Redirect with Group Policy
Application Data	Per-user roaming application data.	Yes	Yes
Cookies	User's Internet Explorer cookies.	Yes	No
Desktop	Desktop items, including files and shortcuts.	Yes	Yes
Favorites	User's Internet Explorer favorites.	Yes	No
Local Settings	Temporary files and per-user non-roaming application data.	No	No
My Documents	User's documents.	Yes	Yes
NetHood	Shortcuts to Network Neighborhood items.	Yes	No
PrintHood	Shortcuts to printer folder items.	Yes	No
Recent	Shortcuts to recently used documents	Yes	No
Send To	Shortcuts to document storage locations and applications.	Yes	No
Start Menu	User's personal start menu.	Yes	Yes
Templates	Per-user customized templates.	Yes	No

Non-Roaming Folders

The default behavior of roaming user profiles in Windows NT 4.0 is to include all the folders in the user profile directory. Thus when a user first logs on, all folders within the profile folder are copied from the server to the client at logon and copied back at logoff,

Windows 2000 introduced a per-user local settings folder into the user profile that is not copied during log on or logoff. This folder is intended for the storage of operating system components and other applications can store non-roaming per-user data. A typical example of the usage of this folder is for Microsoft Internet Explorer to store a user's Favorites in the roaming portion of the user profile but store the Temporary Internet Files in the local (non-roaming) portion of the user profile. This will allow a user to retain access to their favorite URLs, but will save copying of temporary cache files at logon and logoff.

On computers running Windows Server 2003, Windows XP or Windows 2000, the History, Local Settings, Temp and Temporary Internet Files folders do not roam by default. Other Non-Roaming Folders are configured using the Group Policy Editor. The path for this setting in the Group Policy name space is:

User Configuration\Administrative Templates\System\User Profiles\Exclude directories in roaming profile

Once enabled this allows multiple folder names to be defined, all relative to the root of the user's profile. Once included in the policy these folders will not be copied to the local machine at logon, nor copied back to the server at logoff. This setting is likely to result in decreased time taken for a user to logon, by restricting the amount of data within a user profile that really does roam with the user.

How Do Users Get Their Profile?

The way in which users get their profiles depends on the type of profile they're configured to use. This section describes this process.

Local Profile - New User

1. The user logs on.
2. The operating system checks the list of user profiles located in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList to determine if a local profile exists for the user.
3. Because this is a new user, no local profile is found. If the computer is part of a domain, the operating system checks if a domain wide default profile exists in a folder named **Default User** on the domain controller's **NETLOGON** share.
   - If a domain wide profile exists, it is copied to a subfolder on the local computer with the username under %SYSTEMDRIVE%\Documents and Settings\. For example, a new user with the username JDoe would have a profile created in %SYSTEMDRIVE%\Documents and Settings\JDoe.
   - If a default domain profile does not exist, then the local default profile is copied from the % Systemdrive%\Documents and Settings\Default User folder to a subfolder on the local computer with a username under %Systemdrive%\Documents and Settings\.
4. If the computer is not part of a domain, the local default profile is copied from the %Systemdrive% \Documents and Settings\Default User folder to a subfolder on the local computer with a username under %Systemdrive%\Documents and Settings\.
5. The user's registry hive (NTUSER.DAT) is mapped to the HKEY_CURRENT_USER portion of the registry.
6. The users %userprofile% environment variable is updated with the value of the local profile folder
7. When the user logs off, a profile is saved to the local hard disk of the computer.

Local Profile - Existing User

1. The user logs on.
2. Windows checks the list of user profiles located in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList to get the path to the user's profile.
3. The user's registry hive (NTUSER.DAT) is mapped to the HKEY_CURRENT_USER portion of the registry.
4. The users %userprofile% environment variable is updated with the value of the local profile folder.
5. When the user logs off, the profile is saved to the local hard disk of the computer.

Roaming Profile - New User

1. The user logs on.
2. The path to the users roaming profile is retrieved from the user object on the Domain Controller.
3. Windows checks to see if a profile exists in the roaming path, if no profile exists a folder is created.
4. Windows checks the list of user profiles located in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList to determine if a cached copy of the profile exists. If a local copy of the profile is not found, and the computer is part of a domain, Windows checks to determine if a domain wide default profile exists in the Default User folder on the domain controller's NETLOGON share.

- If a domain wide profile exists, it is copied to a subfolder on the local computer with their username under %Systemdrive%\Documents and Settings\.
- If a default domain profile does not exist, then the local default profile is copied from the %Systemdrive%\Documents and Settings\Default User folder to a subfolder on the local computer with their username under %Systemdrive%\Documents and Settings\.

5. The user's registry hive (NTUSER.DAT) is mapped to the HKEY_CURRENT_USER portion of the registry.
6. The users %userprofile% environment variable is updated with the value of the local profile folder
7. The user can then run applications and edit documents as normal. When the user logs off, their local profile is copied to the path configured by the administrator. If a profile already exists on the server, the local profile is merged with the server copy (see merge algorithm later in this paper for more details).

Roaming Profile - Existing User

1. The user logs on.
2. The path to the users roaming profile is retrieved from the user object on the Domain Controller.
3. Windows checks to see if a profile exists in the roaming path, if no profile exists a folder is created.
4. Windows checks the list of user profiles located in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList to get the path to the user's cached profile if it exists.
5. The contents of the local cached profile are compared with the copy of the profile on the server, and the two profiles are merged. (See the new merge algorithm later in this paper for more details).
6. The user's registry hive (NTUSER.DAT) is mapped to the HKEY_CURRENT_USER portion of the registry.
7. The users %userprofile% environment variable is updated with the value of the local profile folder
8. The user can then run applications and edit documents as normal. When the user logs off, the local profile is copied to the path configured by the administrator. If a profile already exists on the server, the local profile is merged with the server copy.

Enhancements to User Profiles in Windows Server 2003 and Windows XP

User data management and user settings management features provide several enhancements that increase the usability, resilience, and performance of user profiles:

- New Group Policy settings
- Support for Windows XP fast network logon
- New System Service profiles
- More robust roaming

New Group Policy Settings

User profiles policies have moved to their own node in the Group Policy Editor: Administrative Templates\System\User Profiles. In addition there are three new policies under computer policies:

- **Prevent Roaming Profile Changes from Propagating to the server.** This policy determines if the changes a user makes to their roaming profile are merged with the server copy of their profile. If this policy is set at login, the user will receive their Roaming Profile, but any changes a user makes to their profile will not be merged to their roaming profile at logoff.
- **Add the Administrator security group to the roaming user profile share**. In Windows 2000, the default file permissions for newly generated roaming profiles are full control, or read and write access for the user, and no file access for the administrators group. This policy allows an administrator to choose the same behavior as Windows NT 4.0, and have the administrators group given full control of the user's profile directories.
- **Only allow local user profiles**. This setting determines if roaming user profiles are available on a particular computer. By default, when roaming profile users log on to a computer, their roaming profile is copied down to the local computer. Using this setting, an administrator can prevent users configured to use roaming profiles from receiving their roaming profile on a specific computer.

Support for fast network logon

Fast network logon overview

Windows XP includes new features that provide faster start up of a computer by not waiting for the network during boot and logon.

By default, Windows XP (but not Windows Server 2003) does not wait for the network to be fully initialized at

startup and logon. Any existing users logging on are logged on using cached credentials, which results in shorter logon times. Because the computer doesn't wait for the network to be fully started, Group Policy is applied in the background once the network becomes available. This has a number of effects on the logon process:

- **Changes to some Group Policy extensions can take up to three logons to become effective.** Because background refresh becomes the default behavior, some policy extensions such as Software Installation and Folder Redirection may require as many as three logons to apply changes. This is because to be able to operate safely, these extensions require that no users be logged on, so they must be processed in the foreground before users are actively using the computer. In the case of Advanced folder redirection, because policy is evaluated based on security group membership three logons will be required: the first logon to update the cached user object (and security group membership), the second logon for policy to detect the change in security group membership and require a foreground policy application, and the third logon to actually apply folder redirection policy in the foreground.
- **Changes to some user object properties may take two logons to become effective.** Because users are logged on using cached credentials, changes that are made to the user object, such as adding a roaming profile path, home directory, or user object logon script, may take up to two logons to be detected. The user object is updated in the background after the user has logged on, so any changes to its properties will not take effect until the next logon at least. Certain key fields in the user object are also checked at logoff, so if the user is logged on at the time of the change, the change may be detected at logoff.

Changes in roaming user profiles to support fast network logon

When a user logs onto a computer they have not logged onto for some time, the timestamps of the local user registry hives are compared to the server registry hive and the newest "wins". Typically this is the server copy of the registry, as the timestamps are checked before the hive is loaded.

However, when Windows XP is operating in fast network logon mode, the user is always logged on with a cached profile. The effect of this is that when the system detects that the user is now a roaming user, the local registry hive has already been loaded and therefore the hive timestamp is always changed. This introduces the possibility that if a user logs onto multiple computers, an older profile can overwrite a newer server profile because the user's roaming status is one step behind (due to the cached logon). To avoid this situation, the roaming profile algorithm treats the transition from local to roaming on a given computer as a special case:

At logon, checks are made to see which of the following conditions are true:

- Is this is the first roaming logon for a user that previously had a local profile?
- Is there a server copy of the user's profile?

If all of these conditions are met, then the algorithm is subtly changed, the new algorithm does the following:

1. The contents of the local profile are merged with the server copy of the profile as normal, with the exception of the user registry hive (ntuser.dat).
2. The server copy of the user registry is always copied from the server profile to the local profile, regardless of the time stamps on the hives.

In all other cases, the algorithm remains unchanged. It's only the first time that a user becomes roaming on a specific computer that this check is made. Once the user has become a roaming user, the computer always waits for the network (so that the profile can be downloaded) and the behavior is exactly the same as Windows 2000.

With this change, it is recommended that if an administrator removes the profile path from a user's user object, that they either rename or delete the corresponding profile folder. If the profile folder is not removed, and the administrator re-adds the same profile path, the user will receive the older server copy of their registry.

New System Service profiles

Windows XP and Windows Server 2003 introduce three new user profiles for the System:

- LocalService
- NetworkService
- System

LocalService and NetworkService profiles

The LocalService and NetworkService profiles are automatically created for two new built in user accounts that are used by the Service Control Manager to host services that do not need to run as the local system account. While these two new profiles are normal user profiles, because they are required by the system to run, they are treated slightly differently:

- LocalService and NetworkService profiles are not shown in the profiles list on the system properties dialog.
- Both LocalService and NetworkService profiles are located in %systemroot%\Documents and Settings by default, but are marked as super hidden so that they are not ordinarily visible.

System Profile

In Windows 2000, when an application or service used the LoadUserProfile API to load a user profile for a process running as the local system, Windows created a profile named %computername%**$** , where % computername% is the name of the local computer. This could cause problems for some applications and services, because depending on whether the system profile was loaded, HKEY_CURRENT_USER could in fact resolve to different registries – either HKEY_USERS \S-1-5-18 or HKEY_USERS\.DEFAULT depending on whether another component has loaded the SYSTEM profile.

To avoid this, Windows Server 2003 and Windows XP create a new profile for the system, located in % systemroot%\System32\Config\SystemProfile. This profile is always loaded, and is a link to HKEY_USERS\.DEFAULT. This ensures that system components always have a consistent profile and registry.

More robust roaming

In Windows 2000, an issue exists whereby poorly written applications and services that keep registry keys open during logoff prevent Windows from unloading the user's registry hive. When this occurs, changes that a user has made to their profile are not saved to the server. This has three symptoms:

- The user experience is impacted, as users may wonder why changes have not been saved when they log onto another computer.
- Since "locked" profiles never get unloaded, they end up using a lot of memory on a terminal server that has many users logging in.
- If a profile is marked for deletion at logoff (to cleanup the machine or for temporary profiles), profiles do not get deleted.

The three symptoms are solved as follows:

- In Windows 2000 when a user logs off, if the profile is "locked", Windows polls the profile for 60-seconds before giving up. Windows Server 2003 and Windows XP now save the users registry hive at the end of the 60-second delay, and roam the profile correctly.
- When the application or service closes the registry key "unlocking" the profile, Windows Server 2003 or Windows XP will unload the users registry, thus freeing the memory consumed by the profile.
- If a profile is marked for deletion at logoff, when the reference count drops to zero, it will be unloaded and deleted. In the event that the application never releases the registry key, Windows Server 2003 or Windows XP will delete all profiles marked for deletion at the next machine boot.

Note that if a roaming user logs onto back onto a machine that failed to unload her profile previously, and the profile has still not unloaded, the user will receive the currently loaded profile. If the user has logged onto another computer in the meantime, and made changes to their profile, the changes will not be available on the machine with the “locked” profile.

Improved Merge Algorithm

This section describes how Windows Server 2003 or Windows XP reconciles local and server copies of a user’s profile. To improve the experience of users, roaming profiles have a new algorithm to synchronize copies of a profile. This prevents problems from occurring when a user logs into two different computers simultaneously. The Windows NT 4.0 algorithm worked well in the most common cases where users logged on to only a single computer. However, when a user logged onto multiple computers at the same time, the user sometimes experienced unexpected behavior caused by the assumption that each computer had the master copy of the profile.

For Windows Server 2003, Windows XP, and Windows 2000, the algorithm was changed to support the merging of user profiles at the file level and to provide support for last writer wins.

To illustrate the behavior of the new algorithm, several examples are presented that compare the behavior of Windows NT 4.0 to the current model.

Overview of the Windows NT 4.0 Algorithm

In Windows NT 4.0, the algorithm is an Xcopy with full synchronization support, meaning it has the ability to mirror a profile from one location to another, and any extra files or directories in the destination location are removed. The algorithm is based on the concept that there is only one master profile at any one time. When the user is logged on, the master profile is on the local computer. When the user is not logged on, the master profile is on the server.

1. The user logs on to computer A, the primary computer.

2. The roaming profile is Xcopied from the server location to the local profile location.
3. The user creates documents, changes colors, and so on. All of these changes are stored in the local profile location.
4. As the user logs off the computer, the profile is Xcopied from the local profile location back to the server location.

This is an exact mirroring process. If there are any extra files in the server location, they are deleted to ensure that the server location is a duplicate of the local profile. As mentioned previously, this works well in the majority of cases, where a user logs on to only a single computer; but a user who logs on to multiple computers at the same time might experience unexpected behavior.

Examples of Windows NT 4.0 Merge Algorithm Issues

When using Windows NT 4.0, a problem arises if the user logs on at two or more computers. Building on the preceding example:

1. The user logs on to computer A.
2. The user logs on to computer B.
3. The user creates a document on computer A and stores it in the user profile.
4. The user logs off of computer A.
5. The user logs off of computer B.

The document that the user created in step 3 is deleted because, from the perspective of computer B, the master profile is stored locally. The extra files on the server must be deleted so that the local profile is currently the master server profile.

The Windows XP algorithm preserves the document because it is able to compare the time the document was created with the time the profile was loaded. If the document was created or modified after the profile load time, the file must be preserved because it came from a different source.

A similar problem can occur when files are modified. For example, suppose that the user has a document called Document.doc in his or her My Documents folder in the server copy of the profile:

1. The user logs on to computer A.
2. The user logs on to computer B.
3. The user modifies the document on computer A.
4. The user logs off computer A.
5. The user logs off computer B.

The changes made to the document on computer A are lost because when the user logged off computer B, the computer overwrote the new version of the document with the old one; the computer is programmed to recognize that it had the master version of the profile.

The current algorithm preserves the changes to the document because it compares the time the document was modified with the time the profile was loaded. This results in a much better experience for the user.

Overview of Windows Server 2003 Merge Algorithm

Windows Server 2003 and Windows XP merge user profiles at the file level. The merged profile contains the superset of files that are in the local computer and server copies of the user's profile. In the case where the same file is in both the local and server copy of the profile, the file that was modified most recently is used. This means that new files are not deleted, and updated versions of existing files are not overwritten.

When a document or file is updated, the new algorithm compares the timestamp of the destination file with the timestamp of the source file. If the destination file is newer, it is not overwritten.

When a user logs on to a computer, the current time is saved; when the user logs off, this timestamp is used to determine which files are new in the server profile and which files have been deleted in the local profile. For example, if the server profile has a document in the **My Documents** folder called Review.doc and this file does not exist in the local profile, either it is a new file from a different computer, or it was originally in the local profile and the user deleted it. Knowing the time when this new profile was loaded, it is possible to compare it against the timestamp of Review.doc. If Review.doc was created or written to after the profile load time, the file must be preserved because it came from a different source. If the Review.doc timestamp is older than the profile load time, Review.doc must be deleted because it would have been copied to the local computer at load time.

In addition, some files might need to be removed from the local cache so that items that were deleted between sessions remain deleted. For example:

1. The user logs on to computer A.

2. The user creates or modifies a document on computer A.
3. The user logs on to computer B.
4. The user logs off computer B; computer B has a copy of the document.
5. The user deletes the document and logs off computer A.

To ensure that the files are deleted, the cached version of the profile is synchronized with the profile on the server when a user logs on. All files in the local cache that are not present in the server and that were not modified since the last logoff time are removed. By using these changes, Windows XP can merge user profiles.

There are several files that will **always** be copied because the timestamp on those files is changed as part of the profile unloading process. The ntuser.dat and ntuser.ini files will always be copied to the server.

Quotas on Profile Size

Often, over time a roaming user profile may potentially grow to a large size, as the user stores more data on their desktop, installs more applications and increases the complexity of their roaming environment. While much of this enhances the user experience, it may result in greater logon and logoff times for the user, as the data is copied down from or back up to the server.

While excluding some of the profile folders from roaming can reduce profile size, there may be situations in which it is more useful to actively restrict the overall quota size, to prevent it growing to an excessive size. The Proquota.exe program is a tool that you can set to monitor the size of a user's profile. If an individual's user profile exceeds the predetermined file limit, the user cannot log off from the computer until the user reduces the size of files.

Profile quota size is managed using the Group Policy snap-in. You can use the **Limit Profile Size** policy, available in the **User Configuration\Administrative Templates\System\User Profiles** node of the Group Policy snap-in to set the maximum size of the roaming user profile and to determine the system's response when the limit is reached. Click the Explain tab of this policy setting for more details.

Deleting cached roaming profiles

If you are concerned with disk size on a multi-user computer — for example, a public computer where thousands of users can log on, you can also use the Group Policy setting that removes cached versions of the profile on logoff. The policy is called **Delete cached copies of roaming profiles**, and it is accessed under the **Computer Configuration\Administrative Templates\System\User Profiles** node of the Group Policy snap-in.

Changes to the way Guest profiles are handled

Windows 2000 and Windows NT 4.0 always delete the user profile of users belonging to the local Guests security group when users log off. Windows XP and Windows Server 2003, continue to delete the profile of guest users, **only** when the computer is joined to a domain. When the computer is part of a workgroup, the user profile of users belonging to the local Guests group is not deleted at logoff.

The exception is when the user is a member of the local Guests group AND a member of local Administrators, in this case the profile is NOT deleted when in a domain.

Group Policy Settings for Roaming User Profiles

See the Appendix for a list of policy settings related to roaming user profiles. For details about these policy settings, click the policy's **Explain** tab.

How to Configure a Roaming User Profile

You can configure a roaming profile by using the following procedure.

To configure a roaming profile for users:

1. Create a folder on the server where user profiles will be stored. This will be the top-level folder that contains all the individual user profiles.
2. Configure the folder as a shared folder, and give all users **Full Control** permissions.
3. Open the **Active Directory Users and Computers** snap-in and navigate to the individual's **User** object.
4. Right-click the **user's name** and click **Properties** on the shortcut menu.
5. Click the **Profile** tab.
6. For the **Profile Path**, type the path to the network share where the user profile is to be stored. For example, for a user whose network name is JDoe, the following path, \\NetworkShare\Profiles\%username%, would create a directory called JDoe in the Profiles share on the server used to store user profiles.

You can also populate the profile path by using an Active Directory Scripting Interface (ADSI) script. ADSI

provides a single set of interfaces for managing network resources. Administrators can combine ADSI with Visual Basic® Scripting Edition (VbScript) or Jscript® scripts to manage resources in the directory service such as users, services, and so on.

To learn about ADSI and ADSI scripts, see the Microsoft Platform SDK.

User Profiles Troubleshooting

The first troubleshooting step should be to examine the Application event log on the client computer, and determine the error.

If this is a roaming profile, be sure to check for the correct permissions (see Security Considerations when Configuring Roaming User Profiles for the required permissions) - one of the most common causes of roaming user profile errors is incorrect permissions on the profile share.

In addition to logging events in the Application Event log, User Profiles can provide a detailed log to aid troubleshooting. To create a detailed log file for user profiles:

1. Start regedit and locate the following path:
   HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
2. Create a new value called UserEnvDebugLevel as a REG_DWORD, and set the value to 30002 in hexadecimal format.

The log file can be found at: %windir%\debug\usermode\userenv.log

Security Considerations when Configuring Roaming User Profiles

When creating the roaming profile share, limit access to the share to only users that need access.

Because a users roaming profile contains personal information, such as documents and EFS certificates care should be taken to protect it as well as possible. In general:

- Restrict the share to only users that need access. Create a security group for users that have profiles on a particular share, and limit access to only those users.
- When creating the share, hide the share by putting a $ after the share name. This will hide the share from casual browsers; the share will not be visible in the network neighborhood.
- Unless you need special permissions on the profile folder, don't pre-create profile folders for the user, allow the system to create them.
- Only give users the minimum amount of permissions needed. The permissions needed are shown in the tables below:

Table 3 NTFS Permissions for Roaming Profile Parent Folder

User Account	Minimum permissions required
Creator/Owner	Full Control, Subfolders And Files Only
Administrator	None
Security group of users needing to put data on share.	List Folder/Read Data, Create Folders/Append Data - This Folder Only
Everyone	No Permissions
Local System	Full Control, This Folder, Subfolders And Files

Table 4 Share level (SMB) Permissions for Roaming Profile Share

User Account	Default Permissions	Minimum permissions required
Everyone	Full Control	No Permissions
Security group of users needing to put data on share.	N/A	Full Control,

Table 5 NTFS Permissions for Each User's Roaming Profile Folder

User Account	Default Permissions	Minimum permissions required
%Username%	Full Control, Owner Of Folder	Full Control, Owner Of Folder
Local System	Full Control	Full Control

Administrators	No Permissions*	No Permissions
Everyone	No Permissions	No Permissions

**Unless the "Add the Administrator security group to the roaming user profile share" policy is set, in which case the Administrators group has Full Control. (requires Windows 2000 Service pack 2 or later)*

Use at least Windows 2000 servers to host profile shares.

Because a users roaming profile contains personal information which is copied to and from the client computer, and the server hosting the roaming profile, it is important to ensure that data is protected as it travels over the network.

The biggest potential threats to the privacy and integrity of a user's data come from intercepting the data as it passes over the network, tampering with the data as it passes over the network, and spoofing the server hosting the user's data.

Several features of Windows 2000 and Windows Server 2003 can help to secure a user's data:

- **Kerberos** - Kerberos is standard on all versions of Windows 2000 and Windows Server 2003s, and ensures the highest level of security to network resources. While NTLM authenticates the client only, Kerberos authenticates the server and the client. When NTLM is used, the client doesn't know whether the server is valid – this is particularly important if the client is exchanging personal files with the server, as is the case with Roaming Profiles. Kerberos provides better security than NTLM and is not available on Windows NT version 4.0 or earlier operating systems.
- **IPSec**- The IP Security Protocol (IPSec) provides network-level authentication, data integrity, and encryption ensuring that roamed data is:
  - Safe from data modification while enroute.
  - Safe from interception, viewing, or copying.
  - Safe from being accessed by unauthenticated parties.

  More information on IPSec can be found in the IP Security for Windows 2000 Server white paper.
- **SMB Signing**- The Server Message Block (SMB) authentication protocol supports message authentication, which prevents active message and "man-in-the-middle" attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. In order to use SMB signing, you must either enable it or require it on both the SMB client and the SMB server. Note: SMB signing imposes a performance penalty; although it doesn't consume any more network bandwidth, it does use more CPU cycles on the client and server side.

Always use the NTFS Filesystem for volumes holding users data.

For the most secure configuration, configure servers hosting roaming profiles to use the NTFS File System. Unlike FAT, NTFS supports Discretionary access control lists (DACLs) and system access control lists (SACLs), which control who can perform operations on a file and what events will trigger logging of actions performed on a file.

Best Practices for User Profiles

To get the best experience possible from roaming user profiles, it is important to read all the documentation and plan your implementation thoroughly. This section presents best practices for using roaming user profiles.

Turn off the fast logon enhancement

With the fast logon "enhancement" in Windows XP when users change from a local to a roaming profile, it will take two logons on each machine for profile changes to be registered. This is because the user always logs on with cached credentials; therefore it takes one logon for the network to notice that the user has become roaming and the second logon to apply these settings.

To ensure the best possible experience, enable the setting **Always wait for the network at computer startup and logon**, located at Computer Configuration\Administrative Templates\System\Logon.

Redirect the location of the My Documents Folder outside of the users Roaming Profile.

To decrease initial logon time to a new computer, it is recommended that you redirect the location of the My Documents folder outside of the user's roaming profile. The best way to do this is with Folder Redirection. If you don't have Active Directory enabled, you can do this with a logon script or instruct the user to do so manually.

Let the system create profile folders for each user.

To ensure that Roaming user profiles work optimally, create only the root profile share on the server, and let the system create the folders for each user. If you must create folders for the users, ensure that you have the

correct permissions set. For details on the required permissions see **Security Considerations when Configuring Roaming User Profiles.**

Dont use Offline Folders on Roaming Profile Shares.

Make sure that you turn off Offline Folders for shares where roaming user profiles are stored. If you do not turn off Offline Folders for a user's profile, you may experience synchronization problems as both Offline Folders and Roaming Profiles try to synchronize the files in a user's profile.

Note This does not affect using Offline Folders with redirected folders such as My Documents.

Do not use Encrypted File System (EFS) on files in a Roaming User Profile.

The Encrypted File System is not compatible with files within Roaming User Profiles. If you encrypt profile folders or files using EFS the user's profile will not roam.

Note This does not affect encrypting files on remote shares.

Do not Set Disk Quotas too low for users with Roaming Profiles.

If a user's disk quotas are set too low, roaming profile synchronization may fail. Make sure enough disk space is allocated to allow the system to create a temporary duplicate copy of a user's profile. Because the temporary profile is created in the user's context as part of the synchronization process, it debits his or her quota.

Use Group Policy loopback policy processing sparingly if you use roaming profiles.

Group Policy loopback processing enables a different set of user type Group Policies to be applied based on the computer being logged onto. This policy is useful when you need to have user type policies applied to users of specific computers. There are two methods for doing this. One allows for the policies applied to the user to be processed, but to also apply user policies based on the computer that the user has logged onto. The second method does not apply the user's settings based on where the user object is, but only processes the policies based on the computer's list of GPOs.

Use caution when using loopback policy processing and roaming profiles—especially when users may roam between Windows 2000 or Windows XP-based computers and Windows NT 4.0-based computers. You may see some "tattooing"— applications can store policy settings in HKCU\Software\Policies regardless of operating system version. Windows NT 4 also stored some explorer policy settings in HKCU\Software\Microsoft\windows\currentversion\explorer\policies. Windows 2000 and Windows XP clears these keys each time before re-applying current policy, but because Windows NT 4 does not clear them, you will get settings left if you roam from a Windows 2000-based machine.

Roaming between the same operating system versions

Because the contents of the user's registry are opaque to roaming user profiles, you should minimize as much as possible significant differences between operating system installations on computers the users will roam between. When using roaming profiles, try to ensure that:

- The same application versions are installed.
- Applications are installed to the same path and drive.
- The operating system is installed on the same %systemdrive% and in the same %windir%.
- The operating system language and system locale are the same.

Roaming between different operating system versions

Although roaming between Windows 2000 and Windows XP should be a smooth process, there are some precautions you can take to minimize possible issues:

- If you can avoid roaming between versions of the operating system, then do so. There's nothing inherent in roaming that will cause problems, but the data that applications put in the profile may have unintended side effects on other versions of the operating system.
- Make sure that you have the same application versions installed.
- Make sure that applications are installed to the same path and drive.
- Make sure that the different versions of the operating system are installed on the same %systemdrive% and in the same %windir%.
- If Users roam between Windows NT 4.0-based clients and Windows XP- Windows 2000-based clients, consider setting the Profile Path during install on Windows XP or Windows 2000. Differences in the default profile path (%windir%\Profiles vs. %systemdrive%\Documents and Settings) may cause problems for users roaming between Windows NT 4.0-based clients and Windows XP- or Windows 2000-based clients. To minimize the chance of problems, make sure the path to the profile is the same on both clients.

Folder Redirection Overview

Folder redirection is a feature of IntelliMirror that allows users and administrators to redirect the path of a folder to a new location. The new location can be a folder on the local computer or a directory on a network share. Users have the ability to work with documents on a server as if the documents were based on the local drive. For example, you can redirect the My Documents folder, which is usually stored on the computer's local hard disk, to a network location. The documents in the folder are available to the user from any computer on the network. The My Documents folder is the location on the Windows Server 2003, Windows XP or Windows 2000 desktop where the user can save documents and graphic files.

Previously, administrators who wanted to redirect folders to the network had to use logon scripts to change registry values. In Windows Server 2003 and Windows XP, the same task can be accomplished by using Group Policy.

Advantages of Using Folder Redirection

Folder redirection provides a number of advantages. Some of the following benefits relate to redirecting any folder, but redirecting My Documents can be particularly advantageous.

- Even if a user logs on to various computers on the network, the user’s documents are always available.
- The system administrator can use Group Policy to set disk quotas, limiting the amount of space taken up by users' special folders.
- Data specific to a user can be redirected to a different hard disk on the user's local computer from the hard disk holding the operating system files. This protects the user's data if the operating system needs to be reinstalled.
- Data stored on a shared network server can be backed up as part of routine system administration. This is safer and it requires no action on the part of the user.

You can also combine Folder Redirection and roaming user profiles to decrease logon and logoff times for roaming and mobile users. Besides the improved availability and backup benefits of having the data on the network, users also have performance gains with low-speed network connections and subsequent logon sessions. Because only some of their documents are copied, performance is improved when the users’ profiles are copied from the server. Not all of the data in the user profile is transferred to the desktop each time the user logs on — only the data that user requires.

When you combine the use of Folder Redirection and roaming user profiles, you can provide fast computer replacement. If a user's computer needs to be replaced, the data that a user requires can quickly be re-established on a replacement computer. By using Folder Redirection to redirect the My Documents and Application Data folders, in conjunction with roaming user profiles and Group Policy-based deployment of applications, an organization can move the key user state to a network location. This means the user’s documents, settings, and applications follow them, regardless of which Windows XP computer the user logs on to.

For increased availability, Offline File technology gives users access to My Documents even when they are not connected to the network. For more information, see the Complementary Technologies section later in this article. This is particularly useful for those who use laptop computers.

Folders that Can Be Redirected

My Documents, Application Data, Desktop, and Start Menu are the top level folders that can be redirected. These were identified as the key folders that an organization would need to redirect to preserve important user data and settings. There are several advantages to redirecting each of these folders. The usefulness of each will vary according to your organization’s needs.

- **My Documents.** The place in the shell for users to save their documents and pictures. Because common dialog boxes in Windows Server 2003 and Windows XP point to the My Documents folder by default, there is a greater tendency for users to save files there. Data stored on a shared network server can be backed up as part of routine system administration, and is safer because it requires no action from the user.
- **Application Data.** Often applications place large data, such as dictionaries, in the Application Data portion of the user's profile, which roams with the user. To improve performance, Application Data was added to the list of folders that can be redirected. This means that users can still have access to Application Data (such as the custom dictionary), but without the need to download the (possibly large) files at every logon.
- **Desktop.** Some organizations want to configure computers to look the same. By redirecting the desktop for a group of users, you can ensure that all users share the same desktop, with the same desktop items.
- **Start Menu.** For compatibility with Windows NT 4.0, Windows Server 2003 and Windows XP allow you to use Folder Redirection to redirect the **Start** menu folder. **Start** menu redirection is treated differently from other redirected folders in that the contents of the user’s **Start** menu are not copied to the redirected location. It is assumed that a redirected **Start** menu has been pre-created by an administrator and that all users **Start** menus will be the same. As a best practice for computers running Windows Server 2003 or

Windows XP, do not use Folder Redirection to redirect the **Start** menu folder, use Group Policy to control what appears on the **Start** menu.

Folder Redirection Improvements for Windows XP and Windows Server 2003

This section provides information on the differences between Windows 2000 and Windows Server 2003.

User Interface changes

The Folder Redirection user interface has been simplified for Windows Server 2003. The main goals of these changes were to simplify the use of Folder Redirection by removing the requirement that administrators be familiar with environment variables such as %USERNAME%.

In addition to the simplified UI, several new redirection options have been added:

- **Create a folder for each user under the root path**

  Rather than having to enter a UNC path such as \\server\share\%username%\MyDocuments, the administrator can simply type in the path to the share such as \\server\share, and Folder Redirection will automatically append the username and the folder name when the policy is applied. This removes the need for administrators to be familiar with environment variables, and minimizes the chances of errors and spelling mistakes.

- **Redirect to home directory (My Documents Only)**

  Windows Server 2003 and Windows XP allow you to redirect a user's My Documents folder to their home directory. This option is intended only for organizations that have a legacy deployment of home directories and wish to transition users to the My Documents metaphor while maintaining compatibility with their existing home directory environment. ***You should only select this option if you have already deployed home directories in your organization.***

  Folder redirection treats redirection to the home directory as a special case and certain checks are skipped:

  - Redirection to the home folder is only supported on Windows XP and Windows Server 2003 computers. **Redirection to the home directory policy will fail to apply on Windows 2000 computers.**
  - Security is not checked – it is assumed that the administrator has set directory security correctly, no ACL check is made and no reACLing is done. The **Grant the user exclusive rights to My Documents** checkbox on the settings page of the property sheet is disabled**.**
  - No ownership checks are made - normally folder redirection will fail if a user is not the owner of the folder they are being redirected to. Because redirection to the home directory is intended for use in a legacy environment, this ownership check is skipped.
  - Users must have the home folder property correctly set on their user object - The folder redirection client side extension retrieves the actual path for the user's home directory from the user object at logon time. Users affected by Folder Redirection Policy must have this path correctly set or folder redirection will not apply.

- **Redirect to a specific path**

  This option is intended to allow an administrator to redirect folders to an alternate local drive/partition, or to enter unusual configurations not anticipated by the new user interface. Functionally it works in exactly the same way as the Windows 2000 folder redirection user interface.

- **Redirect to the local user profile**

  This option is intended to allow an administrator to redirect the selected folder to the default location in the local user profile, for example: %userprofile%\<Folder Name>. This setting can be used to remove redirection for a particular folder, without removing the GPO. Note: Setting the redirection option to "Not Configured" (or "No Administrative policy specified" in the Windows 2000 UI) **does not** redirect the folder to the local profile, this option means that Folder Redirection is not configured – *if a folder was previously redirected it will continue to be redirected to the previous location.* If an administrator wished to return the folder to the local user profile they can use this redirection setting.

My Pictures no longer shown in the Folder Redirection Node

To simplify the user interface and to help support the best practice that the My Pictures folder should always follow the My Documents folder, the My Pictures folder is not shown in the Folder Redirection node for new GPO's. If you have previously redirected the My Pictures folder separately, the My Pictures node will still appear.

Redirected Folders automatically made available offline

By default in Windows XP and Windows Server 2003, any redirected shell folders such as My Documents, Desktop, Start Menu, and Application Data are automatically made available offline. This is in contrast to

Windows 2000, which required administrators to configure the "Administratively assigned offline files" policy setting to ensure all files in the redirected folders were always available offline. This setting was difficult to use with advanced folder redirection, and involved extra administrative overhead.

The default behavior can be overridden by enabling the "Do not automatically make redirected folders available offline" policy. This setting can be found in the Group Policy Editor in the User Configuration\Administrative Templates\Network\Offline Files section.

Note that on Windows Server 2003 Offline files are disabled by default.

How to Configure Folder Redirection

Administrators manage Folder Redirection settings by using the Group Policy snap-in.

To configure Folder Redirection:

1. To start the Group Policy snap-in from the Active Directory Users and Computers snap-in, click Start, point to Programs, click Administrative Tools, and then click Active Directory Users and Computers.
2. In the MMC console tree, right-click the domain or the OU for which to access Group Policy, click Properties, and click Group Policy.
3. To create a new Group Policy object (GPO), right-click the domain or OU you want to associate with the GPO, select Properties from the context menu, and then in the domain or OU container's Properties page, click the Group Policy tab.
4. Click New, and type the name to use for the GPO. For example, type Redirect MyDocuments GPO.
5. Click Edit to open the Group Policy snap-in and edit the new GPO.
6. In the Group Policy console, expand the User Configuration, Windows Settings, and Folder Redirection nodes. Icons for the personal folders that can be redirected will be displayed.
7. To redirect any of these folders, right-click the folder name, click Properties, and then select one of the following options from the Setting drop-down box:
   - Basic - Redirect everyone's folder to the same location. All folders affected by this Group Policy object will be stored on the same network share.
   - Advanced – Specify locations for various user groups. Folders are redirected to different network shares based on security group membership. For example, folders belonging to users in the Accounting group can be redirected to the Finance server, while folders belonging to users in the Sales group are redirected to the Marketing server.
8. On the My Documents Properties page, in the **Target folder location** drop down box select **Create a folder for each user under the root path.** In the Root Path text box, type the name of the shared network folder to use, or click **Browse** to locate it. Note: Unlike Windows 2000, you do not need to type in the %username% variable. The folder redirection code will automatically create a My Documents folder for each user, inside a folder based on their username. For example, type **\\FolderServer\MyDocumentsFolders** rather than **\\FolderServer\MyDocumentsFolders\%username%** as you would on Windows 2000.
9. In the folder's **Properties** dialog box, select the **Settings** tab, configure the options you want to use, and then click **Finish** to complete the Folder Redirection. The available options for settings are:
   - **Grant the user exclusive rights to My Documents.** If selected, this sets the NTFS security descriptor for the %username% folder to Full Control for the user and local system only; this means that administrators and other users do not have access rights to the folder. This option is enabled by default. Note: Changing this option after the policy has been applied to some users will only effect new users receiving the policy.
   - **Move the contents of My Documents to the new location.** Moves any document the user has in the local My Documents folder to the server share. This option is enabled by default.
   - **Leave the folder in the new location when policy is removed**. Specifies that files remain in the new location when the Group Policy object no longer applies. This option is enabled by default.
   - **Redirect the folder back to the local user profile location when policy is removed.** If enabled, specifies that the folder be copied back to the local profile location if the Group Policy object no longer applies.

     The My Documents Properties page provides two additional options for the My Pictures folder:

     Make My Pictures a subfolder of My Documents. If selected, when the My Documents folder is redirected, My Pictures remains a subfolder of My Documents. By default, My Pictures automatically follows the My Documents folder.

     Do not specify administrative policy for My Pictures. If selected, Group Policy does not control the location of My Pictures; this is determined by the user profile.

An important point to note is that you should not pre-create the directory defined by username. Folder Redirection will handle setting the appropriate ACLs on the folder. If you choose to pre-create folders for each user, be sure to set the permissions correctly (see the permissions tables in the Best Practices section later in this paper).

For more information about using the Group Policy snap-in and the Folder Redirection extension, refer to the Windows Server 2003 online Help, the Step-by-Step Guide to Understanding the Group Policy Feature Set at http://www.microsoft.com/windows2000/techinfo/planning/management/groupsteps.asp and the Step-by-Step Guide to User Data and User Settings at http://www.microsoft.com/windows2000/techinfo/planning/management/userdata.asp.

Changing settings after Folder Redirection policy has been applied.

It is possible to change the Folder Redirection options on the Settings tab after the policy has been applied, you should note that changing the value of the **Grant the user exclusive rights to <folder name>** setting will only apply to new users effected by the policy. Any existing users that received the policy will use the original **Grant the user exclusive rights to <folder name>** setting.

Folder Redirection and environment variables

The folder redirection client side extension is only able to process two environment variables: %username% and %userprofile%. Other environment variables such as %logonserver%, %homedrive% and %homepath% will not work with folder redirection.

Folder Redirection and mapped drives

Because folder redirection is processed early in the logon process, drives mapped via logon scripts (including the homedrive for folders other than My Documents), the folder redirection client side extension is not able to redirect to these locations. At the time that redirection takes place, the drives do not exist hence redirection fails.

Folder Redirection Troubleshooting.

Folder redirection processing contains 5 steps:

1. Determine which folders to redirect based on changes to policy at logon time.
2. Determine desired redirected location and verify access.
3. If folder does not exist: create folders, set ACLs.
4. If folder exists, check ACLs and ownership.
5. If desired, move contents.

Folder redirection failures only affect the folder redirection extension on a per folder basis. If you're pre-creating folders rather than letting the folder redirection extension automatically create the folder, typical errors include:

- Redirecting to a folder that is incorrectly ACL'd.
- User is not the owner of the folder.
- Destination does not exist.

Enabling logging

In addition to logging events in the Application Event log, Folder Redirection can provide a detailed log to aid troubleshooting. To create a detailed log file for folder redirection, use the following registry key:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics
- Set: FdeployDebugLevel = Reg_DWORD 0x0f

Note The log file can be found at: %windir%\debug\usermode\fdeploy.log

Using Logon Scripts to Redirect Folders

Although using Group Policy to redirect users' folders is the recommended method, there are alternate ways to achieve similar results. You can use logon scripts to set the values of the User Shell Folders key in the registry, which will give you basic functionality similar to Folder Redirection.

Alternatively, you could use Windows NT 4.0 system policies to set the appropriate values. However if you choose to do this, you loose the advantages of using Group Policy to set folder paths, such as automatic moving of files when the path changes, and the registry settings will persist.

Security Considerations when Configuring Folder Redirection

When creating the redirection share, limit access to the share to only users that need access.

Because redirected folders contain personal information, such as documents and EFS certificates care should be taken to protect them as well as possible. In general:

- Restrict the share to only users that need access. Create a security group for users that have redirected folders on a particular share, and limit access to only those users.
- When creating the share, hide the share by putting a $ after the share name. This will hide the share from casual browsers; the share will not be visible in the network neighborhood.
- Only give users the minimum amount of permissions needed. The permissions needed are shown in the tables below:

Table 12 NTFS Permissions for Folder Redirection Root Folder

User Account	Minimum permissions required
Creator/Owner	Full Control, Subfolders And Files Only
Administrator	None
Security group of users needing to put data on share.	List Folder/Read Data, Create Folders/Append Data - This Folder Only
Everyone	No Permissions
Local System	Full Control, This Folder, Subfolders And Files

Table 13 Share level (SMB) Permissions for Folder Redirection Share

User Account	Default Permissions	Minimum permissions required
Everyone	Full Control	No Permissions
Security group of users needing to put data on share.	N/A	Full Control,

Table 14 NTFS Permissions for Each User's Redirected Folder

User Account	Default Permissions	Minimum permissions required
%Username%	Full Control, Owner Of Folder	Full Control, Owner Of Folder
Local System	Full Control	Full Control
Administrators	No Permissions	No Permissions
Everyone	No Permissions	No Permissions

Use at least Windows 2000 servers to host redirected file shares.

Because a user's redirected files contain personal information which is copied to and from the client computer, and the server hosting the redirected folders, it is important to ensure that data is protected as it travels over the network.

The biggest potential threats to the privacy and integrity of a user's data come from intercepting the data as it passes over the network, tampering with the data as it passes over the network, and spoofing the server hosting the user's data.

Several features of Windows 2000 and Windows Server 2003 can help to secure a user's data:

- **Kerberos** - Kerberos is standard on all versions of Windows 2000 and Windows Server 2003, and ensures the highest level of security to network resources. While NTLM authenticates the client only, Kerberos authenticates the server and the client. When NTLM is used, the client doesn't know whether the server is valid – this is particularly important if the client is exchanging personal files with the server, as is the case with Roaming Profiles. Kerberos provides better security than NTLM and is not available on Windows NT version 4.0 or earlier operating systems.
- **IPSec**- The IP Security Protocol (IPSec) provides network-level authentication, data integrity, and encryption ensuring that roamed data is:

- Safe from data modification while enroute.
- Safe from interception, viewing, or copying.
- Safe from being accessed by unauthenticated parties.

More information on IPSec can be found in the IP Security for Windows 2000 Server white paper.

- **SMB Signing**- The Server Message Block (SMB) authentication protocol supports message authentication, which prevents active message and "man-in-the-middle" attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. In order to use SMB signing, you must either enable it or require it on both the SMB client and the SMB server. Note: SMB signing imposes a performance penalty; although it doesn't consume any more network bandwidth, it does use more CPU cycles on the client and server side.

Always use the NTFS Filesystem for volumes holding users data.

For the most secure configuration, configure servers hosting redirected files to use the NTFS File System. Unlike FAT, NTFS supports Discretionary access control lists (DACLs) and system access control lists (SACLs), which control who can perform operations on a file and what events will trigger logging of actions performed on a file.

Do not rely on EFS to encrypt users files when transmitted over the network

When using the Encrypting File System (EFS) to encrypt files on a remote server, encrypted data is not encrypted when in transit over the network, but only when stored on disk.

The exceptions to this are when your system includes Internet Protocol security (IPSec) or Web Distributed Authoring and Versioning (WebDAV). IPSec encrypts data while it is transported over a TCP/IP network. If the file is encrypted before being copied or moved to a WebDAV folder on a server, it will remain encrypted during the transmission and while it is stored on the server.

Encrypt the Offline Files cache

While the Offline Files cache is protected on NTFS partitions by ACLs by default, encrypting the cache enhances security on a local computer. By default, the cache on the local computer is not encrypted, so any encrypted files cached from the network will not be encrypted on the local computer. This may pose a security risk in some environments.

When encryption is enabled, all files in the Offline Files cache are encrypted. This includes existing files as well as files added later. The cached copy on the local computer is affected, but the associated network copy is not.

The cache can be encrypted in one of two ways:

1. Via Group Policy, by enabling the **Encrypt the Offline Files Cache** setting, located at Computer Configuration\Administrative Templates\Network\Offline Files, in the Group Policy editor.
2. Manually, by selecting Tools and then Folder Options in the command menu of Windows Explorer. Select the Offline Files tab, and check the **Encrypt offline files to secure data** checkbox.

Note Encryption of the Offline File cache is only available on Windows XP and above, it is not possible to encrypt the cache on Windows 2000 computers.

For more information on encrypting the Offline files cache, see How to Encrypt Offline Files at:
http://www.microsoft.com/windowsxp/pro/using/itpro/securing/encryptoffline.asp

Let the system create folders for each user.

To ensure that Folder Redirection works optimally, create only the root share on the server, and let the system create the folders for each user. Folder Redirection will create a folder for the user with appropriate security.

If you must create folders for the users, ensure that you have the correct permissions set, also note that if pre-creating folders you must uncheck the "grant the user exclusive rights to XXX" checkbox on the settings tab of the Folder Redirection page. If you don't uncheck this checkbox, then Folder Redirection will first check a pre-existing folder to ensure the user is the owner. If the folder is pre-created by the administrator, this check will fail and redirection will be aborted. Folder Redirection will then log an event in the Application event log:

Error: Folder Redirection
Event ID: 101
Event Message:
Failed to perform redirection of folder XXXX. The new directories for the redirected folder could not be created. The folder is configured to be redirected to \\server\share, the final expanded path was \\server\share\XXX .

The following error occurred:
This security ID may not be assigned as the owner of this object.

It is strongly recommended that you do not pre-create folders, and allow Folder Redirection to create the folder for the user.

Ensure correct permissions are set if redirecting to a users home directory.

Windows Server 2003 and Windows XP allow you to redirect a user's My Documents folder to their home directory. When redirecting to the home directory, the default security checks are not made - ownership and the existing directory security are not checked and any existing permissions are not changed - it is assumed that the permissions on the user's home directory are set appropriately.

If you are redirecting to a users home directory, be sure that the permissions on the user's home directory are set appropriately for your organization.

Best Practices for Folder Redirection

To get the best results from using Folder Redirection, it is important that you read the Group Policy documentation and plan your implementation thoroughly, particularly with respect to Group Policy.

To learn more about how Group Policy and Folder Redirection were developed in Windows 2000, see the Windows 2000 Management Services page at http://www.microsoft.com/windows2000/technologies/management/default.asp.

Do not use redirect to home directory option unless you have already deployed home directories in your organization.

Windows Server 2003 allows you to redirect a user's My Documents folder to the user's home directory. This option is intended only for organizations that have a legacy deployment of home directories and wish to transition users to the My Documents metaphor while maintaining compatibility with their existing home directory environment. You should only select this option if you have already deployed home directories in your organization.

Let the system create folders for each user.

To ensure that Folder Redirection works optimally, create only the root share on the server, and let the system create the folders for each user. If you must create folders for the users, ensure that you have the correct permissions set. See Security Considerations when Configuring Folder Redirection for the permissions required.

Considerations for Group Policy Removal

It is important to consider the behavior of your Folder Redirection policy settings when Group Policy is removed.

You specify policy removal options in the selected folder's Properties page, shown in Figure 2 below. This is accessed under the User Configuration\Windows Settings\Folder Redirection node of the Group Policy snap-in by right-clicking a folder, and clicking Properties**.** See Configuring Folder Redirection.

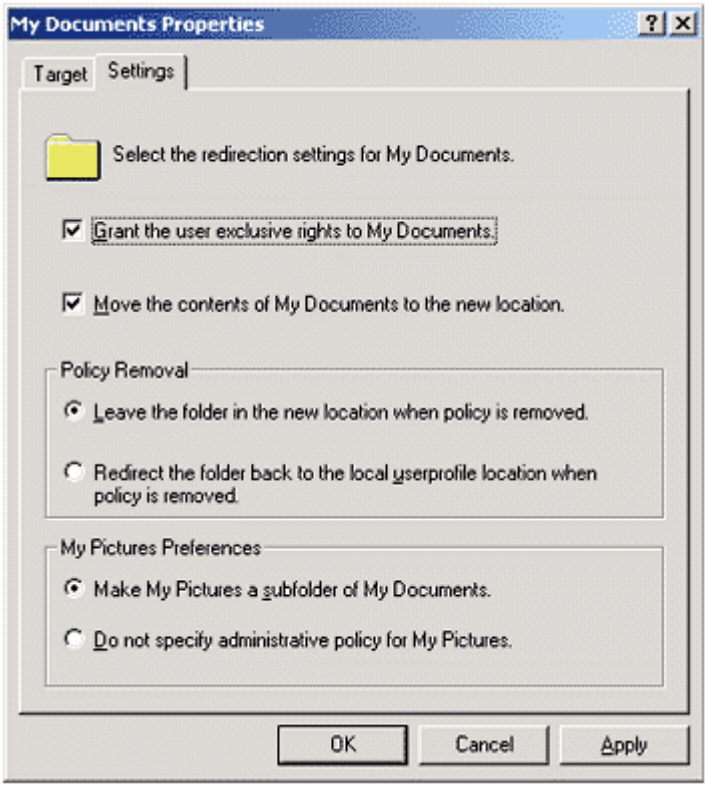

Figure 2 Specifying policy removal in a folder properties page.

Table 10 below summarizes what happens to Redirected Folders and their contents when the Group Policy object no longer applies.

Table 10 Summary of Redirected Folders

Folder Properties page settings		**When policy is removed:**
State of the Move the contents of special folder to the new location option	Setting selected for the Policy Removal option	
Enabled	**Redirect the folder back to the user profile location when policy is removed**	The special folder returns to its user profile location. The folder contents are copied back to the user profile location. The contents are not deleted from the redirected location. The user can continue to access the contents, but only on the local computer.
Disabled	**Redirect the folder back to the user profile location when policy is removed**	The special folder returns to its user profile location. **Note:** In this case, the folder contents are not copied or moved to the user profile location. As a result, the user can no longer see the contents.
Either Enabled or Disabled	**Leave the folder in the new location when policy is removed**	The special folder remains at its redirected location. The contents remain at the redirected location. The user continues to have access to the

		contents at the redirected folder.

Important Changing the redirection option to "Not Configured" **does not** redirect the folder to the local profile, this option means that Folder Redirection is not configured—*if a folder was previously redirected it will continue to be redirected to the previous location.* If an administrator wished to return the folder to the local user profile they should use the **Redirect to the local user profile** setting.

Use Offline Folder settings on a server share where the users data is stored.

This is especially useful for users with laptops. In particular, redirected folders of any type should be coupled with Offline Files.

Table 11 below details the recommended configuration to use for Offline Files.

Table 11 Recommended Configuration for Offline Files

Redirected Folder	Recommended Offline Folder Settings
My Documents	Auto-caching for documents or manual caching for documents (if you want users to have to manually make files and folders available offline).
My Pictures	Auto-caching for documents or manual caching for documents (if you want users to have to manually make files and folders available offline).
Application Data	Auto-caching for programs.
Desktop	Auto-caching for programs if the desktop is read only.

Always enable the Synchronize all offline files before logging off Group Policy setting.

Enabling this setting ensures that offline files are fully synchronized and that all the files in the user's redirected folder are available when they are working offline. If this setting is not enabled, the system only performs a quick synchronization, and as a result only recently used files will be cached.

Have My Pictures follow My Documents.

It is recommended that you configure the My Pictures folder to follow the My Documents folder, unless you have a compelling reason not to..

In general, accept the Default Settings for Folder Redirection.

If you are storing roaming profiles on the same server as Offline Files is enabled, Redirected Folders ensure that Offline Files are set to synchronize at logon and logoff.

When a share is unavailable, Offline Files considers the whole server to be unavailable until the offline cache is manually synchronized. Roaming profiles will not be synchronized with the server while Offline Folders considers the server to be unavailable. If you are using Offline Files in conjunction with Folder Redirection and roaming user profiles, for the best performance you should ensure that you leave the default setting of synchronizing Offline Files at logoff enabled.

Do not open multiple instances of Outlook 2000 when redirecting the Application Data folder.

If a user has redirected Application Data and has multiple instances of the Outlook® 2000 messaging and collaboration client running on different machines, and one of those instances is Outlook 2000, the user will experience poor performance opening e-mails. Outlook 2000 continually holds the file outcmd.dat open. This file stores information about toolbar customizations (such as position) made in Outlook. When another instance of Outlook attempts to access this file, it cannot do so since it is locked by the running instance of Outlook 2000. The second copy of Outlook keeps trying to access outcmd.dat many times, which causes a long delay when opening messages, replying to messages, and so on.

Note Outlook version 2002 (included in Office XP) doesn't hold outcmd.dat open—this is only a problem when running Outlook 2000 on one of the machines.

Related Technologies: Offline Files and Synchronization Manager

This section highlights technologies that complement the Folder Redirection feature.

Offline Files

Offline Files is a feature introduced in Windows 2000 that complements Folder Redirection. Offline Files let users disconnect from the network and work as if they were still connected. When the computer is offline, the files and folders appear in the same directory as they did online—as if they still resided in the same location on the network. This allows the user to edit files when they are disconnected. The next time they connect to the network, the offline changes are synchronized with the network share.

By using Offline Files, users can continue to work with a copy of network files even when they are not connected to a network. If your organization has mobile users with portable computers, Offline Files gives them access to their files when they are not connected to the network, and ensures that they are always working with the current version of network files. By using a cached version of the files, users can open and update files even when they are not connected to the network. Offline Files stores the data in the computer's cache to make network files available offline. The cache is a portion of disk space that a computer accesses when it is not connected to the network. The view of shared network items that you have made available offline remains as it is when connected, even if users lose a connection to the network or they remove a portable computer from the docking station. Users can continue to work with the Offline Files as they normally do when online. Users have the same access permissions to those files and folders as when they are connected to the network. When users dock a portable computer and the network connection is restored, any changes they made while working offline are updated to the network.

If two users on the network make changes to the same file, they can save their version of the file to the network, or keep the other user's version, or save both.

Shared files or folders on a Window Server 2003 or Windows XP-based network can be available offline. You can also make files available for offline use from any computer that is sharing files using server message block–based file and printer sharing, including Windows 2000, Windows 95, Windows 98, and Windows NT 4.0.

Note The Offline Files feature is not available on Novell NetWare networks.

When configuring a shared folder, you have the option of choosing whether all the files in the folder are automatically available offline, or whether a user must explicitly mark a file to be available offline.

Offline Files is a completely stand-alone technology, which means that you don't need to pair it with Folder Redirection and set up and configure network shares, but it works well if you do pair the two technologies. For example, if a shortcut to a file is available offline, that file is made available offline, but if a shortcut to a folder is available offline, the contents of that folder are not available offline. If you pair the two technologies, Offline Files and Folder Redirection, both the shortcut and the folder are available offline.

By using the manual caching for documents, users manually specify any files that they want available when they are working offline. Automatic caching for documents is recommended for folders that contain user documents. Opened files are automatically downloaded and made available when users work offline. Older copies of the files are automatically deleted to make room for newer and more recently accessed files. The automatic caching of programs is used for folders with read-only data or run-from-the-network applications. To ensure proper file sharing, the server version of the file is always opened.

Synchronization Manager

When using Offline Files and folders, users can synchronize all network resources by using the Synchronization Manager. The Synchronization Manager can be set to automatically synchronize some or all resources. For example, users can set certain files and folders to be synchronized every time they log on or off the network. The Synchronization Manager quickly scans the system for any changes, and if it detects changes, the resources are automatically updated. Only resources that have changed are updated—vastly speeding up the synchronization process.

Common Scenarios for IntelliMirror User Data and Settings Features

This section presents sample scenarios that illustrate some of the practical uses of the user data and settings management features in IntelliMirror.

The scenarios present a snapshot of a user’s computer in various uses and stages throughout a typical lifecycle. Each of the scenarios fits into an entire picture or can be seen as a separate event and shows how IntelliMirror benefits the entire organization by reducing the time and effort associated with maintaining the computing environment.

The following scenarios are explained:

- The New Hire
- The Laptop User
- Computer Replacement
- A Shared Computer Environment

The New Hire

One of the most critical and time consuming IT tasks is setting up the new hire with a computer. In an organization that is using IntelliMirror, the new hire logs on to a new computer and finds documents and shortcuts already on the desktop. There are shortcuts to common files, URLs, and folders that are useful to all employees (for example, the employee handbook, a shortcut to the departmental shared documents store, and a shortcut to the user’s departmental guidelines and procedures). Desktop options, application configurations,

Internet settings, and so on, are all configured to the corporate standard, ensuring that if the user needs to call the help desk, the support staff knows the configuration the user started with.

In this example, the user gets a pre-configured user profile that was set up for all new users, and was configured before the new hire logged on to the network. The administrator configured a computer to look and behave according to the corporate standard, and then using the User Profile[1] utility built into the System Control Panel application, copied the user profile to a Default User folder on the domain controller's Netlogon share. When the new hire logged onto the network for the first time, Windows copied this default profile to the local computer and used this profile as the basis for the new hire's profile. In addition to configuring the default profile the user received, the administrator also used Group Policy 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 Laptop User

A laptop user working at the office creates several documents and saves them to his or her My Documents folder. After saving documents, the user logs off, unplugs the laptop computer from the network and takes it home. While at home and off the network, the user continues to edit the documents saved earlier in My Documents.

The user returns to the office and logs on to the network. Since the user has done some offline work, a dialog box appears advising the user that data in My Documents has changed and is being synchronized with the network copy.

In this scenario, the user's My documents folder has been redirected to a network server, the documents are transparently saved to the network location and also saved in the local computer's cache (because the network folder is setup to be available offline), so that they are available when the computer is disconnected from the network.

The whole process can be transparent to the user; the experience is no different than saving documents to the local hard disk.

As soon as the user reconnects to the network, IntelliMirror attempts to reconnect to the network location of the redirected folders. When IntelliMirror reconnects, it determines if there are differences in the data between the local copy of the folder and the network copy. In this scenario, the user has made modifications to a document on the local computer. IntelliMirror identifies this change and prompts the user to update the version stored on the network.

Computer Replacement

The computer that the user is working on suddenly stops working because of a complete hardware failure. The user calls the support line, and about 20 minutes later a new computer, loaded only with the Windows XP Professional operating system arrives for the user. Without waiting for technical assistance, the user plugs in the new computer, connects it to the network, and boots it. The computer allows the user to log on to the corporate network, and the user finds that the desktop has the same appearance as the original computer that it replaced. It has the same color scheme, the user's preferred background picture is on the screensaver, and all the application icons, shortcuts, and favorites are present. More importantly, all the user's data files have been restored.

In a disaster recovery scenario, IntelliMirror assists in getting the user's computer replaced and running quickly and with the minimum of support. In this example, because the user was configured to use roaming user profiles, a copy of the user's working environment was safely stored on a network server. When the new computer arrived, the user was able to log on and the server copy of the user's profile was downloaded to the new computer. An administrator could also have used Folder Redirection to redirect the user's key folders such as My Documents and Application Data, to ensure that the user's documents were safely stored on the server.

A Shared Computer Environment

In this scenario, a user works in a department where the computer he or she uses may change from day to day—a call center or IT support environment, for example. The user is working on an important document late one night when the shift ends. The user saves the document and logs off the computer. When the user returns to work the next day, he or she logs onto the first available computer—a different computer from the one used the previous night. The user logs onto the network, and sees that the desktop has the same look and feel as the original computer. The user opens the My Documents folder on the desktop and finds the document exactly where he or she saved it and continues the work started the previous night.

In this example, the user was configured to use roaming user profiles, so that a copy of the user's working environment was stored on a network server. When the user logged onto the computer, the user's existing preferences, shortcuts and documents were copied to the local computer, so that the user could continue working as if using the original computer. A variation on this scenario is using roaming profiles in conjunction with Folder Redirection. Users can have the same work environment and access to the same documents on any

computer. Changes made on one computer are synchronized with the other computer the next time the user logs on.

Summary

By using IntelliMirror on both the server and client, administrators can protect and manage user data and settings. Non-recoverable data from local workstations can be copied to servers, where it can be easily backed up and centrally managed. Personalized data, applications, and settings can follow each user to different computers throughout the network. Administrators can easily replace faulty computers and restore all user data and settings on a new computer.

When fully deployed, IntelliMirror uses Active Directory and Group Policy for policy-based management of user desktops. A computer running Windows Server 2003, Windows XP, or Windows 2000 Professional desktop can be automatically configured to meet specific requirements of a user's business roles, group memberships, and location. Group Policy and the Active Directory are not necessary for every IntelliMirror feature. Some of the features can be set on the local level or through local polices. An organization can tailor use of IntelliMirror to its needs. When planning to use IntelliMirror, an organization should assess which features it needs and then implement the technology required.

This article addressed two of the key components for user data and settings management–User Profiles and Folder Redirection. It also provided an architectural overview of these features and presented sample scenarios.

Appendix

Group Policy Settings for Roaming User Profiles

Policy	Location in Group Policy Snap-in	Description
Limit profile size	User Configuration\Administrative Templates\System\User Profiles	Sets the maximum size of a roaming user profile and determines the system's response when a roaming user profile reaches the limit.
Connect home directory to root of the share	User Configuration\Administrative Templates\System\User Profiles	Restores the definitions of the %HOMESHARE% and %HOMEPATH% environment variables to those used in Windows NT 4.0 and earlier.
Exclude directories in roaming profile	User Configuration\Administrative Templates\System\User Profiles	Lets you add to the list of folders excluded from the user's roaming profile.
Delete cached copies of roaming profiles	Computer Configuration\Administrative Templates\System\ User Profiles	Determines whether the system saves a copy of a user's roaming profile on the local computer's hard disk drive when the user logs off. This policy and the related policies in this folder define a strategy for managing user profiles that reside on remote servers. Specifically, they indicate to the system how to respond when a remote profile is slow to load.
Slow network connection timeout for user profiles	Computer Configuration\Administrative Templates\System\ User Profiles	Defines a slow connection for roaming user profiles. If the server on which the user's roaming user profile resides takes longer to respond than the thresholds set by this policy permit, the system considers the connection to the profile to be slow. This policy and related policies in this folder together define the system's response when roaming user profiles are slow to load.
Add the Administrator security group to the roaming user profile share	Computer Configuration\Administrative Templates\System\ User Profiles	This policy allows an administrator to choose the same behavior as Windows NT 4.0, and have the administrators group given full control of the user's profile directories.

New for Windows XP and Windows Server 2003		
Prevent Roaming Profile Changes From Propagating to the server *New for Windows XP and Windows Server 2003*	Computer Configuration\Administrative Templates\System\ User Profiles	This policy determines if the changes a user makes to their roaming profile are merged with the server copy of their profile. If this policy is set, at login the user will receive their Roaming Profile, but any changes a user makes to their profile will not be merged to their roaming profile at logoff.
Only allow local profiles *New for Windows XP and Windows Server 2003*	Computer Configuration\Administrative Templates\System\ User Profiles	This setting determines if roaming user profiles are available on a particular computer. By default, when roaming profile users log on to a computer, their roaming profile is copied down to the local computer. Using this setting, an administrator can prevent users configured to use roaming profiles from receiving their roaming profile on a specific computer.
Prompt user when slow link is detected	Computer Configuration\Administrative Templates\System\ User Profiles	Notifies users when their roaming profiles are slow to load, letting a user decide whether to use a local copy or to wait for the roaming user profile. If you disable this policy or do not configure it, when a roaming user profile is slow to load, the system does not notify the user. It loads the local copy of the profile. If you have enabled the **Wait for remote user profile** policy, the system loads the remote copy without prompting the user.
Maximum retries to unload and update user profile	Computer Configuration\Administrative Templates\System\ User Profiles	Windows 2000 Only. Determines how many times the system tries to unload and update the registry portion of a user profile. When the number of trials specified by this policy is exhausted, the system stops trying. As a result, the user profile might not be current, and local and roaming user profiles might not match.
Do not detect slow network connections	Computer Configuration\Administrative Templates\System\ User Profiles	Disables the slow link detection feature. *Slow link detection* measures the speed of the connection between a user's computer and the remote server that stores the roaming user profile. When the system detects a slow link, the related policies in this folder tell the system how to respond.
Wait for remote user profile	Computer Configuration\Administrative Templates\System\ User Profiles	Directs the system to wait for the remote copy of the roaming user profile to load, even when loading is slow. The system waits for the remote copy when the user is notified about a slow connection, but does not respond in the time allowed.
Timeout for dialog boxes	Computer Configuration\Administrative Templates\System\ User Profiles	Determines how long the system waits for a user response before it uses a default value. The default value is used

		when the user does not respond to messages explaining that any of the following events has occurred: • The system detects a slow connection between users' computers and the server that stores the users' roaming user profiles. • The system cannot access users' server-based profiles when users log on or off. • Users' local profiles are newer than their server-based profiles.

Related Links

To learn more about how change and configuration management features were introduced in Windows 2000 Server, see the following Windows 2000 resources:

- Windows 2000 Management Services at: http://www.microsoft.com/windows2000/technologies/management/default.asp.
- Step-by-Step Guide to User Data and User Settings at http://www.microsoft.com/windows2000/techinfo/planning/management/userdata.asp
- Step-by-Step Guide to Understanding the Group Policy Feature Set at http://www.microsoft.com/windows2000/techinfo/planning/management/groupsteps.asp

For the latest information on Windows XP, check out our Web site at http://www.microsoft.com/windowsxp/default.asp.

[1] To access the User Profile utility, click **Start**, point to **Settings**, select **Control Panel**, select **System**, and then select the **User Profiles** tab in the **System Properties** dialog box.
