

*Windows 2000 Server***Chapter 6 - Managing User Data and Settings**

With the User Data Management and User Settings Management components of the IntelliMirror feature of Microsoft® Windows® 2000, you can centrally manage and control user desktops, settings, and data throughout your organization by storing data and settings on network servers and by synchronizing files. To design and configure these technologies, you should be familiar with the Active Directory™ directory service included with Windows 2000, Group Policy, and Microsoft Management Console (MMC). Additionally, you should have completed the following tasks outlined in this book:

- Identify your business, IT, and user requirements as discussed in "Meeting Your Desktop Management Needs with Windows 2000 Change and Configuration Management" and "Assessing Organization and User Needs" in this book.
- Identify how your network can best accommodate the technologies you want to deploy as described in "Preparing Your Network for CCM Technologies" in this book.
- Determine how you want to implement Group Policy in your network as explained in "How Group Policy Works" and "Developing a Group Policy Implementation Strategy" in this book.

In This Chapter

IntelliMirror User Data Management and User Settings Management Technologies

User Data and Settings Management Technologies

Planning and Design Considerations

Testing and Pilots

Implementation of User Data Management and User Settings Management

Sample Scenarios

Additional Resources

- For more information about Redirected Folders and Offline Files, see "Managing Files, Folders, and Search Methods," in the *Microsoft® Windows® 2000 Professional Resource Kit*.
- For more information about setting up a mobile computer using IntelliMirror technologies, see "Mobile Computing" in the *Windows 2000 Professional Resource Kit*.
- For more information about planning for and analyzing network bandwidth, see the book, *Optimizing Network Traffic: Notes From the Field*, Microsoft Press, Redmond, Washington, 1999.
- For more information about how specific components work, see Windows 2000 Server Online Help.

IntelliMirror User Data and User Settings Management Technologies

With IntelliMirror User Data and User Settings Management technologies, you can set up, manage, and control the availability of user data and personal settings. These technologies allow users to move from computer to computer and find that their data and personal settings are available to them. That is, users can log on to any computer and have access to their own data and preferences, without having to understand what is happening to make this occur.

In the course of doing their jobs, people frequently transition between being connected to a network and using their computers while disconnected from the network. User Data and User Settings Management make it possible for data and settings to be available to the user in either case. The increased availability of a user's data and personal environment is a result of storing that information on network servers, and synchronizing online files for offline use. This also means that when a computer becomes unavailable for any reason, IntelliMirror makes it possible for a new computer to replace the previous workstation with no loss of functionality.

Defining User Data and User Settings

To manage user data and settings, it is useful to understand the distinctions between data and settings. *User data* describes data files that are created by and used by a user. Examples of user data are word processing documents, spreadsheets, or graphics files. User data can be said to belong to the user. To be defined as user data, the data must reside independently on the user's computer or on a network share belonging to the user.

Less obvious forms of user data include Microsoft® Internet Explorer cookies and Favorites, or customized templates. User data is usually something that is hard to recreate — for example, a template that has undergone extensive design work and customization. Examples of user-accessed data that are *not* considered to be user data are database records that exist in a corporate database, and documents that are shared by many users and owned by none of them.

User settings are settings that the user has applied to an individual desktop or to applications. Generally, they include things like the customized toolbar settings in an application, desktop color schemes and icon layout, mouse pointers, and language options. Sometimes the distinctions between user data and settings are not clear. For example, in a custom dictionary the dictionary itself is user data, but the configuration within an application to use that specific dictionary is a setting.

As each technology is discussed throughout this chapter, these distinctions are emphasized to keep you aware of the differences between data, settings, and the tools that are used to manage each one.

Introduction to User Data and Settings Management Technologies

The technologies used to implement the IntelliMirror User Data and User Settings Management technologies are:

- Active Directory
- Group Policy
- User Profiles
- Folder Redirection
- Offline Files and Folders
- Synchronization Manager
- Disk Quotas
- Profile Quotas

Active Directory, the Windows 2000 directory service, stores information about all objects on the network in a central repository and provides the foundation upon which IntelliMirror is applied. The Active Directory structure defines domains, organizational units (OUs), groups, and users. This book does not describe how to create your Active Directory structure, but it is important to understand how IntelliMirror, especially Group Policy, relates to that structure. For more information about Active Directory and Group Policy see "How Group Policy Works" and "Developing a Group Policy Implementation Strategy" in this book.

Group Policy is the administrator's primary tool for defining and controlling how programs, network resources, and the operating system behave for users and computers in an organization. For more information about Group Policy see "How Group Policy Works" and "Developing a Group Policy Implementation Strategy" in this book. For information on how to apply specific Group Policy settings to configure User Data and Settings Management, see the Group Policy sections later in this chapter.

User Profiles define the Windows environment that loads when a particular user logs on. The user profile includes all the user-specific settings, such as screen colors, printer connections, desktop icons, mouse settings, and folder settings. A user profile is created the first time that a user logs onto a computer that is running Windows 2000 or Microsoft® Windows NT® 4.0. There are three types of user profiles: local, roaming, and mandatory.

A *local* profile, which is the default type, resides only on the computer at which the user is logged on. If the user logs onto another computer, a new profile is created for them at that computer, and they can see none of their customized settings from the first computer because that local profile exists only on the local hard drive of the first computer.

Best Practice Use a local profile for users who never connect over fast links, such as mobile users who log on over a dial-up line only.

A *Roaming User Profile* (RUP) is intended for users who use different computers within the organization's network, and who need to have their customized settings and data available to them at each computer they use. When using a RUP, the user's profile is copied to a specified server at logoff. When the user logs on to another computer in the network, the user profile information is copied from the server to that computer. When the user logs off the second computer, the profile is copied back to the server, thus maintaining the most current version of the profile on the server. While extremely useful for roaming users, RUPs are also beneficial for users who always use the same computer. For these users, RUPs provide a transparent way to backup the user's profile to a network server, thus protecting this important information against individual system failure. If a user's primary workstation ever needs to be replaced, the new computer receives the user's profile from the server as soon as the user logs on.

Best Practice Use RUPs for users who log on to multiple computers at once and need to have the same settings on each computer, or for users who tend to navigate to various computers during their workday and need to have the same settings wherever they go. RUPs are also useful for users who always use the same computer, so that current backups of their profile are saved.

A *mandatory* user profile is created and managed by only system administrators. It provides a way to force a standardized desktop setting to a user or group of users. With Windows 2000, the preferred way of establishing strict control over desktops is to use Group Policy rather than mandatory profiles.

Be aware that mandatory profiles create administrative overhead. Moving a user from a mandatory profile to another type of profile involves several manual steps, including renaming or deleting the profile on each client, editing the user's profile path, and renaming and moving the server copy of the profile. Mandatory profiles offer no flexibility to the administrator concerning how much of the desktop to control; once a mandatory profile is in place, you cannot change individual settings on a per-user basis. To remove a mandatory profile, the administrator might need to visit each computer, thus adding another administrative task.

Group Policy is easier and faster to apply and remove, and gives the administrator more precise control. The mandatory user profile feature remains in Windows 2000 only to provide compatibility with Windows

NT 4.0-based domains.

Best Practice If you need to provide managed desktop configurations for groups of users or computers, use Group Policy in Windows 2000 instead of mandatory profiles.

Folder Redirection 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, more likely, a directory on a network share. Users can work with files that exist in redirected folders on a server as if they were based on the local drive, and in general do not need to know that the files are not stored locally. For example, you can redirect the **My Documents** folder that is usually stored on the computer's local hard disk to a network drive, making the documents in the folder available to that user from any computer on the network. Folder Redirection provides a simple way to keep user data files backed up and secure on a centrally managed server. Combining folder redirection with roaming profiles gives the benefit of roaming profiles while keeping network traffic and logon times (due to synchronization of the profile) to a minimum.

The following five folders have been identified as the key folders that you can redirect to preserve important user data and settings. There are a number of advantages to redirecting each of these folders. The usefulness of each varies according to your organizations' needs. The folders that can be redirected are:

- **Application Data.** Applications often place large amounts of data in the Application Data folder in the user's profile. By redirecting the Application Data folder, users with roaming profiles can still have access to Application Data (such as a custom dictionary) without needing to download them at every logon.
- **My Documents.** This is the standard location where user documents are stored. By redirecting My Documents to a shared network server, important user data can be backed up as part of routine system administration, requiring no action on the part of the user. Also, the user is able to access all the documents from any computer.
- **My Pictures.** This is the default location for pictures and images in Windows 2000, and is normally contained within the My Documents folder. If My Documents is redirected, My Pictures is also redirected by default.

Best Practice Unless you have a compelling reason not to, configure the My Pictures folder to follow the My Documents folder.

- **Desktop.** Some organizations want to configure computers to have a common look and feel. By redirecting a group of users to a read-only copy of the desktop, you can ensure that all users share the same desktop. However, Group Policy and the Domain Default Profiles provide better ways to accomplish this goal.
- **Start Menu.** For compatibility with Windows NT 4.0, Windows 2000 allows you to use Folder Redirection to redirect the Start menu folder. For Windows 2000-based computers, do not use Folder Redirection to redirect the Start menu folder. Instead, use Group Policy to control what displays on the Start menu.

Offline Files and Folders that are shared can be made available to users when they are offline. Offline Files provides a way for users to work with a copy of network files even when the user's computer is not connected to a network. You can make files available for offline use from any computer that is sharing files using Server Message Block (SMB), including all versions of Windows as well as any non-Windows share that uses SMB.

If your organization has mobile users who use 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 most current version of the files. These benefits are also useful to onsite workers who might temporarily lose network connectivity due to server maintenance or technical problems.

Offline Files does not need to be paired with Folder Redirection, but the two technologies complement each other well. For example, if a folder is redirected and set to offline, that folder receives the benefits of being safely stored on a server drive, accessible by any computer the user logs on from, and also available on the user's computer in case of network inaccessibility.

Synchronization Manager synchronizes Offline Files with local copies of the same files. For more information on the various ways to initiate and control synchronization, see Synchronization Manager later in this chapter.

Disk Quotas control the amount of disk space that is occupied by user data. Disk quotas allow you to prevent users from using too much disk space. An event is created in the event log when a user is within range of exceeding a predefined limit.

Profile Quotas can be controlled by a Group Policy setting. This allows you to prevent users from having roaming profiles that take up too much server disk space, or that are too large to roam effectively. When a user's profile exceeds the defined limit, they receive a message that instructs them to reduce the size of their profile. The user cannot log off until their profile has been reduced to the allotted size.

Using Components in Combination

The previously listed IntelliMirror components can be used either separately or together to meet your objectives for managing user data and settings. When fully deployed, these components use Active Directory and Group Policy to provide policy-based management of users' desktops. Group Policy is the

primary means used to define and configure most user settings. Active Directory provides the structure within which the settings are applied.

If you have a Windows 2000 domain, it is strongly recommended that you take advantage of Active Directory and Group Policy to deploy these settings. Redirecting folders without Active Directory is difficult because you cannot use Group Policy to do so; to redirect folders without Active Directory requires manipulating the registry on the client. However, if you do not have a Windows 2000 domain, you can still redirect folders. It is also possible to redirect My Documents manually if you do not have Active Directory set up on your network. Roaming User Profiles and Offline Files do not require the presence of Active Directory or Group Policy.

Solving Problems with User Data and User Settings Technologies

Deployment of a new technology is intended to resolve a business or technical problem. This section describes problems that can be solved or situations that can be improved by using User Data and Settings Management. Here are some common problems that these IntelliMirror technologies can help you solve.

- **Disconnected users cannot access necessary network files.** Users often need access to some files even when the network is inaccessible. Offline files and Folder Redirection each provide ways to keep data available to users even when disconnected. (Note: these won't help when the user is disconnected and needs access to .pst and other files that have their own synchronization methods, or if the user needs access to shared, multi-user databases.)
- **Important user data and user settings are stored on workstations, making it difficult to backup and restore this information.** Administrators need an easy way to back up user information that typically resides on individual hard disks. This can be resolved by using Roaming User Profiles and Folder Redirection. The combination of these two technologies ensure that user data and settings are always stored on a network drive so they can be easily backed up along with other important network data.
- **Exchanging computers for upgrades or when equipment fails.** When computers need repair or upgrading, organizations need to quickly replace them to get users working productively. With Roaming User Profiles and Folder Redirection, user data and settings are located on a network drive. Once the new computer is in place and the user logs on, their profile and user data is immediately available to them.
- **User confusion results in support calls.** Changes to a user's environment can result in additional support calls. When users encounter the same environment on any computer they log on to (enabled with Roaming User Profiles and Folder Redirection), they do not become confused or distracted by unexpected screens; therefore, support calls and costs are reduced.
- **Some users use too much shared disk space.** When user data and settings are stored on a server, some users take up more disk space than can reasonably be allotted to them. You can use disk quotas to control how much shared disk space each user consumes.
- **Budgeting requires that network costs be distributed across corporate cost centers.** Organizations often distribute the costs of their computer equipment across various cost centers. To do so judiciously, they need to track the resources used by each cost center. Disk quotas provide a way to accurately track the amount of shared (network) disk space that is used by each user, and therefore, by each department.
- **Need to determine additional resources.** Disk quotas provide important statistical data that can be used to determine network upgrades and equipment purchases.
- **Users want their own data and settings to appear on any computer they log on to.** Roaming User Profiles provides a way to do this. Once RUPs are assigned to users, any computer they log on to will receive their personalized settings.
- **Administrators need to manage and secure desktops.** Group Policy provides the ability to control the desktop or workstation environment. For example, policy settings can standardize a desktop background, a screen saver, or to modify the Start menu. Some situations require tightly controlled desktops or a standardized desktop for all users on all computers. In a classroom setting, for example, you can use the Default Domain Profile and Group Policy to mandate and preserve standardized settings.
- **When users work both offline and online, they can become confused about which file has the most recent changes.** This is particularly difficult to track when multiple people are accessing the same files. You can reduce confusion by using Offline Files with Synchronization Manager.

User Data and Settings Management Technologies

When planning your deployment, it is important to have a conceptual overview of how these technologies work together. This background information will assist you in determining your use of User Profiles, Folder Redirection, and Offline Files.

User Profiles

A User Profile is comprised of a registry hive and a set of folders stored in the file system. The registry is a database used to store computer- and user-specific settings; these databases are called *hives*, and can be

saved as files. These files can then be reloaded for use as necessary. User Profiles take advantage of the hive feature to provide roaming profile functionality.

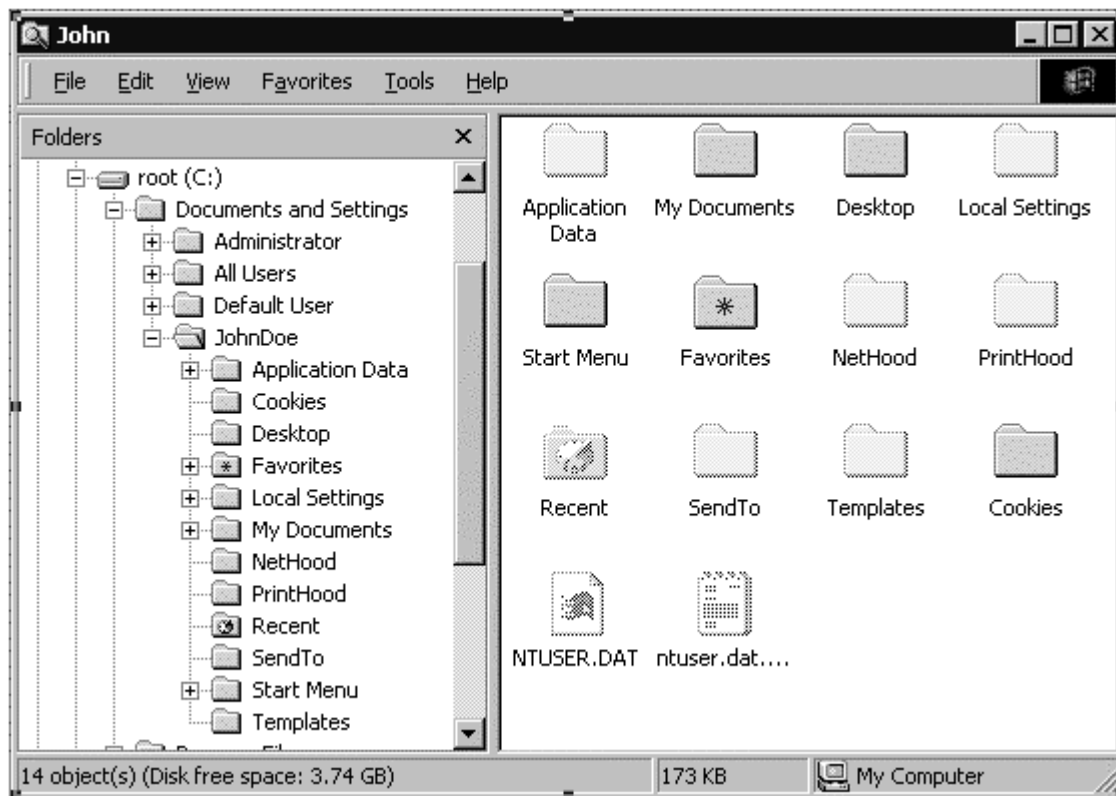
The User Profile registry hive is the NTuser.dat in file form, and is mapped to the HKEY_CURRENT_USER subtree in the registry when the user logs on. The NTuser.dat hive maintains the user's environment preferences when the user is logged on. It stores those settings that maintain system settings, Control Panel configurations unique to the user (such as the desktop color and screensaver), and some settings specific to applications. The profile folders store shortcut links, desktop icons, Start menu, some application settings, and so forth. Together, the registry hive and profile folders record all user-configurable settings.

Among the user's registry settings stored in the NTuser.dat file are:

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

User Profile Contents

Figure 6.1 shows the structure of the user profile:



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.1 User Profile Structure

Table 6.1 lists the default RUP behavior for user profile folders, and states whether these folders can be redirected using Group Policy.

Table 6.1 Profile Folders Default Behavior

Folder Name	Description	Roams with profile by default	Can be Redirected using Group Policy
*Application Data	Per-user roaming application data. This folder stores application state data, such as toolbar settings and other non-registry-based settings. Application vendors decide what to store here.	Yes	Yes

Cookies	User's Internet Explorer cookies	Yes	No
Desktop	This folder contains user-specific contents of the desktop. The size of this folder varies widely depending on usage. It is recommended that the desktop be included in RUPs unless users save large or many data files on the desktop. It is also recommended that users be trained to save shortcuts only on the desktop, instead of the files themselves. If many files are saved to the desktop, consider redirecting this folder instead of including it in RUPs.	Yes	Yes
Favorites	This folder contains a user's Internet Explorer favorites. It is typically a very small folder.	Yes	No
*Local Settings	This folder contains temporary files and per-user non-roaming application data. It is a container for application settings and data that do not roam with the profile. These are usually computer-specific, or too large to roam effectively. Application vendors decide what data to store in this folder.	No	No
*History	This folder is a subfolder under Local Settings, and it contains the Internet Explorer history. Because it is part of Local Settings, it neither roams nor redirects.	No	No
*Temp	This folder contains temporary files and is part of Local Settings.	No	No
*Temporary Internet Files	This folder contains the Internet Explorer offline cache. By default, its size is set to 10% of the drive although this setting is user configurable. Part of Local Settings.	No	No
My Documents	This folder is the new default location for any documents that the user creates. Applications need to be written to save files here by default. This folder is usually too large to roam. As a best practice, it is recommended that you always redirect this folder and mark it to be available offline.	Yes	Yes
My Pictures	This folder is the new default location for user's graphics files. Since My Pictures is a subfolder to My Documents, it needs to follow the redirection and offline files settings that you establish for My Documents.	Yes	Yes
*NetHood	This folder contains shortcuts to Network Neighborhood items.	Yes	No
*PrintHood	This folder contains shortcuts to printer folder items.	Yes	No
*Recent	This folder contains shortcuts to the most recently used documents, such as Most Recently Used (MRU) lists in applications.	Yes	No
*Send To	This folder contains shortcuts to document storage locations and applications.	Yes	No
Start Menu	This folder contains shortcuts to program items and is typically small in size. It must be included in RUPs because it is a small amount of data that is an important part of the user's environment. In general, do not redirect this folder, because that would trigger network traffic every time the user clicked the Start button on the desktop. If you want a group of users to have the same menu, redirect the menu to a read-only location and cache it with offline files.	Yes	Yes

*Templates	This folder contains shortcuts to per-user customized template items and is usually fairly small.	Yes	No
------------	---	-----	----

(Folders with a * are hidden by default.)

Caution Users must not store Encrypting File Systems (EFS) encrypted files in their roaming profile. The combination of RUPs with EFS is not supported under Windows 2000. If a roaming profile contains encrypted files, it ceases to roam and the user gets an error message. Also, do not encrypt the Temp directory. Encrypting the Temp directory can cause additional errors.

Non-roaming Folders

A non-roaming folder is a local settings folder within the user profile that is *not* copied during logon or logoff sessions, and that can store non-roaming data for each user. With it, operating system components and other applications can store non-roaming data. Roaming user profiles are copied from the server to the client when the user logs on, and copied back when the user logs off. Windows 2000, and Windows NT 4.0 Service Pack 4 and later include this per-user local settings folder.

For example, Internet Explorer can store a user's Favorites in the roaming portion of the user profile, and store the temporary Internet files in the local, non-roaming portion of the user profile. By default, the Temp and Temporary Internet Files folders are excluded from the Roaming User Profile. You can configure additional folders to *not* roam using Group Policy (found in the Group Policy snap-in under **User Configuration\Administrative Templates\System\Logon/Logoff\Exclude directories in roaming profiles**). However, you cannot force the Temp and Temporary Internet Files folders to roam using Group Policy.

Roaming User Profiles with Windows 2000 and Windows NT 4.0

Roaming User Profiles are for users who need to have their customized settings and data available to them on any computer they use. In general, the implementation of RUPs in Windows 2000 is similar to the Windows NT 4.0 implementation. Note that the default location of user profiles has been changed for Windows 2000, to allow you to secure the operating system folders without adversely affecting user data.

Profiles on a Windows NT 4.0-based computer are stored inside the system directory, at %SYSTEMROOT%\profiles folder (typically WINNT\profiles). On a clean installed Windows 2000 computer, profiles are stored in the %SYSTEMDRIVE%\Documents and Settings folder. If you upgrade a computer from Windows NT 4.0 to Windows 2000, the profile location remains %SYSTEMROOT%\profiles. The profile location can be changed only at setup time in Windows 2000.

Some older applications use hard-coded paths for determining where a user's local (cached) profile is located on the local computer. When a user roams between computers running Windows NT 4.0 and Windows 2000, problems can occur if a program is hard-coded to find the user's locally cached profile in the %SystemRoot%\Profiles folder. If users roam between clients running Windows NT 4.0 and Windows 2000 operating systems, set the profile path to be the same on both clients, to minimize the chance of problems.

If roaming profiles are stored on a Windows NT 4.0 share, ensure that users are given Full Control share permissions. Not having the share permissions set to Full Control can result in profiles not synchronizing.

Best Practice If many of your users roam between Windows NT 4.0 clients and Windows 2000 clients, consider setting the profile location to the same as on Windows NT 4.0 during Install on Windows 2000. You can do this by using unattend.txt files to customize installation.

Table 6.2 shows the location of user profiles for each possible installation scenario.

Table 6.2 User Profile Locations

Windows 2000 Installation Type	Location of user profile
Windows 2000 Clean installation	%SYSTEMDRIVE%\Documents and Settings; for example, C:\Documents and Settings
Windows 2000 upgrade from Windows NT 4.0	%SYSTEMROOT%\Profiles; for example, C:\WinNT\Profiles
Windows 2000 upgrade from Microsoft® Windows NT® 3.51	%SYSTEMDRIVE%\Documents and Settings; for example, C:\Documents and Settings
Windows 2000 upgrade from Microsoft® Windows® 95 or Microsoft® Windows® 98	%SYSTEMDRIVE%\Documents and Settings; for example, C:\Documents and Settings

Limiting Profile Size

Profile quota size is managed using the Group Policy snap-in (found at **User Configuration\Administrative Templates\System\Logon/Logoff\Limit Profile Size**). In general, set profile limits only if users tend to put large quantities of data onto the desktop. If an individual's user profile exceeds the allocated size, the user cannot log off until they reduce the size of their profile.

If you are combining Roaming User Profiles with Folder Redirection of My Documents, it is best to not use quotas on the profile. This is because when My Documents is removed from the profile, the remaining items in the profile are written by the operating system and applications. The user is not aware of these, and will find them difficult to remove without damaging their application settings.

You can set a policy to remove cached versions of the profile on logoff (found in the Group Policy snap-in at **Computer Configuration\Administrative Templates\System\Logon\Delete cached copies of roaming profiles**). This is practical if you are concerned with disk size on a multi-user computer — for example, a public computer where many users can log on.

How User Profiles Are Created

A user profile is created the first time a user logs on to a Windows 2000-based or Windows NT-based computer. How a user gets their profile is dependent upon the type of profile they are configured to use. The following section describes profile creation.

How a New User Gets a Local Profile

1. The user logs on.
2. Windows checks the list of user profiles located in HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows NT\CurrentVersion\ProfileList registry subkey to see if a local profile exists for the user. Because this is a new user, no profile exists.
3. Because a local profile is not found, and the computer is part of a domain, Windows checks to see if a domain default profile exists in a folder named "Default User" on the domain controller NETLOGON share. (See How to Configure a Domain Default Profile in the Implementation section of this chapter for instructions on how to create a domain-wide default profile.)
4. If the domain default profile exists, it is copied with the username to a folder on the local computer under %SYSTEMDRIVE%\Documents and Settings\. For example, a new user with the username Kevin will have his profile copied to his local computer under %SYSTEMDRIVE%\Documents and Settings\Kevin.
5. If a default domain profile does not exist, then a default profile is copied with the new username from the %SYSTEMDRIVE%\Documents and Settings\Default User folder to a folder on the local computer under %SYSTEMDRIVE%\Documents and Settings\. Using the previous example, this would be %SYSTEMDRIVE%\Documents and Settings\Kevin.
6. The user's registry hive (NTuser.dat) is mapped to the HKEY_CURRENT_USER subtree in the registry.
7. When the user logs off, his or her profile is saved to the %SYSTEMDRIVE%\Documents and Settings\%USERNAME% directory on their local hard disk. The next time the user logs on, this profile is loaded as described in step 2 above.

How an Existing User Gets a Local Profile

1. The user logs on.
2. Windows checks the list of user profiles located in the HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows NT\CurrentVersion\ProfileList registry subkey to get the path to the user's profile.
3. The user's registry hive (NTuser.dat) is mapped to the HKEY_CURRENT_USER subtree in the registry.
4. When the user logs off, his or her profile is re-saved to the local hard disk of their computer. The next time the user logs on, this profile is loaded as described in step 2 above.

Note If a user from a different domain logs on to the same Windows 2000 computer using the same down-level account name (for example, Jay), and the security identifiers (SIDs) of the two Jay user accounts are not identical, a new folder is created. This folder has an extension denoting how many times the profile experienced this exception, (as shown below). This occurs if a user account is deleted and later re-created, or if the system is re-installed.

- Original user account: %SYSTEMDRIVE%\Documents and Settings\Jay
- First additional user account: %SYSTEMDRIVE%\Documents and Settings\Jay [DOMAIN].000
- Second additional user account: %SYSTEMDRIVE%\Documents and Settings\Jay [DOMAIN].001

How a New User Gets a Roaming Profile

1. The user logs on.
2. Windows checks the list of user profiles located in the HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows NT\CurrentVersion\ProfileList registry subkey to see 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 see if a domain wide default profile exists in a folder named "Default User" on the domain controller NETLOGON share.
3. If this profile exists it is copied with their username to a folder on the local computer under %SYSTEMDRIVE%\Documents and Settings\.
4. If a default domain profile does not exist, then the local default profile is copied with their username

from the %SYSTEMDRIVE%\Documents and Settings\Default User folder to a subfolder on the local computer under %SYSTEMDRIVE%\Documents and Settings\..

5. The user's registry hive (NTuser.dat) is loaded and mapped to the HKEY_CURRENT_USER subtree in the registry
6. When the user logs off, his or her 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 below for details).

How an Existing User Gets a Roaming Profile

1. The user logs on.
2. Windows checks the list of user profiles located in the HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows NT\CurrentVersion\ProfileList registry subkey to get the path to the user's locally cached profile.
3. The contents of the local cached profile are compared with the copy of the profile on the server, and the two profiles are merged.
4. The user's registry hive (NTuser.dat) is mapped to the HKEY_CURRENT_USER portion of the registry.
5. When the user logs off, his or her 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 the following section on the Merge Algorithm for details).

Merge Algorithm

To improve user experience of roaming profiles using Windows NT 4.0, Windows 2000 roaming profiles have a new algorithm to synchronize copies of a profile. Windows 2000 solves problems that can occur when a user logs into two different computers simultaneously.

The Windows NT 4.0 algorithm worked well in the most common case where users logged on to only a single computer. However, when users logged onto multiple computers at the same time, they sometimes experienced unexpected results due to each computer's assumption that it had the master copy of the profile.

In Windows 2000, the algorithm now supports the merging of user profiles at the file level, and support was added so that what was written last is what is saved.

Overview of the Windows NT 4.0 Algorithm

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

- The user logs on to computer A, the primary computer.
- The roaming profile is Xcopied from the server to the local profile location. If the server version of the profile is newer than the local copy, the local profile is deleted and replaced with the server copy.
- The user creates documents, changes colors, and so on. All of these changes are stored in the local profile location.
- As the user logs off the computer, the profile is Xcopied from the local profile location back to the server location. If the server version of the profile is older than the local copy, it is overwritten.

Windows NT 4.0 Merge Algorithm Issues

When using Windows NT 4.0, a problem arises if the user has 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 computer A
5. The user logs off computer B

The document that the user created in step 3 is deleted because, from the perspective of computer B, it has the master profile. Any extra files on the server are deleted to preserve the local profile as the master profile.

A similar problem can occur when files are modified. For example, suppose that the user has a document called example.doc in the 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 and stores 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.

Windows 2000 Merge Algorithm

Windows 2000 merges user profiles at the file level. This means that the merged profile contains the superset of files that are in the local and server copies of the profile. If the same file exists in both the local and server copies of the profile, the file that was modified most recently is used. This means that new files will not be deleted and updated versions of existing files will not be overwritten. This resolves both problems described above.

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 compare the local profile against the server profile to determine which files are new and which files have been deleted in the local profile.

For example, if the server profile contains a document called Review.doc and this file does not exist in the local profile, it is either a new file created from a different computer, or it was in the original local profile and the user deleted it. Because the system knows what time the new profile was loaded on the local computer, it can compare that time 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 load time, Review.doc will be deleted. Because it was copied to the local computer at load time, the user has deleted Review.doc during the most recent logon session.

In addition, some files might be removed from the local copy of the profile 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 make sure that the files are properly deleted, the local version of the profile is synchronized with the server copy of the profile when a user logs on. All files in the local profile that are not present in the server and that were not modified since the last logoff time are removed. With these changes to the algorithm, Windows 2000 can merge user profiles.

Folder Redirection

Folder Redirection is an extension of Group Policy that processes the group policy settings that apply to the user at logon time. The folder is redirected to the specified location only if the user belongs to the security group represented by the corresponding group SID. For more information and recommendations for folder redirection, see Table 6.1 Profile Folders Default Behavior.

If the folder redirection policy was created using basic settings (see Folder Redirection Implementation), this consists of the SID for the group Everyone. If advanced redirection settings are applied, then the group policy will contain one entry per security group. Because the folder redirection extension parses redirection settings in order, if the user belongs to multiple security groups, then the folder redirection extension uses the redirection settings for the first group to which the user was added. Each time the user logs on, the folder redirection client extension checks to see if any redirection policies have been changed or added.

To prevent a folder from being redirected to an invalid location, the folder redirection client always ensures that the destination exists. If the destination folder does not exist, it is created. When the redirection client creates the destination folder, it also sets the user as the owner of the folder.

The folder redirection client prevents the folder from inheriting the discretionary access control list (DACL) from its parent. This ensures that another user is not able to gain access to this user's folder by pre-creating the parent of the folder or by adding special access control entries (ACEs) to the DACL of the parent folder. By default, even administrators do not have access to a user's redirected folders. To ensure the best operation of folder redirection, ensure that users have Full Control share permissions. Security is enforced by means of NTFS permissions. For more information about the default and minimum permissions, see Table 6.5 NTFS Permissions Needed for Root Folder later in this chapter.

If the destination folder already exists, a check is performed to determine whether the user is the owner of the destination folder. If the user is not the owner of the destination folder, the redirection will fail.

Immediately before physically moving the files, two important checks are performed:

- *Check to see if the source and destination paths are identical.* If the source and the destination are

actually the same location, no files are moved.

- *Check to see if the destination is a subfolder of the source.* If the source path is a parent folder to the destination folder, then any attempt to recursively copy the source to the destination will result in an infinite recursion. To avoid this, redirection is aborted when such a situation is detected.

Moving Redirected Files From One Network Share to Another

When an administrator moves a redirected folder from one network share to another, the following steps are performed:

First, all files are first copied to the destination, and then they are deleted from the source. The files are not deleted from the source until all the files are successfully copied over to the destination. If a folder is being moved from one share to another share *on the same server*, the redirection might fail in certain cases, with an error indicating a lack of space on the disk even if the user seems to have sufficient quota on the server.

For example, if a user has a quota of 100 MB on the server (with the default option on the quota page checked to **Deny disk space to users exceeding quota limit option**), and the user's folder takes up 60 MB on the server, then the copy phase will require an additional 60 MB on the server — that is, a total of 120 MB, which is more than the user's quota. In this case, the redirection will fail due to a lack of disk space. For this failure to happen, both the source and destination shares must be on the same server, and the folder must use up more than half of the user's quota of disk space.

Additional considerations to note when moving redirected folders:

- In case of an error during the copy phase, redirection is aborted, but no attempt is made to remove any files that were successfully copied to the destination.
- Errors that occur during the delete phase are ignored and do not prevent the redirection from succeeding.
- If a file at the destination has the same name as a file at the source, the file that was modified more recently is preserved.

Files are not deleted from the source when you move files from a network share to a local computer.

Offline Files

Offline Files, which are shared files or folders available to users when they are offline, works by storing specified network files in the local computer's cache. The database containing information about Offline Files resides in the hidden system folder called %systemroot%\CSC. The Client Side Caching (CSC) directory contains all offline files requested by any user on the computer.

Note On a file allocation table (FAT) file system or a FAT file system converted to NTFS, users might be able to read information that is cached by other users in the %systemroot%\CSC directory. Do not move or delete files directly from the CSC directory. For instructions on how to safely delete cached files, see "Managing Files, Folders, and Search Methods" in the *Windows 2000 Professional Resource Kit*.

You can use Offline Files Cache Mover (cachemov.exe), available in the Windows 2000 Professional Resource Kit, to change the cache location. The default cache size is set to 10 percent of available drive space. This setting can be adjusted in the **Offline Files** tab of **Folder Options**.

Offline files and folders do retain file and system permissions, but do not retain encryption. If a user encrypts a file or folder on a network share using EFS, and then makes the file or folder available offline, the offline version of the file or folder is not encrypted. Additionally, you cannot encrypt the Offline Files folder itself.

Note Do not set up Offline Files on a Distributed File System (DFS) share. Windows 2000 does not support this configuration.

By default, *.slm, *.mdb, *.ldb, *.mdw, *.mde, *.pst, and *.db? files are not synchronized because they are large or have their own internal synchronization mechanisms. You can override these defaults through Group Policy, but be aware that doing so can cause very long synchronization times, or synchronization conflicts resulting in data corruption.

If you store roaming profiles on the same server as cached and redirected folders, make sure that Offline Files are set to synchronize at logon and logoff. When a share is unavailable, Offline Files regards the whole server as unavailable until the offline files are manually synchronized. As long as Offline Files perceives the server as offline, roaming profiles are not synchronized because both technologies use the same redirector. For the best result, leave the default setting of **Synchronize Offline Files Logoff** enabled.

Do not use Offline Files to cache roaming profiles. Make sure that you turn off caching for shares where roaming user profiles are stored, or synchronization problems can occur, as both Offline Files and roaming profiles try to synchronize the files in a user's profile. This is not applicable for redirected folders because, unlike RUPs, redirected folders do not have a synchronization mechanism.

When configuring a shared network folder, you are offered several types of caching from which to choose. The cache type is a property of the network share, not the client workstation. The following table shows the recommended folder configuration for Offline Files.

Note A non-Windows 2000 share (Windows NT 4.0, Windows 95, or Windows 98) set for Automatic caching behaves like the Manual Caching for Documents setting.

Table 6.3 Offline Files Folder Recommendations

Redirected Folder	Recommended Offline File Settings
My Documents	Auto-caching for Documents or Manual Caching for documents
My Pictures	Auto-caching for Documents or Manual Caching for documents
Application Data	Auto-caching for Programs
Desktop	Auto-caching for Programs if the desktop is read only

Manual Caching for Documents

The Manual Caching for Documents is the default setting for a share, and also the setting for shares on servers running Windows NT 4.0, Windows 95 or Windows 98. This setting makes a file or a folder available on a user's computer when that computer is offline. This happens only when the file is manually *pinned* to the user's computer. *Pinning* refers to the act of explicitly marking a file for offline use; the user can right-click the file name and then click **Make Available Offline** to accomplish this. Files can also be pinned by an administrator using Group Policy (located in the Group Policy snap-in at either **Computer Configuration** or **User Configuration\Administrative Templates\Network\Offline Files\Administratively assigned offline files**).

Pinned files are treated as Xcopied files, and are not counted towards the local cache size limitation. When a file is pinned, it is deleted from the local computer only when the user deletes it. If a file or folder is *not* pinned to the user's computer, it is not guaranteed to be available offline. However, non-pinned files can be available offline:

- If they are cached through one of the automatic caching mechanisms described in the following sections.
- If they are newly created within the manual cache share.

Newly created files are always cached, even if the share in which they are stored is set to Manual caching. This is because most applications do the following when they modify a file:

1. Read the file.
2. Create a new temporary file and write all the changes to it.
3. Rename the original to a temporary file.
4. Rename the new file to the original name.
5. Delete the temporary file.

Offline Files caches the files created in step 2, so that step 4 works. Therefore, Offline Files caches all files that are created on this computer so that applications continue to work. A new file created in this manner is pinned if it subsequently replaces a file that was already pinned (in step 4 above). A new file that does not replace a pinned file is cached, but not pinned.

Note This scheme saves bandwidth by saving the data created in step 2. This way the data does not have to be obtained from the network more than once.

You can pin folders as well as files. When you pin a folder, all files in the folder are also pinned. If you pin a folder that contains subfolders, you are given the opportunity to pin the subfolders at the same time.

Enabling the Group Policy setting **\Local Computer Policy\Administrative Templates\Network\Offline Files\Subfolders always available offline** causes subfolders to be automatically pinned.

If you later create a new file in a pinned folder, the new file is automatically pinned. However, if you later create a new subfolder in a pinned folder, the new subfolder is not automatically pinned unless you enable the Group Policy setting defined in the preceding paragraph.

Manual caching is recommended for users who frequently work on their mobile computer without a network connection, but still need access to files on the network. In this case, the administrator or the user can manually pin folders to the user's mobile computer, making those folders available when the user is disconnected from the network. Automatic caching is not ideal in this case, because the files in the network folder are not stored locally unless the mobile computer user opens each file while connected.

Automatic Caching for Documents

Automatic caching for documents means that every network file a user opens is downloaded and cached — this includes both documents and executables. Automatic caching is recommended for folders that contain user documents. You can manually pin a folder or a file even when the folder or file has been configured for automatic caching. In this case, pinning forces the file or folder to be stored. Therefore, pinning has precedence over automatic caching.

Automatic caching for documents does not make every file in the shared folder offline: only files the user

has opened. *In a share that is set for automatic caching, files that have not been opened are not available offline.*

Automatically stored files might not always be available in the local cache because Windows 2000 might remove (purge) them from the cache when the cache becomes full. Windows 2000 selects files for purging on the basis of how often they are used. If the quota for offline files is exceeded, less frequently used copies of the files are automatically deleted from the local cache to make room for newer and more recently accessed files. The server version is not deleted in this case, nor are locally cached files deleted if they contain offline changes.

The local cache quota can be found and changed by opening the cached folder, clicking **Tools**, clicking **Folder Options**, and then clicking **Offline Files**. The default quota size is 10 percent of the local drive. You can store up to 2 GB of manually cached files per computer if that much space is available.

Automatic Caching for Programs

Automatic caching for programs is identical to automatic caching for documents, except for executable files (any file opened for execution, typically *.exe, *.dll). This caching option is recommended for shared folders containing applications that are run over the network. When the share is set to automatic caching for programs and a cached file is opened for execution, if the local copy of the file is up-to-date (identical to the server copy), then the file is opened locally only. The server file is not opened at all, thereby reducing network traffic. In contrast, if a cached document is opened for read/write, and the cached copy is up-to-date, then the file is opened both locally and on the server. Reads are satisfied from the local cache and writes go to both the local copy and the server copy. In other words, for all files that are not opened for execution, the results of Automatic caching for programs are just like automatic caching for documents.

Note Opening the file on the server ensures proper sharing semantics. Sharing semantics are not maintained on files opened for execution because there are no outstanding opens against those executables.

Synchronizing Offline Files

When synchronizing offline files, two types of synchronization can be affected: quick synchronization, or full synchronization. For more information on how to synchronize offline files and folders, see Offline Files and Synchronization Manager later in this chapter. The *full* synchronization option synchronizes every file in the local cache with the network share. The *quick* synchronization option only verifies that all files in the cache are complete; it does not verify that they are up-to-date.

For example if you have an auto-cached share containing a 10 MB file named example.doc, when the client opens example.doc for the first time, a directory structure is created for the file in the client database, and the file is marked as incomplete. At this point, a directory entry with the file properties exists on the client, and example.doc is a 0 byte length file. Example.doc is then read from the server in increments. If the application is closed before the entire file is read, the file is saved in an incomplete manner in the local cache. Incomplete files are not available offline. Quick synchronization completes such files.

By default, full synchronization is performed at logoff. If full synchronization at logoff is turned off, then the system automatically performs a quick synchronization. Whenever you manually pin a file, a quick synchronization is automatically performed.

Table 6.4 Synchronization Options and Results

Synchronization commands and options	Send offline changes to the network resource?	Receive cached files from the network resource?
Automatically synchronize the selected items when users log on to their computers	Yes	No
Synchronize all offline files before logging off is enabled	Yes	Yes (Full Synchronization)
Synchronize all offline files before logging off is disabled	No	Yes (Quick Synchronization)
Synchronize the selected items while users computers are idle	Yes	Yes (Quick Synchronization)
Scheduled	Yes	Yes (Full Synchronization)
Clicking Synchronize from the Start menu or on the Tools menu	Yes	Yes (Full Synchronization)
Clicking Synchronize on the File menu	Yes	Yes (Full Synchronization)
Clicking Make Available Offline on the File menu	No	Yes (Quick Synchronization)
From the Offline Files icon in the Status area of	Yes	No

the task bar		
--------------	--	--

The files are synchronized:

- When the user manually forces synchronization
- At logoff
- At intervals specified in Synchronization Manager later in this chapter

Synchronizing Offline Files Over a Slow Link

For Offline Files and synchronization, a slow link is defined as any connection that operates at 64 Kbps or slower, which is the speed of a single-channel Integrated Services Digital Network (ISDN) connection. Therefore, most modem connections through telephone lines are considered slow link connections with regard to Offline Files synchronization.

If necessary, this definition can be overridden by editing the following registry entries:

```
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \NetCache \SlowLinkSpeed
HKEY_LOCAL_MACHINE \Software \Microsoft \Windows \CurrentVersion \NetCache \SlowLinkSpeed
```

The value of the entry in HKEY_LOCAL_MACHINE overrides the value of the entry in HKEY_CURRENT_USER if both are present. The value represents bps/100, so the default of 64,000 is stored as 640 in the registry.

Caution Do not use a registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

A slow link connection affects synchronization in two ways: it prevents shared network folders from automatically converting to an online state, and it prevents files that are newly added to the network share from being pulled to the user's computer during synchronization. These are not configurable.

If the user has a network connection at logon time, the network file and the local file are always opened, even over a slow link. However, if the local cache is up-to-date, all read operations are satisfied by the local cache. All write operations are done to both the network and to the local cache.

After a network share has been offline, it becomes available (online) for the user when three conditions are met:

- No Offline Files from that network share are open on the user's computer.
- None of the Offline Files from that network share have changes that need to be synchronized; that is, there are no offline changes to merge back to the server.
- The network connection is not considered a slow link.

When all of these conditions are satisfied and a user opens a file on the network share, the user is working online on that network share. If one or more of those conditions are not met, then transference to the online state is made when a manual synchronization is performed.

When any one of these conditions is not met and a user opens a file on the network share, the user is still working offline, even though the network share is available. Any changes that the user makes are saved to the offline version of the file only. If files are modified on the cached share (by other users), the local version of the file does not overwrite the server version.

Planning and Design Considerations

The information provided in the preceding sections is valuable for planning and designing your deployment of the User Data and Settings Management technologies.

See "Assessing Organization and User Needs" in this chapter to analyze your users according to their desktop management needs, and assign the User Data and Settings Management features that you want to implement for each type. Make a chart or table that lists your user types and the technologies you want to deploy for them. This information can be used to plan resource allocation for deployment. For sample worksheets, see Appendix A "Deployment Planning Worksheets" in this book.

Local Workstation Disk Storage

Updating your workstations to use IntelliMirror technologies does not mean that additional local disk space is needed, but if your users want to use Offline Files, local disk capacity must be taken into consideration. If local disk space capacity is of concern, there are ways you can minimize its impact.

For example, you have twenty users working on a collective project and each needs to have access to a set of shared files at all times, even when they cannot access the network. In addition to the network disk storage space needed to maintain these files, local disk space is required to keep locally cached copies of the files.

At first glance, it appears that simply looking at the size of the network folder and verifying that each user's local hard drive has sufficient capacity to keep its own copy of these files is sufficient. However, if

the content of Offline Files is very large, you might need to perform more rigorous analyses. Some questions to consider are: Does all the data need to be available both offline and online? Do you need to cache all documents, or only those that are frequently used? Does the entire folder need to be available to all the users, or do users tend to work with only one or two files within the folder? For large projects, answers to these questions can help you determine how to deploy Offline Files. For more information about how best to apply full or quick synchronization and manual or automatic caching methods to your users' files, see the Offline Files Technical Details section above. Understanding how Offline Files work and deciding how your users will work with Offline Files can help you decide the best implementation of this feature, and thus assist you in calculating local disk storage space requirements.

Roaming User Profiles can impact disk storage on computers that are habitually used by a number of users—for example, in a lab or library setting. Each time a new user logs on, their profile is written to the local drive. This can eventually add up to a significant amount of disk storage used only to save roaming profiles. You can apply a Group Policy setting to remove cached versions of roaming profiles when the users log off. This saves disk space from being consumed by roaming user profiles. The policy is called **Delete cached copies of roaming profiles**, and it is accessed under the **Computer Configuration\Administrative Templates\System\Logon** node of the Group Policy snap-in.

Server Disk Storage

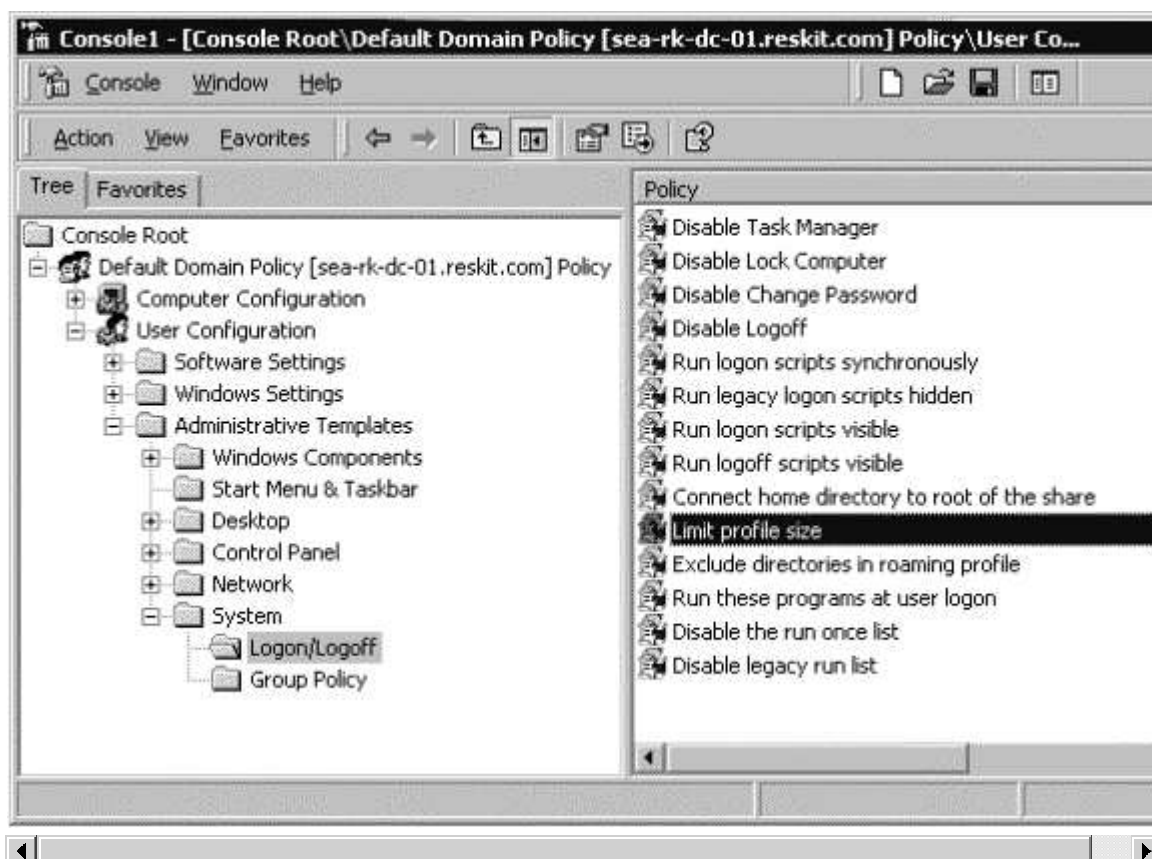
Estimating the amount of server storage space to allocate for user data and profiles is typically more complex than calculating local workstation disk storage requirements. To do so, gather statistical information on how much disk space is currently being used by user data and, separately, by user profiles. The command line utility Diruse.exe can be used to gather information on how much disk space is used along directory trees on a drive. You can put this command into a script, assign it to a workstation, and run it automatically. The utility gathers disk usage data. Then, you can use scripting to calculate the total amount of disk usage data received from a group of workstations.

When analyzing disk space requirements, look at each of the folders that make up a user profile, review the default settings regarding their inclusion in a RUP, and decide whether or not you want to accept those defaults. Review the recommendations provided under User Profile Contents above. You can use the exclusion rule to exclude certain folders from roaming (see the Group Policy snap-in at **User Configuration\Administrative Templates\System\Logon/Logoff\Exclude directories in roaming profile**). Additionally, if you redirect My Documents and My Pictures, you automatically reduce the profile size substantially, as redirected folders are no longer part of the profile.

Use the information gathered above to estimate the amount of server disk storage you need to store user data and profiles. For example, let us say that you have 5,000 users who want to use Redirected Folders. Of these, 4,000 users also need RUPs. You have determined that the average amount of disk space used for each user's personal files is 80 MB. You have also viewed the components available for RUPs and identified that a reasonably sized RUP takes up 15 MB. In this case, you need approximately 400 GB disk space for user data and 60 GB disk space to store roaming user profiles. To be on the safe side, add 20 percent to these numbers, for a total disk storage requirement of approximately 480 GB for user data and 75 GB for user profiles.

Investigate profile sizes to determine typical and maximum sizes for your own users' profiles. See the instructions below for ways to reduce a profile size.

Remember that you can control the maximum size of a user's profile using Group Policy. If a user profile exceeds the allocated size limit, the user cannot log off from the computer until the user reduces the size of their files. You can use the **Limit profile size** policy, available in the **User Configuration\Administrative Templates\System\Logon/Logoff** node of the Group Policy snap-in shown in Figure 6.2, to set the maximum size of the profile and to determine the system's response when the limit is reached.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.2 Limit Profile Size

Although setting profile size limitations can assist with server storage requirements, remember that applications store registry settings in those profiles and users are probably not aware of this. When defining limits, allow sufficient space for the application state data to be saved. Otherwise, you will get help calls from users who cannot log off because they do not understand how to manage the application data portion of their profile.

Best Practice Do not set disk quotas on roaming profile shares. If you want to limit a user's profile size, control the maximum size of a profile by using Group Policy rather than imposing disk quotas on the server. A temporary profile that debits the user's quota is created in the user's context as part of the synchronization process. If the user exceeds their quota limit halfway through logoff, the profile might become corrupted.

Note For information and instructions about calculating disk storage requirements for user state migration, see "User State Migration" in this book.

Bandwidth and Network Traffic Considerations

For User Data and Settings, consider server location in proximity to workstations when deploying RUPs, Offline Files, and Folder Redirection. It is recommended that the servers to which workstations connect for this data be on a fast local area network (LAN) link for quick access. Also look at your network configuration and try to keep hops to a minimum when accessing such frequently needed user information. Keeping this data on the same subnet as the user is one way to keep performance high. For more information about site topologies and bandwidth considerations when using IntelliMirror technologies, see "Preparing Your Network for CCM Technologies" in this book.

The first time a folder is set up for redirection, the user might experience a logon delay while all the files are copied from their local drive to the server. The time this takes is dependent on the amount of data being copied, the speed of the disks involved, the network bandwidth available, the number of hops the data must go through and the quality and speed of the link itself.

RUPs must be small enough to not create significant bandwidth problems; however, if you have a large number of users who log on at the same time every day (for instance, 20,000 users all logging on at 8 a.m.), you might see a decline in network performance at that time. In this case, stagger the users across a number of servers and links to decrease the degradation.

Logon time is usually an item of concern to IT managers. You can manage logon time by:

- Locating the validating domain controller in close proximity to the workstations it needs to validate.
- Simplifying or remove the logon script; Group Policy can now effectively replace many traditional logon script settings. Group Policy does create additional download time at logon, but it is generally

insignificant if Group Policy objects (GPOs) are judiciously used. If Group Policy is used for new folder redirection or software installation, logon time will be increased for those actions.

- Setting limitations on RUP sizes.

Predicting network traffic is not an exact science, but is useful for understanding and balancing network loads. In some cases, it is cost effective to add another server or subnet to handle increased load; in other cases, making simple changes to user work habits can produce equivalent benefits.

When setting up Folder Redirection, stagger the deployment. If you have 1,000 users redirecting My Documents for the first time simultaneously, you might see performance degradation across the network. There are various ways to stagger the deployment — the simplest might be to stagger the addition of users to the security group that specifies Folder Redirection. Again, the number of users you want to update at once depends on the user data and network variables described above.

If you are concerned about the number of servers that exist within a site, you can perform some statistical analyses on existing servers within the desired proximity, using tools such as the System Monitor, to see if you can add some workload to them. For example, a print server can be used for disk storage for RUPs, if it has sufficient disk capacity and can handle the additional network load.

For more information about the various user types you might identify within your organization, see "Assessing Organization and User Needs" in this book. For help matching your users with the components best suited to their needs, use the worksheets in Appendix A "Deployment Planning Worksheets" in this book. This assists you in designing an IntelliMirror deployment that gives your users the best possible performance.

Testing and Pilots

Prior to large-scale deployment, it is important that you thoroughly test and understand your configuration of the User Data and Settings Management technologies you wish to implement.

Controlled Testing

After identifying which IntelliMirror features you want to deploy, set up a test environment so that you can thoroughly test and understand those features. For a sample test configuration, see the Step-by-Step Guide to a Common Infrastructure for Windows 2000 Server Deployment link on the Web Resources page at <http://windows.microsoft.com/windows2000/reskit/webresources>.

For testing User Data and Settings Management technologies, you generally need a domain controller, a server, two or more workstations, and possibly a mobile computer connected through a slow link. These requirements might increase depending on the scale at which you want to test your proposed configuration. To start, see the Step-by-Step Guide to Data and User Settings also on the Web Resources page. Then expand on that set of tests until you have covered all of the requirements for your organization, and understand how the technologies will perform upon deployment.

Pilots

Once you have completed your testing in a controlled environment, define a group of real users to pilot your configuration of the User Data and Settings Management technologies. Keep the number of users within the scope of what you can test and manage easily. One of the reasons for doing a pilot is to encounter and resolve unexpected results and problems on a small scale, and to adjust your configuration accordingly before you deploy on a large scale.

Goals for your pilot might be to:

- Validate that IntelliMirror functionality is beneficial to a wide user base
- Learn how to deploy and support My Documents folder redirection
- Learn how to deploy and support Roaming User Profiles
- Learn how to deploy and support Offline Files
- Develop an operations framework for deployment and support
- Develop an end user communication and training plan for deployment and support
- Demonstrate that the technologies scale to the needed capacity
- Determine what user education is needed
- Learn which combinations of folder redirection and RUP are appropriate for your users

User Education

The impact on users of deploying User Data Management and User Settings Management features can be more significant than the impact of deploying of less visible technologies. For example, all a user might need to know about Software Installation and Maintenance is that now they can go to Control Panel to install an application. However, because User Data Management and User Settings Management directly affects the look, feel, and usage of their desktop and personal files, users need more education when these features are deployed.

Roaming User Profiles (RUPs)

As a rule, RUPs require very little user training. Users who always connect to the network over a LAN appreciate seeing the same desktop settings on any computer they log onto, and are unlikely to create any helpdesk queries over this. There are, however, some considerations such as slow links, unexpected messages, and profile sizes to be explained.

If a roaming profile is used on more than one computer simultaneously, the settings last written to the profile are preserved from the logoff. Users who work on more than one computer at a time need to be aware of this.

Users who work onsite on a fast link, and then offsite using a mobile computer and a modem, need to understand that their two computers do not have the same profile settings unless they log on to the network with the mobile computer over a fast link.

By default, RUPs do not travel over slow links. When a user who has a roaming profile logs on over a slow link, they do not receive their roaming profile. A message displays which explains this to them. You can use Group Policy to disable this message if it is not useful to your users, or you can set the **Timeout for dialog boxes** policy setting (found in the Group Policy snap-in under **Computer Configuration\Administrative Templates\System\Logon**) to 1 so that it is essentially unnoticeable. Users must be educated to keep their profile size to a minimum — for example, to save shortcuts to documents, instead of the actual documents, onto the desktop. If you use the Limit Profile Size policy to manage profile sizes, teach users how to respond to the messages they receive when they exceed that limitation. If you force a user to reduce their profile size before logging off, instruct them on how to safely do so.

Redirected Folders

In general, users do not need to know that their folders are being redirected. If they are used to seeing their documents in the My Documents folder, current applications display and use the files in exactly the same manner as before the files were redirected.

The server path to which the folder is redirected appears when the user right-clicks **My Documents** and then clicks **Properties**. Most users do not notice, but if they do, they need just a brief explanation of why their folders are now on a network share. Two cases emerge in which users need to know that their data is being redirected and to where.

The first case occurs if you are using older applications that do not recognize UNC path names. Such applications see only directories and files in the old Microsoft® MS-DOS® context of <drive letter:\directory\file> (example: C:\MyDocs). They do not see files stored in UNC paths such as \\servername\sharename\file. For these situations, map a network drive to the location of the redirected files, and have them use that drive setting for the older application.

The second case occurs for users who connect to the network using remote access, and whose computer accounts are not a part of the domain to which they are connecting. If a user needs a file from a redirected My Documents folder during a dial-up session, they need to know the full UNC path name so they can connect to the server share that contains the files — for example, \\Servername\Redirected Folders\%username%\My Documents.

When redirecting My Documents, the Recycle Bin size for My Documents defaults to a percentage of the size of the server partition where the redirected My Documents resides. The smallest value you can set is 1 percent. Since a user's Recycle bin can potentially grow large, you need to train your users to periodically empty the Recycle bin. Disk quotas on the server share where the folders are redirected also keep user data to a reasonable size.

Offline Files and Synchronization Manager

User education for Offline Files consists of training the users on Synchronization Manager, how to interpret the various messages they receive when transitioning from offline to online state, and how to resolve file version conflicts. Some users might need to know that some file types, such as *.slm, *.mdb, *.ldb, *.mdw, *.mde, *.pst, and *.db?, are not synchronized.

To manually force synchronization, a user right-clicks the **My Documents** folder on the desktop, and then clicks **Synchronization**. Users can additionally use Synchronization Manager to schedule synchronizations, set synchronization to occur during idle periods, etc. Users also need to know how to manage the file conflict when another user has modified the file they are working on.

Offline Files notifies users when the status of the network connection changes. An informational balloon notifies users when they are offline; the users can continue to work with the files as they normally would. They can click the **Offline Files** icon in the icon tray for more information about their network connection status. When working offline, the user can still browse network drives and shared folders that have been set up for Offline Files. A red X appears over any disconnected network drives that are not currently available.

When the network connection is restored, any changes the user made while working offline are updated to the network. If other users have made changes to the same file, options are offered for resolving the version conflict. For more information on resolving file version conflicts, see the "Synchronization Manager"

heading under "Synchronization Manager" later in this chapter.

Implementation of User Data and User Settings Management

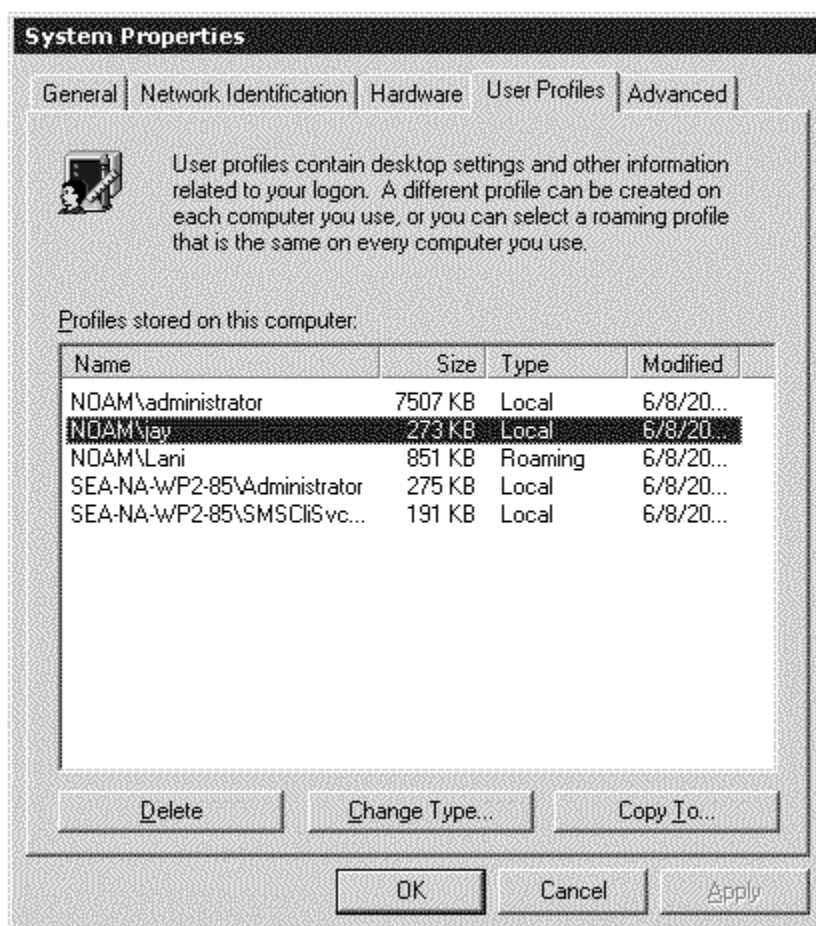
Based on the decisions that you made during the planning stages of deployment, you will now begin to implement your plan. This implementation includes tasks associated with profile configuration, folder redirection, the use of Group Policy settings for profiles, offline files, and synchronization, and the setting of disk and profile quotas.

How to Configure a Domain Default Profile

Domain default profiles are useful when you want all users within a domain who are logging on for the first time to receive the same profile. This provides administrative control over the users' desktops and settings.

To create and define a domain default profile

1. From the **Start** menu, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. Right-click the appropriate domain name in the left pane, click **New**, and click **User**.
3. Enter the parameters for the new user; in our example, this is Jay Jamison.
4. Close the snap-in and log off.
5. Log on as the new user.
6. Configure the desktop as desired.
7. Log off, and log on again as administrator.
8. From the **Start** menu, point to **Settings**, and click **Control Panel**.
9. Double-click the **System** icon.
10. Click the **User Profiles** tab.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.3 User Profiles

11. Click the profile you just created and click **Copy To**.
12. If you want a domain-wide default profile, type or browse to the path to the DC NETLOGON share + Default User; in our example, this is \\Sea-na-dc-01\NETLOGON\Default User. (Note: You are creating

the folder "Default User.")

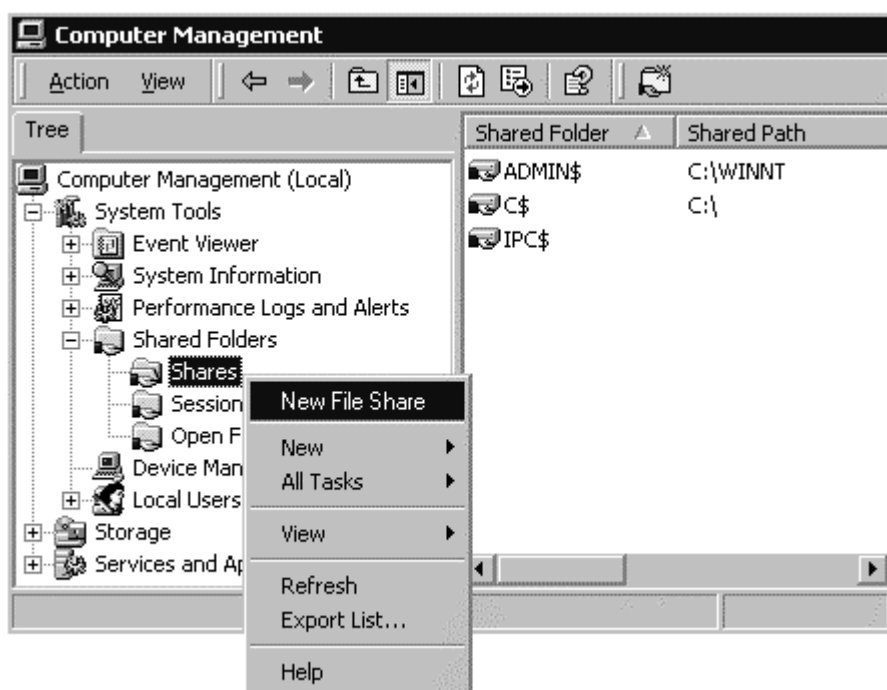
13. If you want to change the default profile for the local computer only, copy the profile to the Documents and Settings\Default User folder.
14. Click the **Change** button under the **Permitted to use** setting. Click **Everyone** to make this the default domain profile for everyone in this domain and then click **OK**.

How to Configure a Roaming User Profile (RUP)

The following steps describe how to deploy Roaming User Profiles. To begin, the Administrator logs on to a server, creates a network share on which to store roaming user profiles, and then designates the set of users that must use the RUPs.

To configure a Roaming User Profile

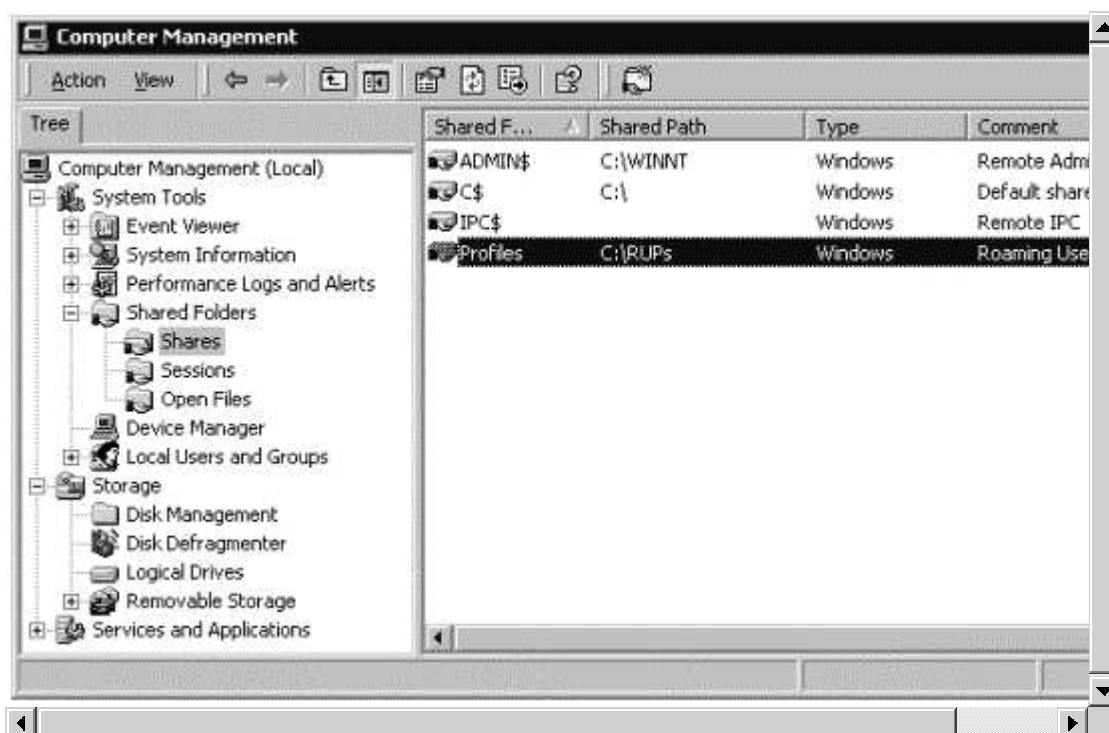
1. From the **Start** menu, point to **Programs**, point to **Administrative Tools**, and click **Computer Management**.
2. Right-click **Computer Management** at the top of the snap-in and click **Connect to another computer**.
3. Double-click the name of the server on which you want to create the share to contain the roaming profiles.
4. Expand the **System Tools** node.
5. Expand the **Shared Folders** node.
6. Right-click **Shares** and then click **New File Share** as shown in Figure 6.4.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.4 New File Share Click Browse.

7. Click the drive letter where you want the folder to exist.
8. If the folder does not already exist, click **New Folder** and type in the name of the folder to create. In our example, this is **RUPs**.
9. Click **RUPs** and then click **OK**.
10. Type in a share name and description and click **Next**.
11. Click **All users have full control** and click **Finish**.
12. You are prompted whether you want to create another folder. Click **No**.
13. The new share is now listed in the right pane of the snap-in. You can close this snap-in.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.5 Roaming User Profile Share

To configure a Roaming User Profile

1. From the **Start** menu, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. Right-click the user's name you want to make a roaming user (in our example, Suki White), and click **Properties**.
3. Click the **Profile** tab.
4. In the profile field, type in the path to the network share where the user profile is to be stored: in this example, \\Profiles\RUPs\%username%. The system creates a directory called Suki in the RUPs share when the user Suki first logs on.
5. Repeat this step for each user you want to add as a roaming user.

If you have a large number of users to add, you do not want to repeat these steps for each user. You can create a script file to do this work for you. The following sample script is offered as a starting point for your own script.

```
set Args = Wscript.Arguments
ouName = Args(0)
usrName = Args(1)
RUProot = Args(2)

RUPpath = RUProot & "\\" & usrName

'Get the domain
Set dse = GetObject("LDAP://RootDSE")
Set domain = GetObject("LDAP://" & dse.Get("defaultNamingContext"))

set ou = domain.GetObject("organizationalUnit", "OU=" & ouName )

wscript.echo "Creating user in " & ou.Name

set usr = ou.Create("user", "cn=" & usrName )
usr.Put "samAccountName", usrName
usr.Put "userPrincipalName", usrName
usr.Put "Profilepath", RUPpath

usr.SetInfo

wscript.echo " User " & usrName & " was created successfully in " & ou.Name & "with a RUP
Path of: " & RUPpath
```

If there are specific computers upon which you do not want RUPs to land (for instance, in a lab environment), you can effectively disable RUPs on those computers by disabling the Group Policy setting at

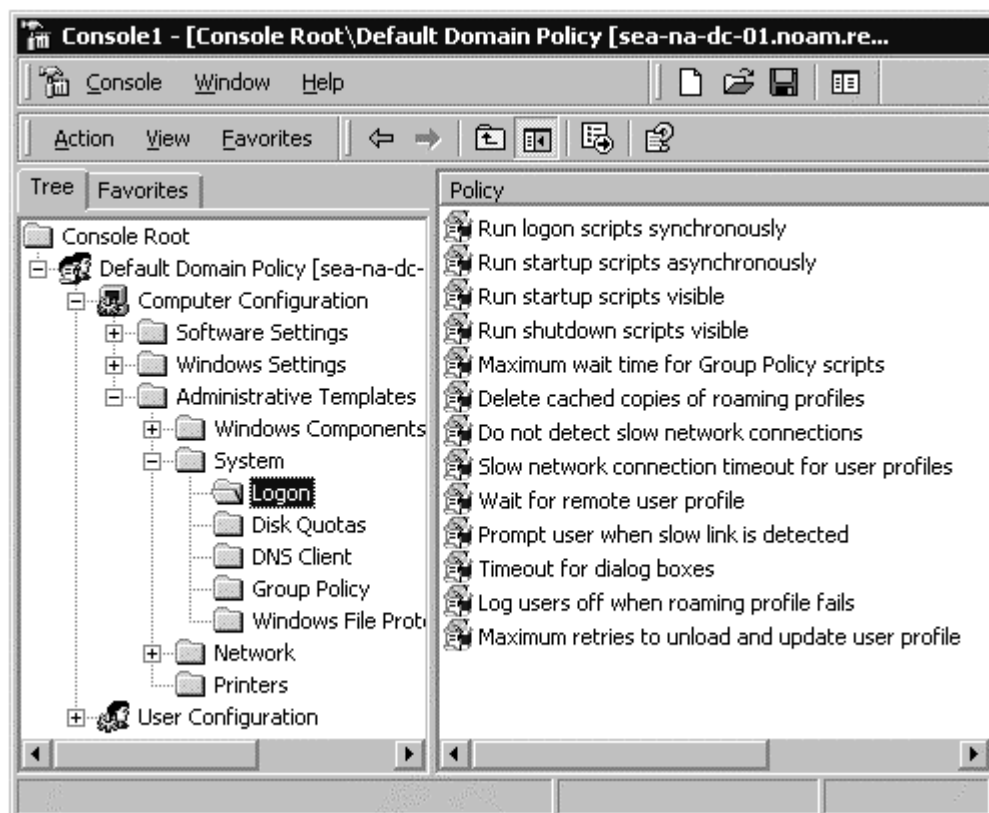
Computer Configuration\Administrative Templates\System\Logon\Wait for remote user profile.

Group Policy Settings For Roaming User Profiles

While Group Policy is not required to enable roaming profiles, Group Policy settings can help control the ways in which the profiles behave. One example of this has already been shown — that is, setting a policy to delete locally cached versions of roaming user profiles when the user logs off which saves disk space on computers that are used by many different users. Additionally, you can enhance your control of the profile size and logon time by specifying certain folders to exclude from the profile. This setting is found in the Group Policy snap-in at **User Configuration**

Administrative Templates\System\Logon\Logoff\Exclude Directories in Roaming Profile.

Additional Group Policy settings for RUPs are shown in Figure 6.6. To learn more about any setting, open the Group Policy snap-in, double-click the setting, and then click the **Explain** tab.



If your browser does not support inline frames, [click here](#) to view on a separate page.

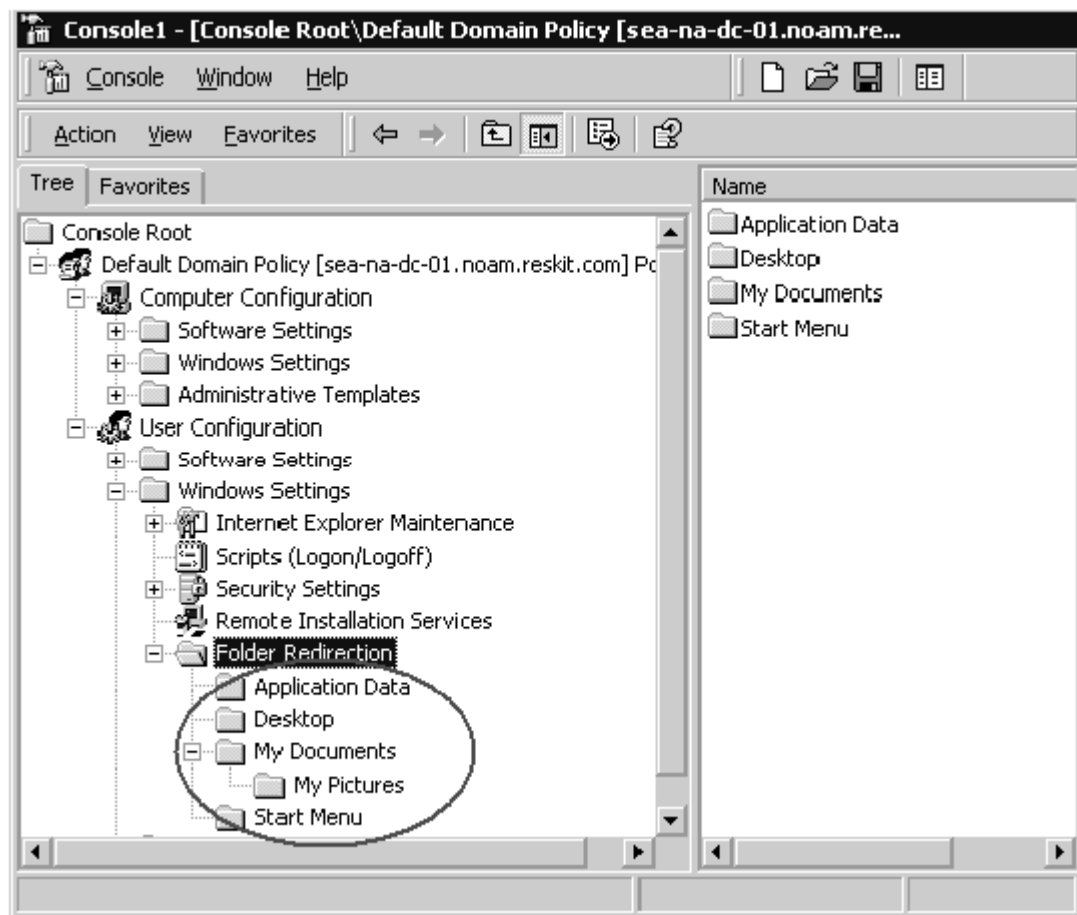
Figure 6.6 Group Policy Settings for Roaming User Profiles

How to Configure Folder Redirection

Administrators manage folder redirection settings by using Group Policy.

To configure folder redirection

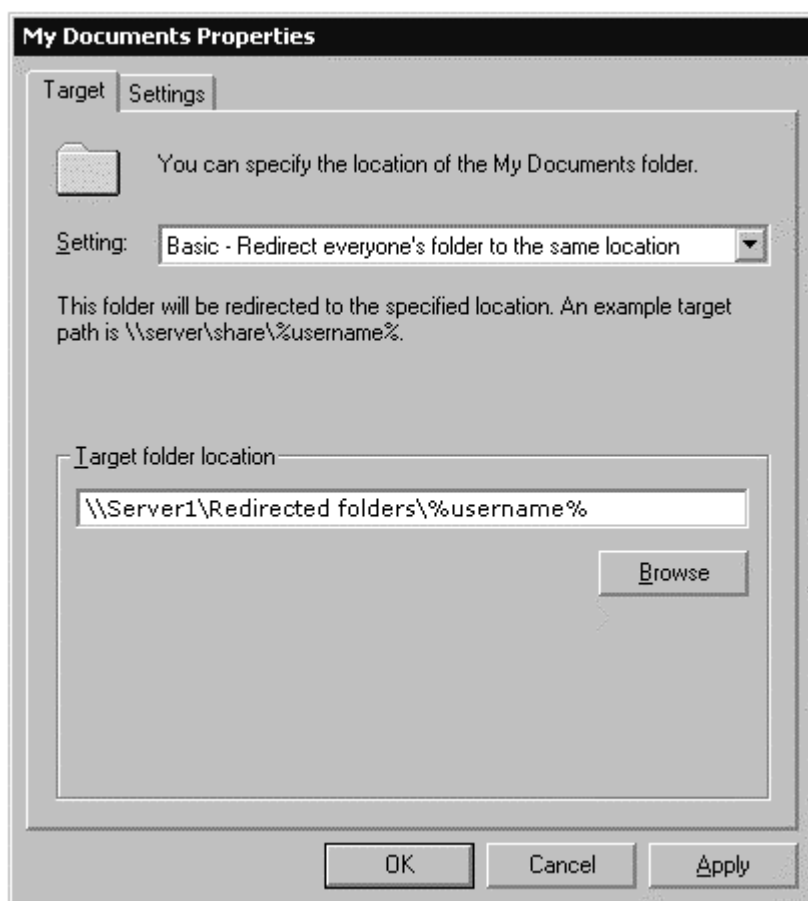
1. Open the Group Policy snap-in for the desired site, domain, or OU.
2. Expand the **User Configuration** node. Expand the **Windows Settings** and **Folder Redirection** nodes in the same way. Icons for the five folders that can be redirected are visible:



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.7 Folders Available for Redirection

3. Right-click the folder name you want to redirect (in our example, **My Documents**) and click **Properties**.
4. Click the down-arrow adjacent to the **Setting** text box.
5. If you want all users' redirected folders to be assigned to the same network share, click **Basic**, and supply the name of the target folder location, such as \\servername\redirected_folders\%username%. Click **Browse** to find the target directory name. If you are redirecting to a network share, always use the UNC name here.



If your browser does not support inline frames, [click here](#) to view on a separate page.

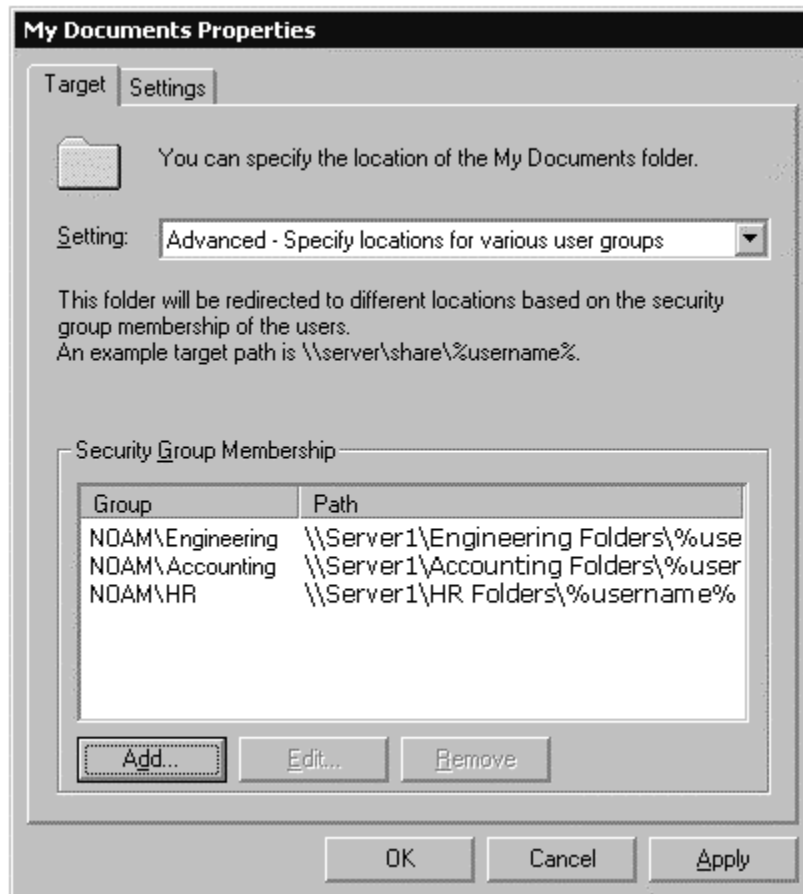
Figure 6.8 Basic Folder Redirection

6. If you want to redirect folders to different network shares based on security group memberships, click **Advanced**.
7. Next, supply the names of the security groups and the paths to which their files will be redirected. To begin, click **Add**.
8. Type in the name of the security group or click **Browse** to find it. Use the same method for entering the target folder location. If you are redirecting to a network share, always use the UNC name here.



Figure 6.9 Adding Security Group for Folder Redirection

9. Repeat step 8 until you have entered all security groups.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.10 Advanced Folder Redirection: Security Groups and Target Directories

10. Click **Apply**, and then click **OK**.

Best Practice Do not create the folder in advance for individual users. Create only the root share on the server, and let the system create the folders for each user. Incorporate %username% into fully qualified universal naming convention (UNC) paths. When you use the %username% environment variable, Windows can easily create folders for users based on their user name.

If you decide you must create folders for the users, ensure that you have set the correct permissions. The tables below outline the default and minimal permissions needed.

Table 6.5 NTFS Permissions Needed for Root Folder

User Account	Folder Redirection Defaults	Minimum Permissions Needed
Creator/owner	Full Control, this folder, subfolders, and files	Full Control, this folder, subfolders, and files
Local Administrator	Full Control, this folder, subfolders, and files	Full Control, this folder, subfolders, and files
Everyone	Full Control, this folder, subfolders, and files	List Folder/Read data, Create Files/Write Data, Create Folders/Append Data - This Folder only
Local System	Full Control, this folder, subfolders, and files	Full Control, this folder, subfolders, and files

Table 6.6 Share level (SMB) Permissions Required for Root Folder

User Account	Folder Redirection Defaults	Minimum Permissions Needed
Everyone	*Full Control	Everyone - no permissions. Use security group that matches the users who need to put data on share

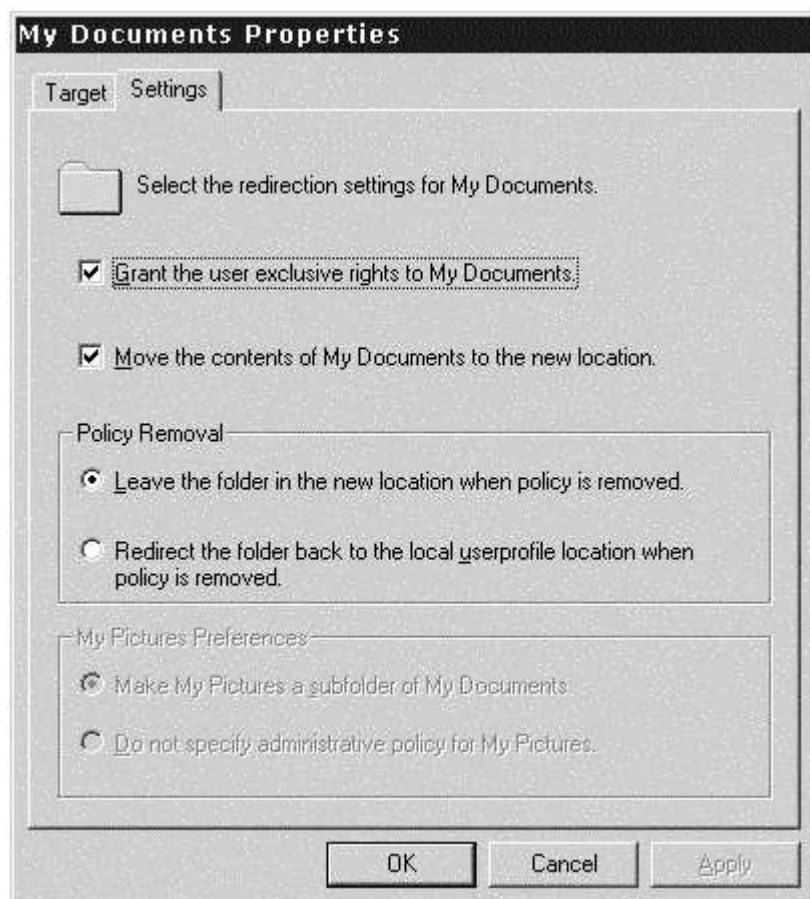
* An exception to this is the Start Menu redirection, or any other folder that is redirected to a read-only folder. In this case, the SMB permissions on the share must also be set to Everyone-Read.

Table 6.7 NTFS Permissions Required for Each User's Redirected Folder

User Account	Folder Redirection Defaults	Minimum Permissions Needed
%username%	Full Control, owner of folder	Full Control, owner of folder
Local System	Full Control	Full Control
Everyone	Traverse Folder, Read Attributes, Read Extended Attributes, and Read Permissions	Everyone - no permissions

Group Policy Removal Considerations

From within the Group Policy snap-in, you can view and change the Group Policy Removal settings for any redirected folder, at the Properties page of the policy setting.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.11 Policy Removal Settings

Table 6.8 and Table 6.9 summarize what happens to redirected folders and their contents when the Group Policy settings no longer apply.

Table 6.8 Policy Removal Effects When *Move the contents of special folder to the new location* Checkbox Is Enabled

Policy Removal Option	Results When Policy Is Removed
Redirect the folder back to the user profile location when policy is removed	<ul style="list-style-type: none"> • The special folder returns to its user profile location. • The contents are copied, not moved, back to the user profile location. • The contents are not deleted from the redirected location. • The user continues to have access to the contents, but only on the local computer.
Leave the folder in the new location when policy is removed	<ul style="list-style-type: none"> • 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.

Table 6.9 Policy Removal Effects When *Move the contents of special folder to the new location* Checkbox Is Disabled

Policy Removal option	Results when policy is removed
Redirect the folder back to the user profile location when policy is removed.	<ul style="list-style-type: none"> • The special folder returns to its user profile location. • The contents are not copied or moved to the user profile location. Caution: This means the user can no longer see them.
Leave the folder in the new location when policy is removed	<ul style="list-style-type: none"> • 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.

How to Configure Offline Files

Typically, the shares that contain Offline Files already exist on a server, and the users are already accessing that share over the network. If this is the case, you can go directly to **Setting the server share or folder as offline**, below. However, to show the complete process, the steps required to create an Offline Files share are given here.

To create a server share for offline use

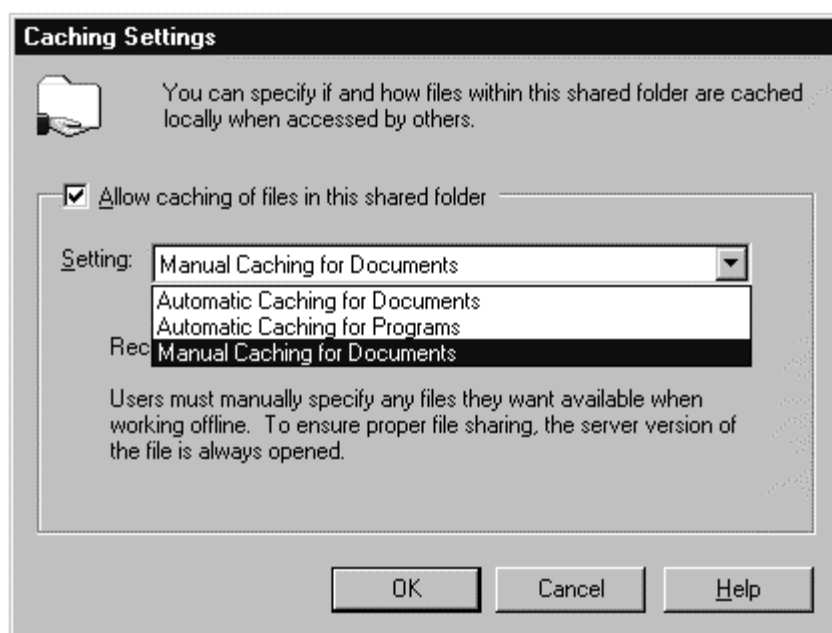
1. Log on to the server as an administrator.
2. From the **Start** menu, point to **Programs**, point to **Administrative Tools**, and click **Computer Management**.
3. If you are not logged on to the server where you want the share to be, right-click **Computer Management** and click **Connect to another computer**. When the directory displays, click the name of the server you want to use and click **OK**.
4. Expand the **System Tools** node.
5. Expand the **Shared Folders** node.
6. Right-click **Shares**, and then click **New File Share**.
7. Type in the name of the folder if it already exists, or click **Browse** to find it if you do not know its exact name. Click **Browse** if you need to create a new folder.
8. Expand the drive letter share (for example, **C\$**) on which you want to find or create the folder. To create a new folder, click **New Folder**, type in the folder name, and click **OK**; then, click its name in the file list and click **OK**. (If the folder already exists, just click its name and click **OK**.)
9. Type in a share name and optional description and click **Next**.
10. The next screen allows you to specify access permissions to the folder. Set the permissions to your specifications and click **Finish**. You are prompted whether you want to create another shared folder. Click **No** (unless you want to create more shared folders at this time.)
11. Exit this snap-in.

Setting server share caching

Navigate to the server share using Windows Explorer or My Computer. Right-click the folder you want to set as Offline.

To set server share caching

1. Click **Properties**, click the **Sharing** tab, click **Share this folder**, and then click **Caching**.
2. Select the type of cache you want to use and click **OK**. (For more information about the three types of caching, see "Offline Files" earlier in this chapter.)



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.12 Select Cache Option

3. Click **OK**.
4. If you are creating a new share, by default, the group Everyone has full control over this folder. To change this default, click the **Permissions** button and apply permissions, as you desire. You can also define the maximum number of users who can access this share by using the **User Limit** setting.
5. Click **OK** to save your settings and exit.

The remainder of the steps for setting up Offline Files is performed at the client workstation. The first step is to ensure that Offline Files is enabled on the client. By default, Offline Files is enabled on computers running Windows 2000 Professional, and disabled on computers running Windows 2000 Server.

To enable Offline Files at the client

1. Double-click **My Computer** on the desktop.
2. Click **Folder Options** on the **Tool** menu.
3. Click the **Offline Files** tab.
4. Make sure the **Enable Offline Files** box is checked.

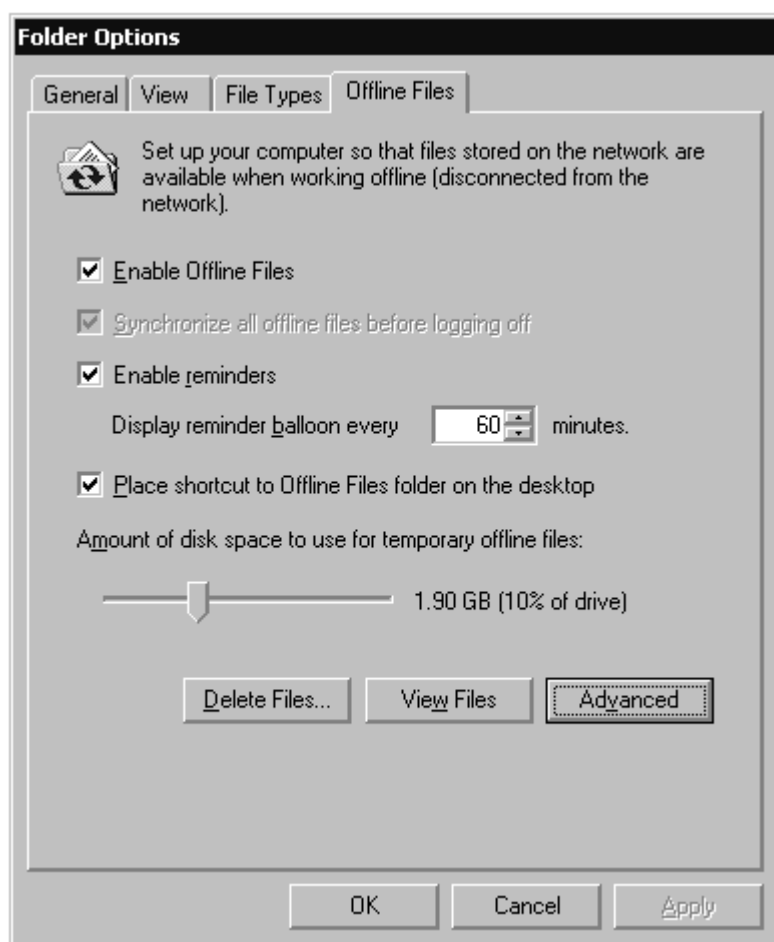


Figure 6.13 Enabling Offline Files on a Computer

5. Click **OK** and exit.

Once Offline Files are enabled on the computer, network files and folders can be selected to be available offline. Any shares set for Automatic caching are now cached automatically without any further user intervention. See the technical discussion on Offline Files regarding the three caching types.

To manually pin a file or folder to be available offline on a client computer, follow the steps outlined below.

To manually pin a file or folder

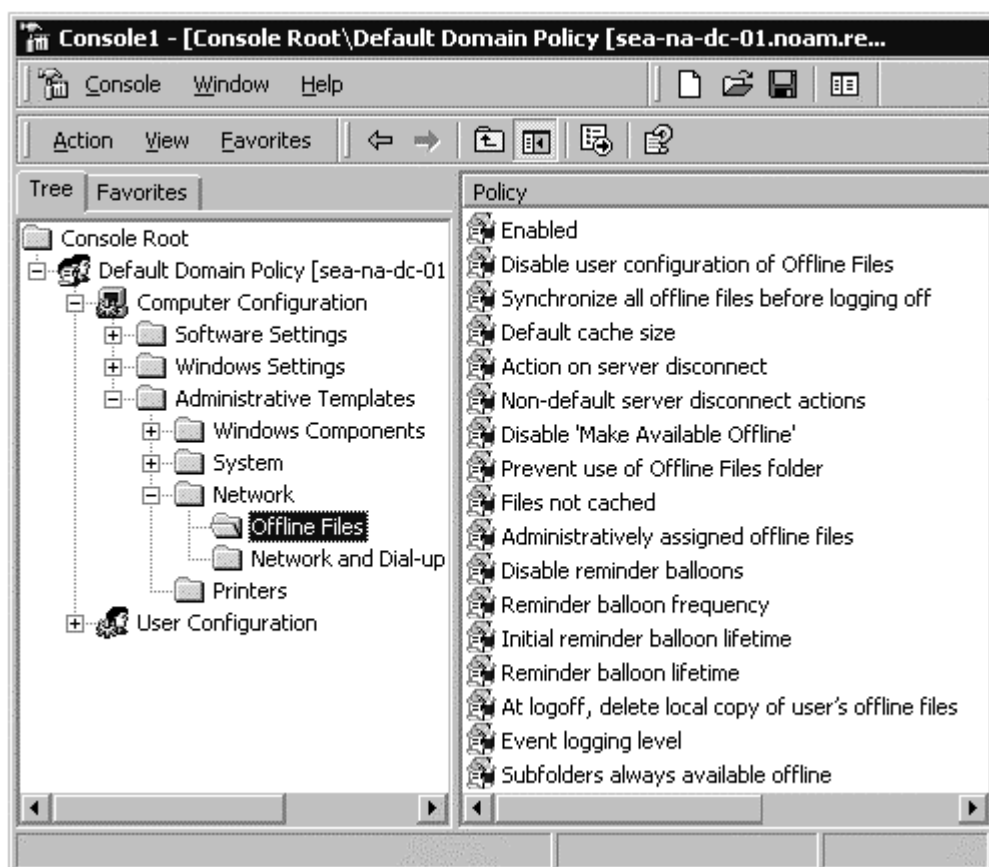
1. Navigate to the server folder via a desktop shortcut or **My Network Places**.
2. Right-click the file or folder and click **Make Available Offline**. The **Welcome to the Offline Files** wizard will start. Click **Next** to continue.
3. The wizard's options allow you to:
 - o Enable or disable automatic synchronization at logoff
 - o Enable or disable reminders
 - o Create a shortcut to Offline Files on the desktop. (Note: if the user already has a desktop shortcut to this folder, this is an unnecessary addition; it might also cause user confusion.)

Tip You can set multiple folders at once for Offline Use using the Group Policy setting, **Administratively assigned offline files**. See the Group Policy snap-in screens below for reference.

After you make your selections, a copy of the file is placed on the hard drive of the local computer. This displays on the screen as a synchronization. When the computer is disconnected from the network, the user can use the local version of the document. When network access is available, any changes the user made to the local version of the document are copied back to the network file.

Group Policy Settings for Offline Files

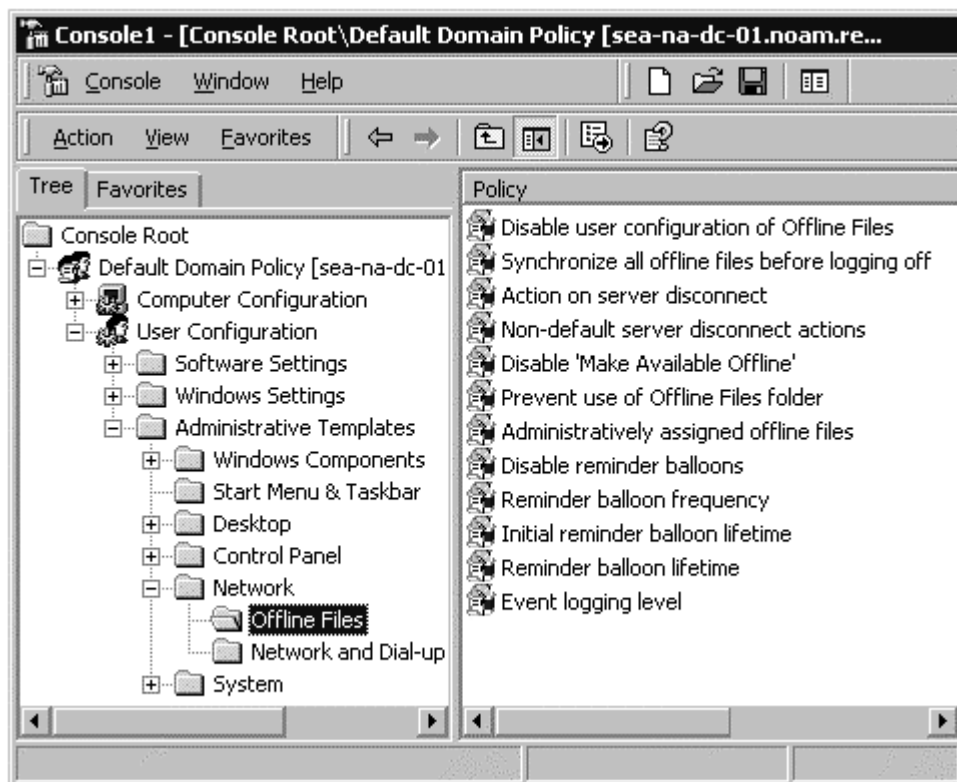
The Group Policy settings for Offline Files are stored in two locations within the Group Policy Editor snap-in. These include **Computer Configuration\Administrative Templates\Network\Offline Files** for computer-based settings, and **User Configuration\Administrative Templates\Network\Offline Files** for user-based settings. Some settings are identical for either user or computer; remember that the computer policy always takes precedence over a user policy.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.14 Group Policy Computer Configuration Settings for Offline Files

Note For more information about a setting, click the **Explain** tab associated with each Group Policy setting.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.15 Group Policy User Configuration Settings for Offline Files

Note For more information about a setting, click the **Explain** tab associated with each Group Policy setting.

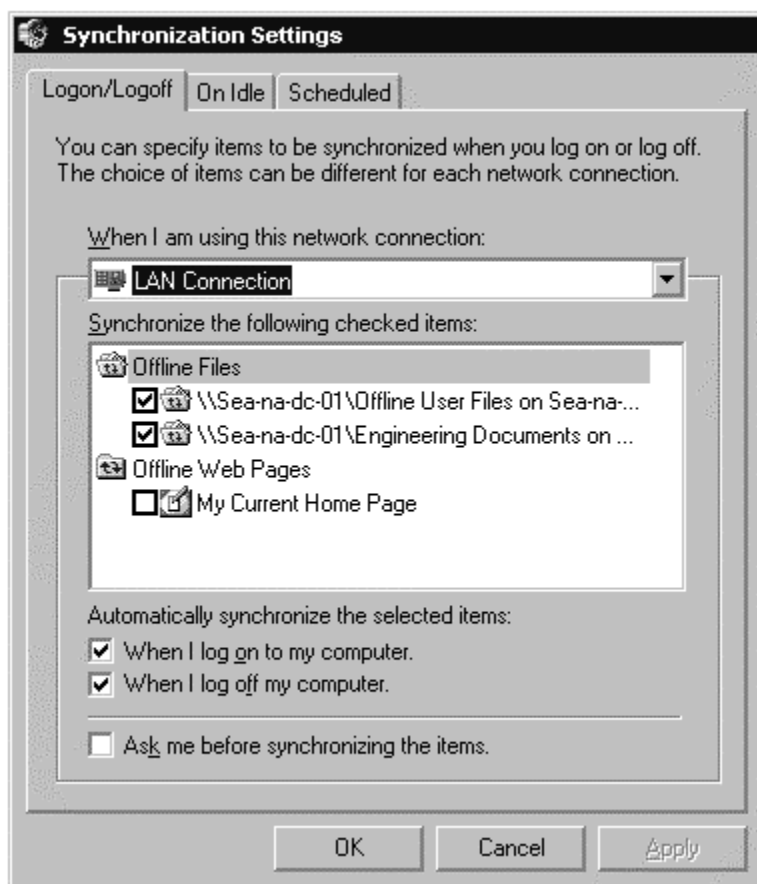
Synchronization Manager

Synchronization Manager is a tool that users employ on their own workstations. Synchronization Manager synchronize files:

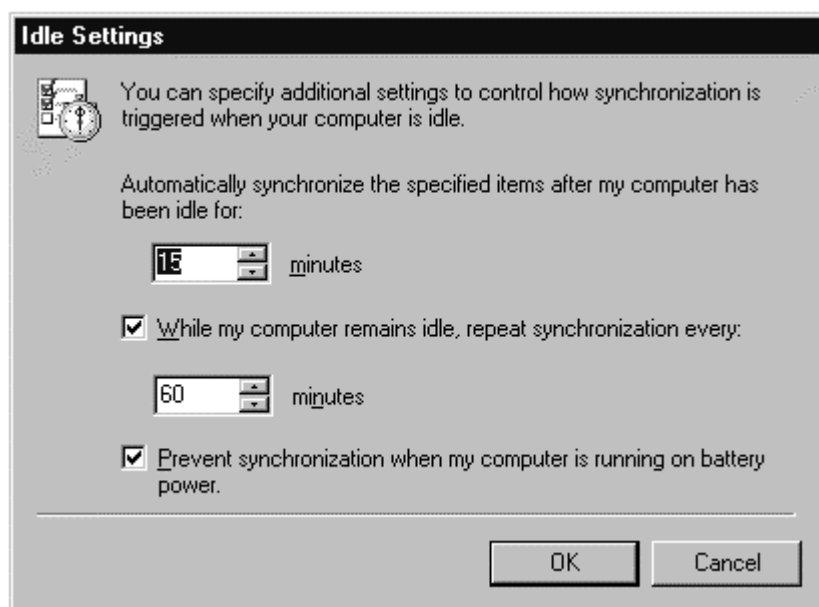
- Every time the user logs on or off the computer, or both.
- At specific intervals while the computer is idle.
- At scheduled times.

To open Synchronization Manager

1. From the **Start** menu, point to **Programs**, point to **Accessories**, and click **Synchronize**.
 - a. Select any Offline Files folder and click **Properties** to display all files in that folder.
 - b. Click **Synchronize** to force an immediate synchronization of all Offline Files.
2. Click **Setup** to customize your settings for Offline Files. Setup allows you to specify how to treat Offline Files synchronization at logoff or at logon. You can require that Synchronization Manager prompt you before synchronizing files.

**Figure 6.16 Synchronization Settings**

3. To set synchronization to occur during idle times, click the **On Idle** tab.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.17 Offline Files

4. To add synchronization tasks to your computer's schedule, click the **Scheduled** tab on the Synchronization Settings dialog box. Click **Add** to start the Scheduled Synchronization Wizard. Click **Next** to continue.
5. Check the folders that need to receive the same synchronization schedule. Click **Next**.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.18 Synchronization Schedule Options

6. Set the time parameters for this synchronization and click **Next**.
7. Type in a name for this scheduled synchronization and click **Next**. Click **Finish** to save your settings and exit the wizard.

After you have created the schedule, it is displayed in the Scheduled tab on the Synchronization Settings dialog box. You can add more schedules, remove them, or edit the ones you have created. Advanced scheduling parameters allow you to set start and end dates and times.

Users can also force synchronization on a particular folder at any time by right-clicking the folder name (in Windows Explorer, My Computer, or from a desktop shortcut) and clicking **Synchronize**.

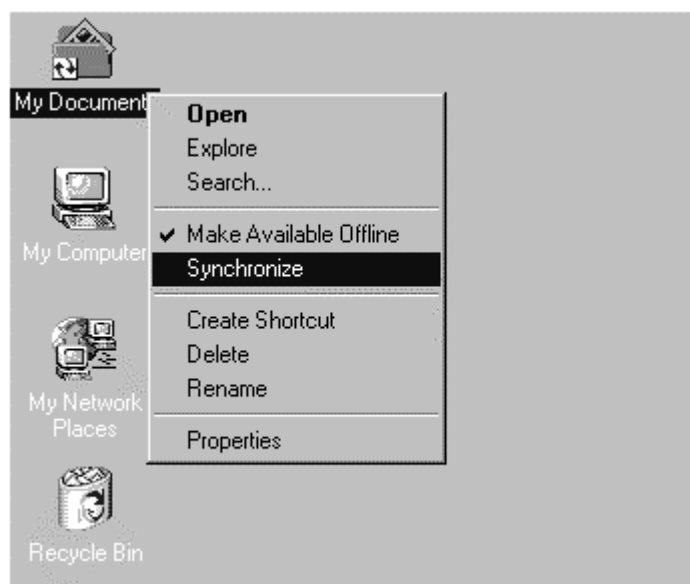
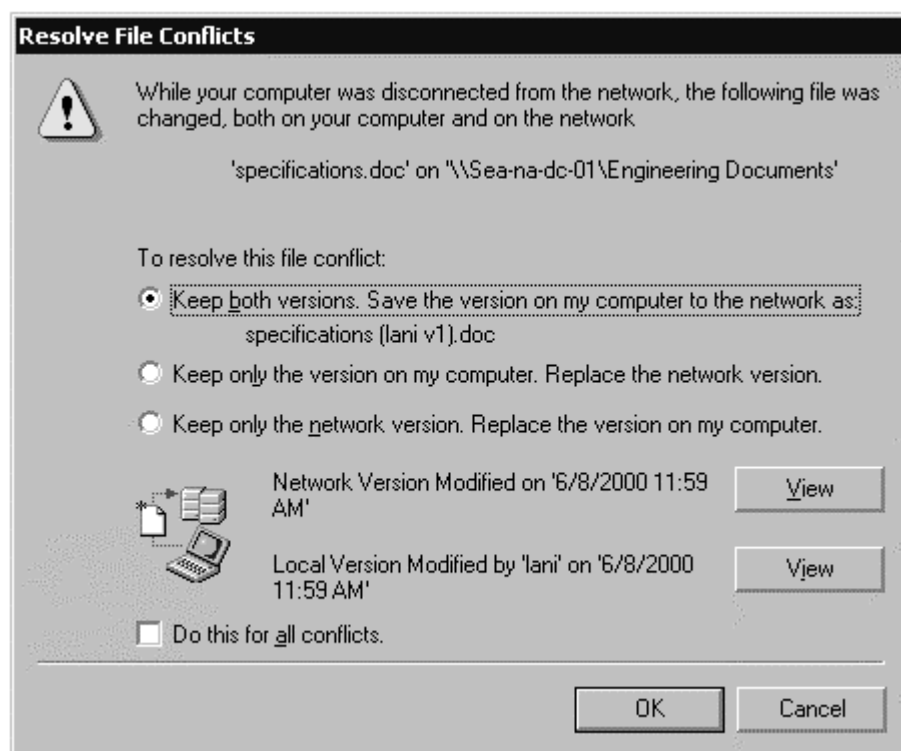


Figure 6.19 Synchronize My Documents

When files are modified offline by more than one user, conflicts can occur. Offline files reference a specific *version* of the corresponding file on the server share. When a file is modified offline, that file replaces the server version when the user reconnects to the network. Synchronization Manager checks the server version to see if it has changed since the last synchronization from this computer.

If the server version has not changed, the local copy of the modified file is copied to the server. If the server version of the file has been modified since the last synchronization from this computer, this typically means that another user has updated the file. Synchronization Manager displays a **Resolve File Conflicts** dialog box, shown in Figure 6.20.

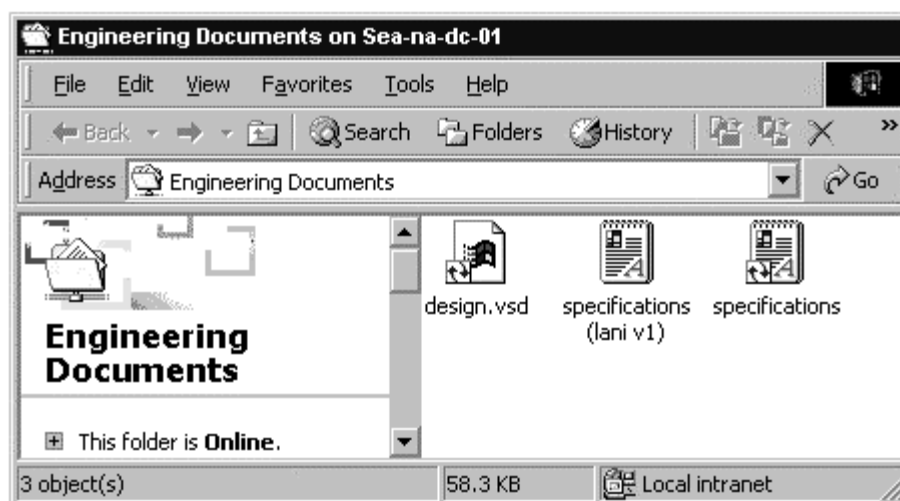


If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.20 File Conflict Resolution

The user can view both files clicking the **View** buttons if they wish to review the modifications before choosing a resolution.

If the user keeps both versions of the file, a new copy of the file is created on the server share with their user name and a version number assigned to it, as shown in Figure 6.21.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.21 New File *Specifications (Lani v1)* Exists After Conflict Resolution

Group Policy Settings for Synchronization Manager

You can use Group Policy to control how offline files are synchronized at logoff. In the Group Policy snap-in under **Computer Configuration\Administrative Templates\Network\Offline Files**, the **Synchronize all Offline Files before logging off** policy allows you to control whether Offline Files are fully synchronized when users log off.

This policy also disables the **Synchronize all Offline Files before logging off** option on the **Offline Files** tab at the user's computer. This prevents users from changing the option while a policy controls it. If you enable this policy, Offline Files fully synchronizes at logoff. If you disable this policy, the system performs a quick synchronization at logoff. If you do not configure this policy, the system performs a quick synchronization by default, but users can change this option.

Disk Quotas

Disk quotas track and control disk space use for user data stored on the network. You can set Disk Quotas through Group Policy. When Disk Quotas are enabled in Group Policy, the settings affect all NTFS volumes on all Windows 2000 computers to which the GPO applies.

You can manually set Disk quotas on a server-by-server basis. In either implementation, you can configure Disk Quotas to:

- Prevent a user from using too much disk space.
- Log an event when a user exceeds a specified disk space limit or warning level.

To manually apply Disk Quotas

1. Log on to the server as a user with local administrative privileges.
2. Double-click **My Computer** on the desktop.
3. Right-click the volume for which you want to assign quotas, and click **Properties**.
4. Click the **Quota** tab.

Note If the volume is not formatted with the NTFS file system, or if you are not a member of the Administrators group, the **Quota** tab is not displayed in the volume's **Properties** dialog box.

5. Click **Enable quota management**.

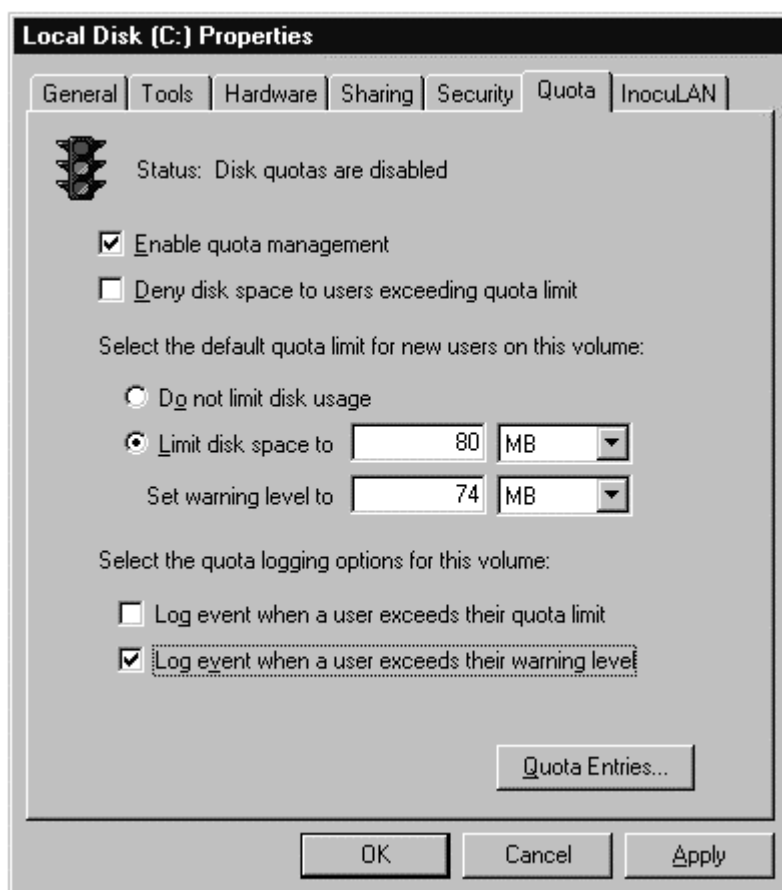


Figure 6.22 Set up Disk Quotas

6. Set the disk space, warning level, and event log parameter as desired.

After disk quotas are set for a volume, the first time each user writes data to that volume, a quota record is created for that user using the default limit and warning threshold from the volume. Because this serves the majority of users, no additional settings are required to apply disk quotas. However, if some of your users have exceptional quota requirements, you can set specific limits for them prior to their first use of the volume.

To apply specific quota limits to specific users

1. To set quotas for individual users, click **Quota Entries**.
2. Click **New Quota Entry** on the Quota menu. A list of all available users in this domain displays. Click the desired user on the list, click **Add**, and then click **OK**.

Note You can add multiple users at once by pressing down the CTRL key as you select user names from the displayed list. If you do so, however, the same quota levels are applied to all users added at this time.

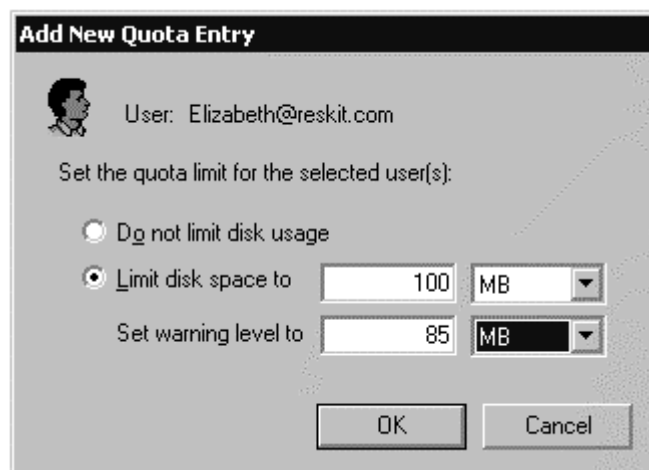
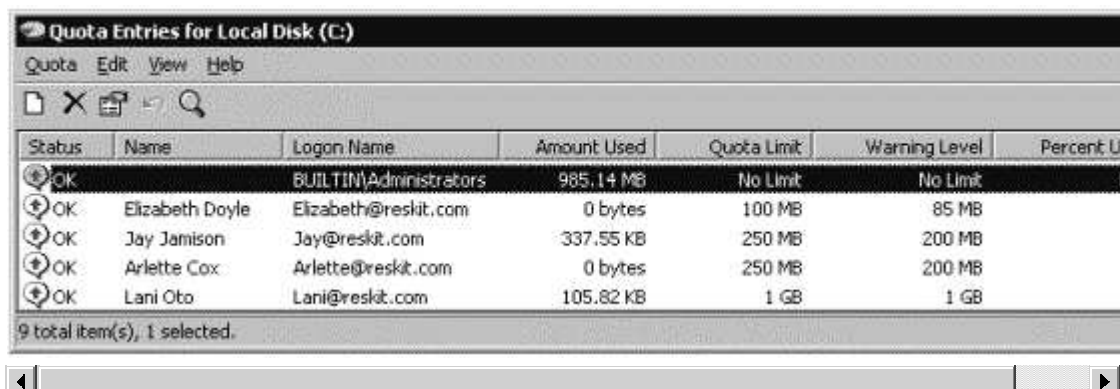


Figure 6.23 Add New Quota Entry

3. Enter the quota parameters desired for this user and click **OK**.

After you have entered all users who need to have quotas applied for this volume, their statistics display on the Quota Entry screen, and you can monitor their usage from this location.



Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent U
OK		BUILTIN\Administrators	985.14 MB	No Limit	No Limit	
OK	Elizabeth Doyle	Elizabeth@reskit.com	0 bytes	100 MB	85 MB	
OK	Jay Jamison	Jay@reskit.com	337.55 KB	250 MB	200 MB	
OK	Arlette Cox	Arlette@reskit.com	0 bytes	250 MB	200 MB	
OK	Lani Oto	Lani@reskit.com	105.82 KB	1 GB	1 GB	

9 total item(s), 1 selected.

If your browser does not support inline frames, [click here](#) to view on a separate page.

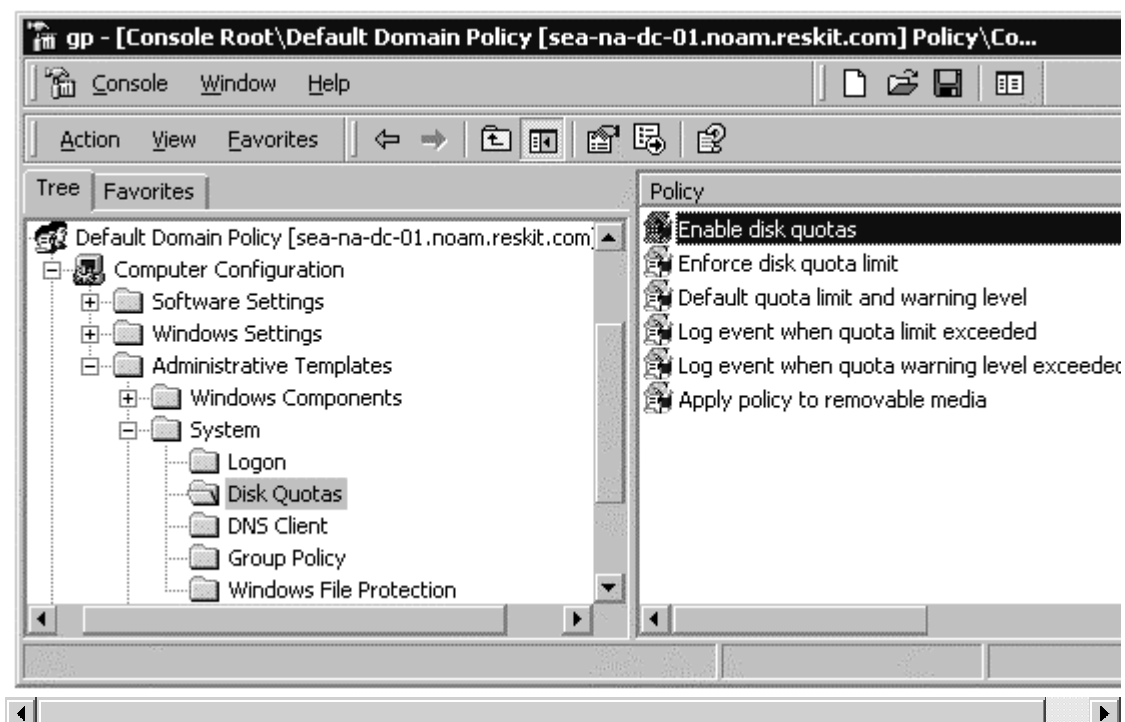
Figure 6.24 Disk Quota Entries

Group Policy Settings for Disk Quotas

You can use Group Policy to enable, enforce, and configure Disk Quotas.

To create disk quota settings

1. Open the **Group Policy** snap-in and navigate down to **Computer Configuration\Administrative Templates\System\Disk Quotas**.
2. The Group Policy settings you can apply are shown in Figure 6.25. For more information about any policy, double-click that policy, and click the **Explain** tab.



If your browser does not support inline frames, [click here](#) to view on a separate page.

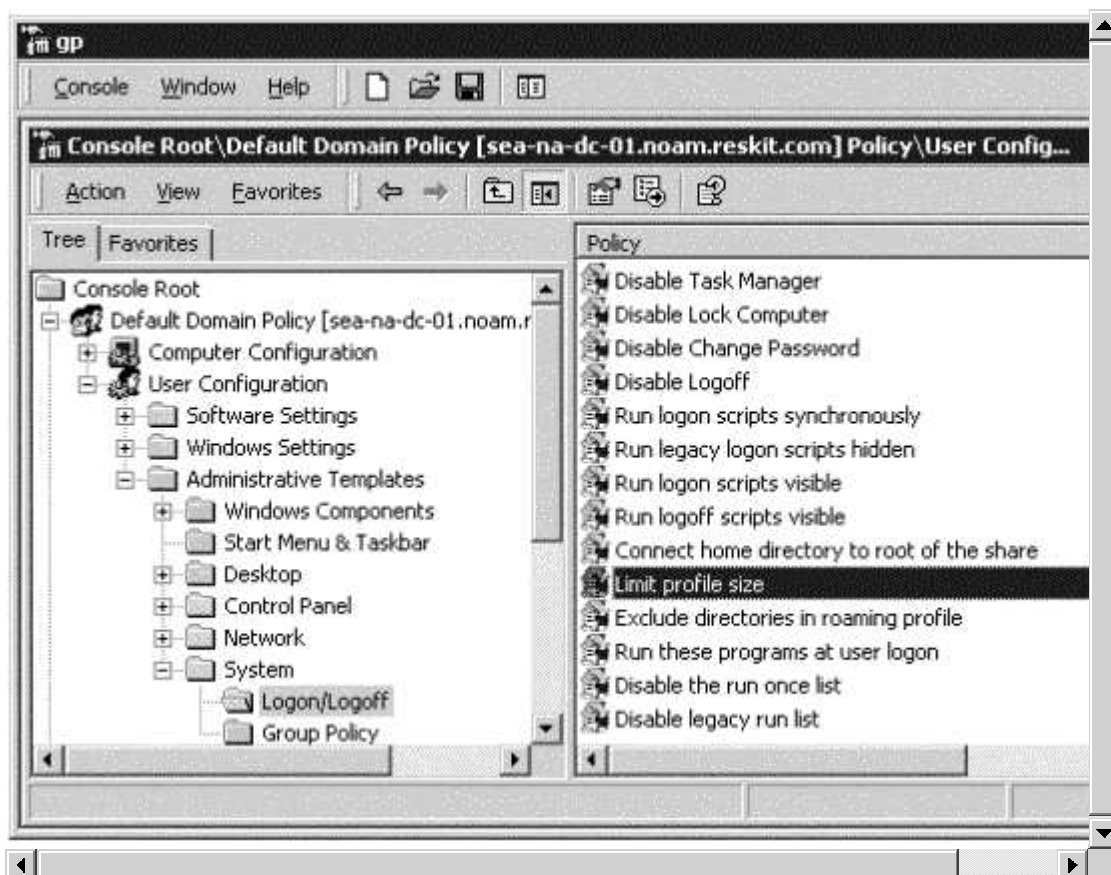
Figure 6.25 Group Policy Settings for Disk Quotas

Profile Quotas

You can use Group Policy to set size limitations on RUPs. Apply this setting with discretion, as it can be difficult for users to reduce the size of their profile if they exceed the size limitation.

To limit the size of user profiles

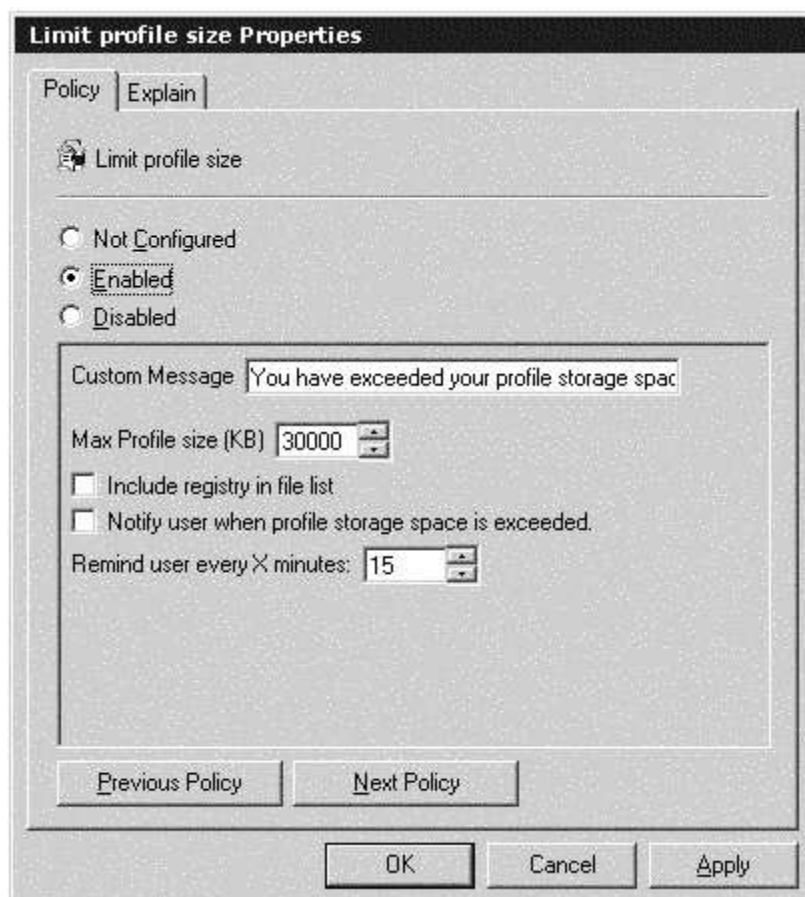
1. Open the **Group Policy** snap-in and navigate to **User Configuration\Administrative Templates\System\Logon/Logoff**.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.26 Limit Profile Size through Group Policy

2. Double-click **Limit Profile Size**, and then click **Enable**.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.27 Limit Profile Size Setting Options

3. Define your parameters for the profile quota and click **OK**.

From an administrative viewpoint, this is all that needs to be done to set profile quotas. When a user exceeds their profile quota, your custom message displays and they cannot log off until they reduce the size of their profile. In this case, the Proquota.exe program launches:

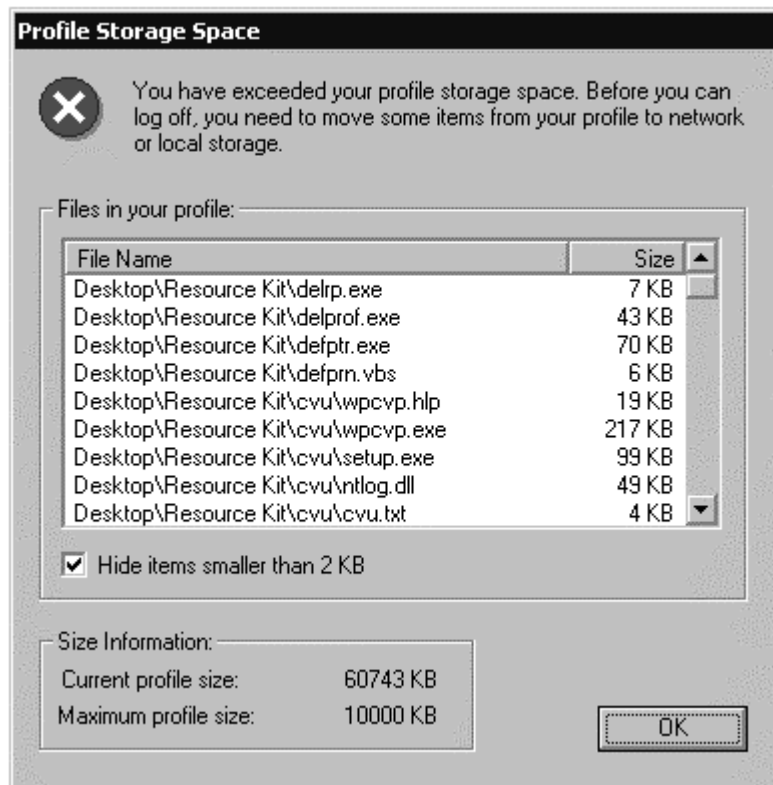


Figure 6.28 Profile Storage Space

Proquota dynamically tracks and displays the size of the profile as the user reduces it by opening My Computer or Windows Explorer, and manually deleting files from within the profile. When the current profile size is lower than the maximum profile size, the user is notified that they can log off.

Sample Scenarios

This section combines the information located throughout this chapter into some specific scenarios that might be useful models for implementing User Data and Settings Management in your organization. The following table provides general recommendations for using User Data and User Settings Management technologies for the various user and computer types that you read about in "Assessing Organization and User Needs" in this book. Use this information as a general framework within which to design your own IntelliMirror implementations.

Table 6.10 General Recommendations for Different User Scenarios

	Kiosk	Task Station	Application Station	PCE	Low TCO Desktop	Portable Computers (Mobile Users)
Users	1(anon)	Multiple	Multiple	Multiple	Multiple	1
RUP Enabled	No	Yes	Yes	Yes	Yes	Yes
Folder Redirection	N/A	My Docs App Data	My Docs App Data	My Docs App Data	My Docs App Data	Depends on usage
CSC Enabled	N/A	Network (Offline Files)	Network (Offline Files)	No	Network (Offline Files)	Network, Offline Files, Local

From this list, portable computers (mobile users), application stations, and low total cost of ownership (TCO) task stations are selected to illustrate implementation.

Portable Computers (Mobile Users)

A growing number of workers who travel perform a significant amount of their work using a portable

computer. These workers are frequently disconnected from the network, and usually reconnect to the network over low-speed lines.

In this scenario the mobile user travels and works primarily offsite, connects to the corporate network over a slow link from various locations and occasionally connects to the network using a LAN link. This user has a desktop computer at the home office that she also uses, so it is preferable that both her portable and desktop computers have the same settings.

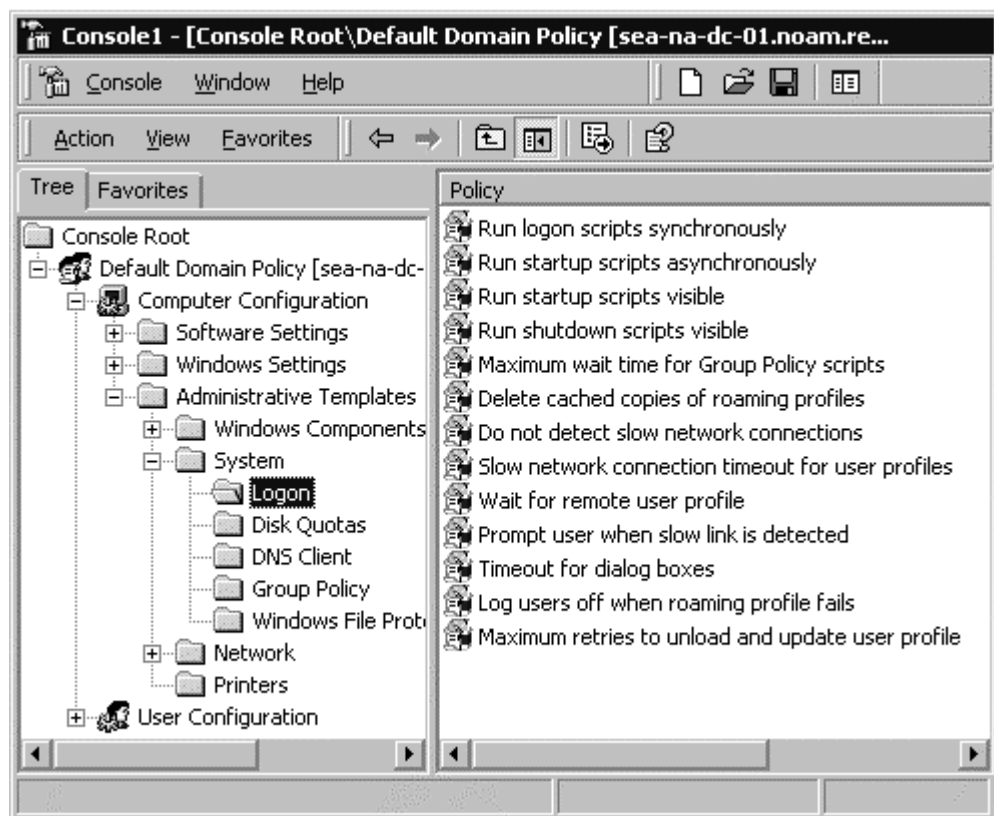
By default, Group Policy disables RUPs over slow links. It is recommended that you apply RUPs to your mobile users so that when they do log on over a fast link, their profile is saved to the server. This provides backup of the user state. If the user never logs on to the network over a fast link, or perhaps does so only once or twice a year, it is not useful to provide RUPs for that user.

If this mobile user connects at high speed from time to time, Folder Redirection and Offline Files are valuable for backup and synchronization benefits. By default, Folder Redirection and Offline Files follow the Group Policy setting to not travel over slow links. This default can be overridden using the Group Policy setting at **User Configuration\Administrative Templates\System\Group Policy\Group Policy Slow Link Detection**.

Warning If you change the default setting for Group Policy Slow Link Detection as described in the previous paragraph, all group policies are affected, and all Group Policy settings are applied over a slow link, including policies that install software, etc. This can cause unacceptably long logon times for users dialing in over a slow link.

For configuring multiple mobile users, set up an OU for mobile computers and apply the same settings to all users in that OU.

The RUP is used to update profiles only when the user connects the mobile computer over a fast link. The policies that can be configured for this are found under **Computer Configuration\Administrative Templates\System\Logon** in the Group Policy snap-in.



If your browser does not support inline frames, [click here](#) to view on a separate page.

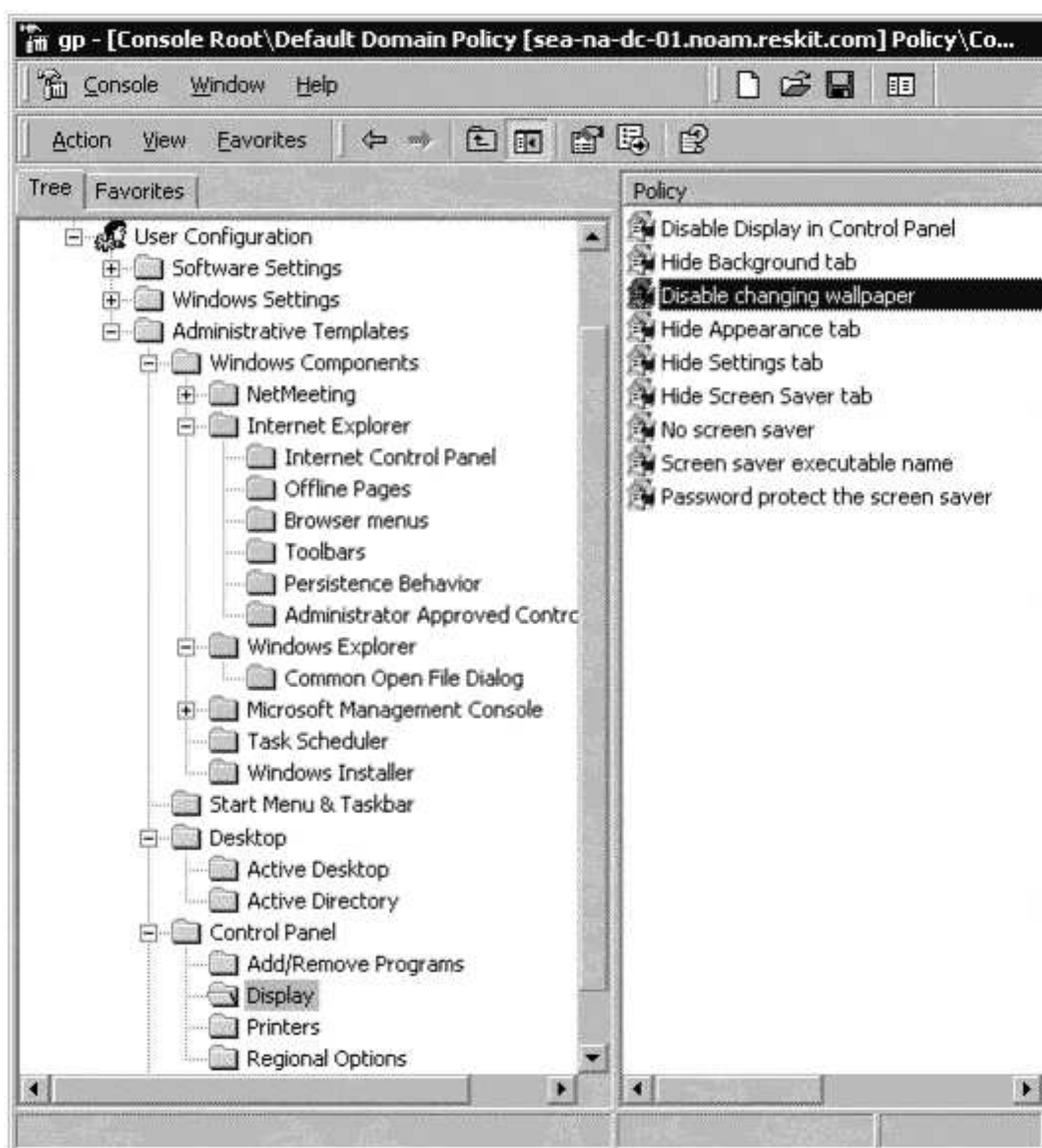
Figure 6.29 Group Policies for Restricting RUP Downloads

1. Set the Computer-level Policy to **Disabled** for **Do not detect slow network connections**. This restricts the user from disabling slow network detection.
2. Set the Computer-level Policy to **Enabled** for **Timeout for dialog boxes** and configure the setting to **1**. This effectively disables the messages the user otherwise receives, notifying them that they are not receiving RUPs because they are logging on over a slow link.
3. Set the Computer-level Policy to **Enabled**, and set a maximum wait time, for **Maximum wait time for Group Policy scripts**. This protects the user from having to wait through a long logon time over a slow link.

Application Station

An application station is set up with a restricted configuration. Users cannot customize the desktop, and they cannot add or remove programs. Multiple users might work on this computer. To support this scenario, RUPs, Folder Redirection, Offline Files, and server disk quotas must be implemented.

1. Set up Roaming User Profiles for users who use application stations, so that their settings follow them to any computer they use. See the preceding steps for implementing RUPs.
2. Set up Folder Redirection and Offline Files. Any files that are redirected must be set as Offline Files, so that in event of network disconnection, the users can continue to work on their important files.
3. Set up Disk Quotas on the servers that contain redirected folders so that individual users cannot use too much disk space.
4. If you have many users accessing the same computer, apply the **Group Policy Computer Configuration\Administrative Templates\System\Logon\Delete cached copies of roaming profiles** setting to remove cached versions of roaming profiles when the users log off.
5. Use Group Policy to restrict users' abilities to change the desktop. These settings must be directed at the OU which contains the users and/or computers to which the policies are to be applied. The screenshot below illustrates some of the policy settings for restricting the desktop as much or as little as you desire. Go into the Group Policy snap-in and navigate through these options; double-click any policy and then click its **Explain** tab for details on how and when to use each policy.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 6.30 Group Policies for Restricting the Desktop

Low TCO Workstations

Lower TCO workstations are usually a good solution for power users or knowledge workers who require a lot of control over their computers, such as software developers or Certified Public Accountants. This scenario illustrates an organization where tightly managed desktops are not acceptable to users.

1. Set up Roaming User Profiles for users who use application stations, so that their settings follow them to any computer they use.
2. Set up Folder Redirection and Offline Files. Any files that are redirected must be set as Offline Files, so that in event of network disconnection, the users can continue to work on their important files.
3. Set up Disk Quotas on the servers that contain redirected folders so that individual users cannot use too much disk space.
4. Do not use Group Policy settings to restrict the user's ability to control their desktop or computer.

By becoming familiar with Group Policy and User Data and Settings Management functionality, you can match the needs of your users with the combination of features that makes their data and settings accessible, secure, and manageable.

[Send feedback to Microsoft](#)

© 2004 Microsoft Corporation. All rights reserved.