

Deploying User Profiles

In this chapter:

Exploring User Profiles	306
Getting User Profiles	314
Using Roaming User Profiles	316
Deploying Default User Profiles.....	323
Coexisting with Earlier Versions of Windows.....	330
Migrating User Settings to Windows	330

Microsoft Windows XP and Microsoft Windows Server 2003 (Windows) store user settings separate from computer settings. The computer's settings affect every user who logs on to Windows. Computer settings include hardware configuration, network configuration, and so on. Typically, only the Administrators group can change computer settings, but some settings are within reach of the Power Users group. On the other hand, a user profile contains settings for a specific user. Users customize the operating system to their liking, and their settings don't affect other users. Users have full control of their own profiles, which contain more than just settings. They also contain files and folders specific to each user.

Deploying and managing user profiles are two of the most significant issues facing IT professionals. Properly deploying and managing user profiles can save companies money. That's because most of the behaviors that users experience in Windows have settings in user profiles, and IT professionals can deploy user profiles that contain defaults for these settings, starting users off correctly. For example, they can populate the Favorites folder with links to the intranet so that users don't have to find those links for themselves. They can add printer connections to a default user profile so that users can print right away without having to figure out how to add a printer. Notice that most of the useful policies that manage operating system and application settings are in user profiles. IT professionals manage the settings in user profiles by applying policies to them.

Mastering user profiles isn't just for IT professionals; power users, particularly those who use multiple accounts on their computers or who work on a home network, can create user profiles to simplify their experience. They can customize a default user profile. Then whenever they reinstall Windows or create a new account, they start

with familiar settings and don't have to spend an hour customizing the operating system to suit their tastes. User profiles aren't that complicated, and power users should use them to their full advantage.

I've written this chapter primarily for the IT professional; power users need master only portions of it. First you learn about the contents of a user profile. Then you learn how to use roaming user profiles on a business network. The most compelling part of this chapter shows you how to build and deploy default user profiles. In that part, I show you two techniques for building default user profiles. The first is traditional but rather messy. I prefer the second method, which is a more precise (and tidy) method of building default user profiles. I wrap up this chapter with a discussion of the Microsoft User State Migration Tool, which can help overcome the difficulties involved with migrating users' settings from earlier versions of Windows.

Exploring User Profiles

Windows loads users' profiles when they log on to a computer and unloads their profiles when they log off. A user profile contains a registry hive with per-user settings and folders, which contain documents and data files. The next section, "Profile Hives," describes the registry hive that the operating system loads. The section "Profile Folders" describes the folders in a user profile.

Before delving into the contents of user profiles, knowing their location on the file system is useful. The default location is different than it was in Microsoft Windows NT 4.0 or other operating systems of that era. Remember that Windows NT 4.0 stored user profiles in %SystemRoot%\Profiles, but this location made it difficult to secure the operating system files while allowing access to users' data. Windows 2000, Windows XP, and Windows Server 2003 store user profiles in a different location, which enables you to pull user data out from under an operating system folder: %SystemDrive%\Documents and Settings, C:\Documents and Settings on most computers. This is the case only with a clean installation of Windows, however.

If you upgrade from a version of Windows earlier than Windows 2000, the profiles remain where they were in the previous operating system. For example, if you upgrade from Windows NT 4.0 to Windows XP or Windows Server 2003, the profiles remain in %SystemRoot%\Profiles. The location of user profiles after upgrading from Windows 2000 to Windows XP or Windows Server 2003 depends on whether you installed Windows 2000 cleanly or upgraded from an earlier version of Windows. In other words, the setup program never moves user profiles during an upgrade.

Windows creates and stores a list of user profiles. Table 12-1 shows the locations of user profiles depending on the scenario. The key `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList` corresponds to the list you see in the User Profiles

dialog box. To open the User Profiles dialog box, from Control Panel, launch System, and in the System Properties dialog box, on the Advanced tab, click Settings in the User Profiles frame. Each subkey is a user profile, and the subkey's name is the Security Identifier (SID) of the account that owns the profile. Each profile in `ProfileList` contains the `REG_SZ` value `ProfileImagePath` that points to a user profile folder in `%SystemRoot%\Documents and Settings`. Figure 12-1 illustrates the relationship between the `ProfileList` key and the user profile folders. This relationship is the reason that you shouldn't just remove a user profile from the file system. Instead, use the User Profiles dialog box to remove user profiles, which cleans the user profile out of the `ProfileList` key as well as off the file system.

Table 12-1 Location of User Profiles

Scenario	Location
Clean installation	<code>%SystemDrive%\Documents and Settings</code>
Upgrade from Windows 2000	<code>%SystemDrive%\Documents and Settings</code>
Upgrade from Windows NT 4.0	<code>%SystemRoot%\Profiles</code>
Upgrade from Windows 98	<code>%SystemDrive%\Documents and Settings</code>

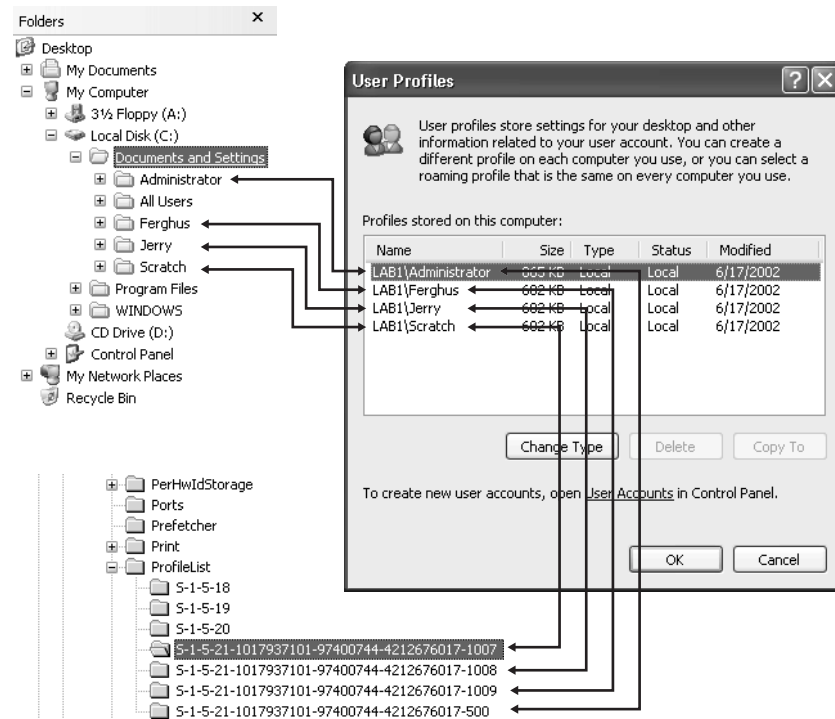


Figure 12-1 The subkeys of `ProfileList` contain a wealth of information about the user profiles that Windows has created, including their paths on the file system.



Note In enterprises that use Windows NT 4.0, IT professionals sometimes move profiles to %SystemRoot%\Profiles when deploying Windows because managing the profiles is often easier if they are in the same location regardless of the platform. Windows answer files offer a setting that enables you to do that. The setting is `ProfilesDir`, and it's in the `[GuiUnattended]` section. Set `ProfilesDir` to the path of the folder in which you want to store profiles. You should begin the path with either %SystemRoot% or %SystemDrive%; otherwise, the setup program ignores it.

Advantages of User Profiles

The primary goal of user profiles is to keep each user's settings and data distinct from that of other users as well as from the computer's settings. This separation has several advantages for enterprise environments and makes Windows more convenient to use at home, too. User profiles enable *stateless* computing. A company can configure Windows to store key user settings and data separately from the computer. This makes backing up and replacing computers much easier because users' data is stored on the network and maintained separately from the computer's configuration. The first time users log on to a replacement computer, the operating system copies their settings from the network, allowing them to get back to work more quickly.

Roaming user profiles also allow users' settings to follow them from computer to computer. They don't have to reconfigure settings at each computer. When they log on to a network that supports roaming user profiles, the operating system downloads their settings from the network. When they log off the computer, the operating system copies users' settings back to the network. Roaming user profiles make sharing computers more feasible because each user has his or her personalized configuration. Roaming user profiles are a must-have in environments such as call centers, where users aren't guaranteed to sit down at the same computer twice. You learn about roaming user profiles in the section "Using Roaming User Profiles," later in this chapter.

Profile Hives

The first half of a user profile is the profile hive: NTUSER.DAT. You learn about the second half in the next section, "Profile Folders." This profile hive is in the root of users' profile folders. Chapter 1, "Learning the Basics," and Chapter 2, "Using Registry Editor," describe hive files and how to work with them. Users' operating system and application settings are stored in profile hives. For example, you find all the per-user settings for Windows Explorer and persistent network connections in profile

hives. Profile hives also contain per-user taskbar, printer, and Control Panel settings. Accessories that come with Windows store per-user settings in the profile hive.

When Windows loads a user profile, the operating system loads the hive file NTUSER.DAT into the subkey `HKU\SID`, where `SID` is the user's SID. (See Chapter 1, "Learning the Basics," for more information about SIDs.) Then Windows links the root key `HKCU` to `HKU\SID`. Figure 12-2 shows this relationship. Windows and most applications reference users' settings through `HKCU`, not `HKU\SID`, because `HKCU` resolves which subkey of `HKU` contains the console user's settings. `HKU` contains a second hive file, `HKU\SID_Classes`, which contains per-user file associations and class registrations. You learn about this in Appendix A, "File Associations."

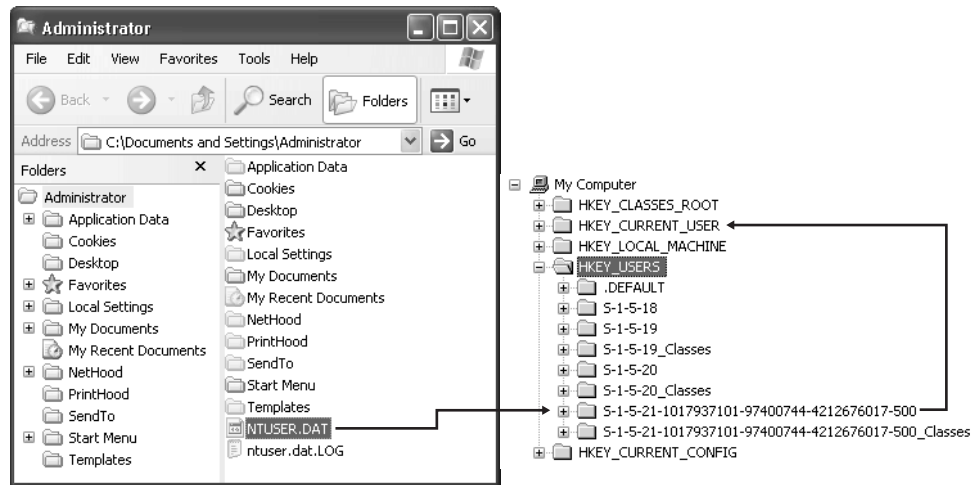


Figure 12-2 Windows loads NTUSER.DAT into `HKU\SID` and then links `HKCU` to it.

The list of profile hives is in the key `ProfileList`, which you learned about in the previous section. It contains one subkey for each user profile. The subkey's name is the name of the hive in `HKU` or the account's SID. The `REG_SZ` value `ProfileImagePath` is the path of the profile hive file NTUSER.DAT for that user profile. `ProfileList` does not contain a value for the `SID_Classes` hives, however. `HKLM\SYSTEM\CurrentControlSet\Control\hiveList` contains one `REG_SZ` value for each hive in `HKLM` and `HKU` that the operating system is currently using. The difference between the values `ProfileList` and `hiveList` is that `ProfileList` contains a list of all user profiles that Windows knows about, loaded or not, and `hiveList` contains a list of all currently loaded hive files.



Tip You can load and edit profile hives in Registry Editor (Regedit) without logging on to the computer using the account that owns that user profile. This is one of the techniques that you use later in this chapter to build default user profiles.

Profile Folders

The folders in a user profile contain per-user application files. For example, Microsoft Office 2003 Editions installs templates and custom dictionaries in the user profile. Microsoft Internet Explorer stores its cookies and shortcuts in the user profile. The most interesting folder in a user profile is the Application Data folder. Figure 12-3 shows a user profile in Windows Explorer. Some of the folders are hidden; show the hidden files in Windows Explorer if you want to see the following folders for yourself:

- **Application Data.** This folder contains application files, such as mail files, shortcuts, templates, and so on. Each application's vendor chooses what files to store here. You can redirect this folder to a network location using Group Policy.
- **Cookies.** This folder contains Internet Explorer cookies.
- **Desktop.** This folder contains files, folders, and shortcuts on the desktop. Users see the contents of this folder on the Windows desktop. You can redirect this folder to a network location using Group Policy.
- **Favorites.** This folder contains Internet Explorer favorite shortcuts. Users see the contents of this folder on Internet Explorer's Favorites menu. Group Policy doesn't support redirecting this folder, but you can redirect it manually as shown in Chapter 18, "Fixing Common IT Problems."
- **Local Settings.** This folder contains application files that do not roam with the profile. The files you find in this folder are either per-computer or too large to copy to the network. This folder contains four interesting subfolders:
 - **Application Data.** This subfolder contains computer-specific application data.
 - **History.** This subfolder contains Internet Explorer history.
 - **Temp.** This subfolder contains per-user temporary files.
 - **Temporary Internet Files.** This subfolder contains Internet Explorer offline files.
- **My Documents.** This folder contains the default location for users' documents. Applications should save users' documents to this folder by default, and this is the location to which the common dialog boxes open by default. This folder also contains the My Pictures folder, which is the default location for users' pictures, and optionally the My Music folder, which is the default location for users' music files. You can redirect this folder to a network location using Group Policy.
- **NetHood.** This folder contains shortcuts to objects on the network. Users can browse the folders to which these shortcuts are linked in the My Network Places folder.
- **PrintHood.** This folder contains shortcuts to printer objects. Users see the contents of this folder in the Printers folder.

- **Recent.** This folder contains shortcuts to the most recently used documents. Users see these shortcuts on the My Recent Documents menu, which is on the Start menu.
- **SendTo.** This folder contains shortcuts to drives, folders, and applications that are copy targets. Users see the contents of this folder when they right-click an object and then click Send To.
- **Start Menu.** This folder contains shortcuts to program items. Users see the contents of this folder on the Start menu and on the Start menu's All Programs menu. IT professionals can redirect this folder to a network location using Group Policy.
- **Templates.** This folder contains template files. Users see the contents of this folder when they right-click in a folder and then click New.

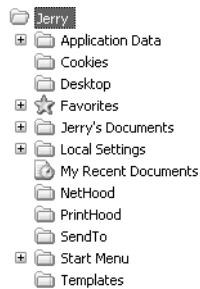


Figure 12-3 The user profile folders that you see in this figure are the default folders in a clean installation of Windows.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders is the key where Windows stores the location of each folder that's part of a user profile. Each value in this key represents a folder, as shown in Table 12-2. These are REG_EXPAND_SZ values, so you can use environment variables in them. Use %UserProfile% to direct the folder somewhere inside users' profile folders and %UserName% to include users' names, particularly when you want to redirect a profile folder to a network location. Redirect users' Favorites folders to the network by setting Favorites to \\Server\Share\%UserName%\Favorites, where \\Server\Share is the server and share containing the folders, for example. Windows does not use the similar key Shell Folders.

Table 12-2 User Profile Folders

Name	Default Path
AppData	%UserProfile%\Application Data
Cache	%UserProfile%\Local Settings\Temporary Internet Files
Cookies	%UserProfile%\Cookies
Desktop	%UserProfile%\Desktop
Favorites	%UserProfile%\Favorites

Table 12-2 User Profile Folders

Name	Default Path
History	%UserProfile%\Local Settings\History
Local AppData	%UserProfile%\Local Settings\Application Data
Local Settings	%UserProfile%\Local Settings
My Pictures	%UserProfile%\My Documents\My Pictures
NetHood	%UserProfile%\NetHood
Personal	%UserProfile%\My Documents
PrintHood	%UserProfile%\PrintHood
Programs	%UserProfile%\Start Menu\Programs
Recent	%UserProfile%\Recent
SendTo	%UserProfile%\SendTo
Start Menu	%UserProfile%\Start Menu
Startup	%UserProfile%\Start Menu\Programs\Startup
Templates	%UserProfile%\Templates

Special Profiles

The profile folders you saw in Figure 12-1 contain more than the standard user profiles that Windows creates when users log on to the operating system. The following describes four special user profiles about which any IT professional should learn:

- **All Users.** This profile folder contains settings that apply to all users who log on to the computer. This profile folder contains a profile hive, NTUSER.DAT, which the operating system doesn't load. Also, this profile folder contains the shared documents and music folders, shared Start menu shortcuts, and so on. The key `User Shell Folders` in `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer` contains the linkages to the subfolders in the All Users profile folder.
- **Default User.** This profile folder contains the default user profile that Windows copies when it creates new user profiles. It contains most of the files and folders that you learned about in the previous section. Customizing this folder is a good way to start each user who logs on to the computer with the same settings. Windows first checks for a Default User folder on the NETLOGON share of the server and uses the local Default User folder only if the network copy isn't available. Customizing this folder is a good way to deploy settings that you don't want to manage. You learn how to customize it in the section "Deploying Default User Profiles," later in this chapter.
- **LocalService.** This profile folder is for the built-in LocalService account, which Service Control Manager uses to host services that don't need to run under the LocalSystem account. This is a normal user profile with limited data. You don't see it in the User Profiles dialog box, and the LocalService folder is super-hidden.

- **NetworkService.** This profile folder is for the built-in NetworkService account, which the Service Control Manager uses to host network services that don't need to run under the LocalSystem account. This is a normal user profile. You don't see it in the User Profiles dialog box, and the NetworkService folder is super-hidden.

In the previous list, the first two profile folders are far more interesting than the last two. IT professionals often customize the All Users profile folder on disk images. The customization, such as a shortcut on the Start menu, affects all users who log on to the computer. However, IT professionals more frequently customize the Default User folder. Doing so is a great way to create custom settings that you don't want to manage. In other words, it's one method for deploying common user preferences while still allowing users to change those preferences if necessary. As you'll learn throughout this chapter, customizing the Default User folder on a disk image isn't necessarily the most efficient means to deploy default user settings. Instead, create a customized Default User folder on the server's NETLOGON share. See the section "Deploying Default User Profiles," later in this chapter.



Tip Many programs install themselves for use by a single user when you really want all users who share the computer to use them. You can tell when a program is installed per-user because its shortcut is in the profile folder belonging to the account you used to install it. If the program re-creates missing settings as it starts, you can change the program from per-user to per-computer by simply moving its shortcut from the user profile folder in which it installed the shortcut to the All Users profile folder. This works the other way, too. You can move a shortcut from the All Users profile folder to a specific user's profile folder so that only a single user sees the shortcut.

Improvements to User Profiles

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

- The user experience is affected because changes are not saved when users log on to another computer.
- Because *locked* profiles never get unloaded, they end up using a lot of memory on a terminal server that has many users logging on to it.
- If a profile is marked for deletion at logoff (to clean up the machine or for temporary profiles), profiles do not get deleted.

The three symptoms are solved as follows:

- In Windows, when a user logs off and the profile is locked, the operating system polls the profile for 60 seconds before giving up. Windows then saves the user's profile hive and roams the profile correctly.
- When the application or service closes the registry key and unlocks the profile, Windows unloads the user's profile hive, freeing memory used by the profile.
- If a profile is marked for deletion, when the reference count drops to zero, Windows unloads and deletes it. In the event that the application never releases the registry key, Windows deletes all profiles marked for deletion at the next machine boot.

Getting User Profiles

How users get their profiles depends on the type of profile you've configured their accounts to use:

- **Local user profile.** This profile is created the first time users log on to their computers. Local user profiles are stored on the local hard disk. Changes that users make to their profiles don't follow them from computer to computer.
- **Roaming user profile.** This profile is available to users from any computer on the network, and changes that users make to their profiles follow them from computer to computer.
- **Mandatory user profile.** This profile is similar to roaming user profiles. Administrators assign mandatory user profiles to users, and Windows throws away users' changes when they log off the operating system. In other words, users start with the same settings every time they log on to the operating system. Microsoft provides mandatory user profiles to provide compatibility with Windows NT 4.0, but you should consider using Group Policy instead.

The following sections describe how Windows creates a profile when users log on to the operating system. The section "Using Roaming User Profiles" describes how to create and manage roaming user profiles. Also, the section "Managing Roaming User Profiles" shows you how to prevent Windows from merging the local copy of a profile with the server copy by using Group Policy.

Local Profiles

Here's an overview of how Windows creates and uses a local user profile for users the first time they log on to their computers:

1. The user logs on to Windows.

2. Windows checks the list of user profiles in the key `ProfileList` to determine if a local profile exists for the user. If an entry exists, the operating system uses it; otherwise, the operating system does one of the following:
 - ❑ If the computer is a domain member, Windows checks the NETLOGON share on the domain controller for a default user profile in a subfolder named Default User. If it exists, the operating system copies NETLOGON\Default User to %SystemDrive%\Documents and Settings*Username*, where *Username* is the name of the user's account.
 - ❑ If the computer is not a domain member or if Windows doesn't find a default user profile on the NETLOGON share, it uses the local default user profile. It copies %SystemDrive%\Documents and Settings\Default User to %SystemDrive%\Documents and Settings*Username*.
3. Windows loads the profile hive NTUSER.DAT into `HKEY_CURRENT_USER` and links the root key `HKEY_CURRENT_USER` to it.

When the user logs off Windows, the operating system saves any changes to the profile in the user profile folder. It doesn't copy the profile folder to the network. It also unloads the profile hive from the registry.

Roaming Profiles

Here's an overview of how Windows creates and uses a roaming user profile for users the first time they log on to their computers:

1. The user logs on to Windows.
2. Windows checks the list of user profiles in the `ProfileList` key to determine whether a local profile exists for the user. If an entry exists, the operating system merges the network copy of the profile into the local profile folder; otherwise, the operating system does one of the following:
 - ❑ Windows checks the NETLOGON share on the domain controller for the Default User folder. If the folder exists, the operating system copies the Default User folder to %SystemDrive%\Documents and Settings*Username*, where *Username* is the name of the user's account.
 - ❑ If Windows doesn't find a default user profile on the NETLOGON share, it copies %SystemDrive%\Documents and Settings\Default User to %SystemDrive%\Documents and Settings*Username*.
3. Windows loads the profile hive NTUSER.DAT into `HKEY_CURRENT_USER` and links the root key `HKEY_CURRENT_USER` to it.

When users log off Windows, the operating system saves their changes to the local profile folders and then unloads the profile hives from `HKEY_CURRENT_USER`. Afterward, the operating system copies their profile folders to the network location specified by the administrator.

If the profile folder already exists on the network, the operating system merges the local copy into the network copy. For more information, see “Understanding the New Merge,” later in this chapter.



Note There are two differences between roaming and mandatory user profiles. First, you create the mandatory profile and copy it to the user’s profile folder instead of allowing Windows to create it when the user logs on to the computer. Second, you rename the NTUSER.DAT to NTUSER.MAN. Windows uses the .MAN file extension to make the profile mandatory. Windows doesn’t merge mandatory user profiles to the network when the user logs off the computer.

Using Roaming User Profiles

You configure roaming user profiles on the server, so the user must be a member of and log on to the domain to use a roaming user profile. Both Microsoft Windows NT Server 4.0 and Microsoft Windows 2000 Server support roaming user profiles, as do Microsoft Windows XP and Windows Server 2003. The following instructions show you how to configure roaming user profiles in Active Directory on Windows Server 2003:

1. Create a folder on the server where you want to store user profiles. This is the top-level folder that will contain individual user profile folders.
2. Share the folder, giving all users full control. (I sometimes reduce users’ permissions to read and execute in this folder and then give them full control of their individual profile folders.)
3. In the Active Directory Users and Computers console, double-click the account that you want to configure to use a roaming user profile.
4. On the Profile tab of the *Name* Properties dialog box, shown in Figure 12-4, type the path where you want to store the user’s profile in the Profile Path text box. The path is `\\Server\Share\Username`, where *Server* is the name of the server, *Share* is the share you created in step 2, and *Username* is the name of the account. Optionally, use `%UserName%` for *Username*, and Active Directory will automatically substitute the current account’s name in its place.

If you want to configure a lot of accounts to use roaming user profiles, doing the job by hand is a monumental task. Instead, use a third-party tool or write an Active Directory Scripting Interface (ADSI) script to do the job. You access ADSI through Windows Script Host using Microsoft Visual Basic Scripting Edition (VBScript) or JScript.



More Info This subject is beyond the scope of this book, but you can find more information about ADSI scripting at http://www.microsoft.com/resources/documentation/windows/2000/server/scriptguide/en-us/sas_ads_overview.msp.

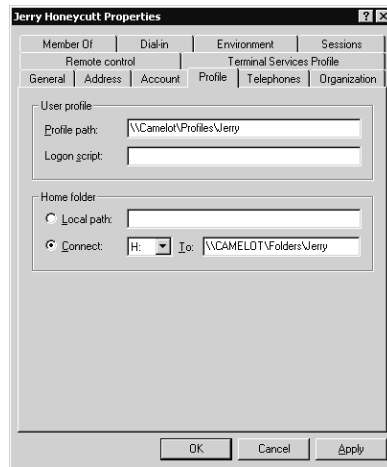


Figure 12-4 Typing a path in the Profile Path box is all that it takes to enable roaming user profiles.

Folder Redirection is a great complement to user profiles, particularly the roaming variety. It enables an IT professional to redirect the location of some profile folders to the network. There's nothing magical about Folder Redirection. Group Policy simply changes the folder's location in the `user Shell Folders` key so that applications automatically look for the folder on the network. From users' perspectives, redirected folders are similar to roaming user profiles because their documents follow them from computer to computer. Unlike roaming user profiles, however, redirected folders always remain in the same place. You can use redirected folders with or without roaming user profiles. If you use them with roaming user profiles, you can reduce the amount of data that Windows transfers when users log on to and off from the operating system. Furthermore, redirected folders are often useful even when you don't intend to use roaming user profiles; you can allow users' documents to follow them without the complexity and sometimes difficulty of using roaming user profiles. You learn about roaming user profiles in the earlier section "Getting User Profiles." Table 12-3 indicates for each profile folder whether the folder can roam and whether you can redirect it.

Table 12-3 Roaming and Redirecting Folders

Folder	Can Roam?	Can Redirect?
Application Data	Yes	Yes
Cookies	Yes	No
Desktop	Yes	Yes
Favorites	Yes	No
Local Settings	No	No
My Documents	Yes	Yes
My Recent Documents	Yes	No

Table 12-3 Roaming and Redirecting Folders

Folder	Can Roam?	Can Redirect?
NetHood	Yes	No
PrintHood	Yes	No
SendTo	Yes	No
Start Menu	Yes	Yes
Templates	Yes	No

Best Practices for Roaming User Profiles

The following are best practices for roaming user profiles:

- Redirect the My Documents folder outside of roaming user profiles. Doing so decreases logon time. Folder Redirection is the best way to do this, but you can redirect the My Documents folder manually, as Chapter 18, “Fixing Common IT Problems,” describes.
- Don’t use Encrypted File System (EFS) on files in a roaming user profile. EFS is not compatible with roaming user profiles. Encrypting a roaming user profile prevents the user profile from roaming.
- Don’t make disk quotas for roaming user profiles too restrictive. If they’re too low, roaming user profile synchronization might fail. The server debits the user’s quota for temporary files that Windows creates during the synchronization process, so ensure that enough disk space is available on the server. Also, make sure enough disk space is available on the workstation to create temporary duplicate copies of the profile.
- Don’t make folders in roaming user profiles available offline. If you use Offline Folders with roaming user profile folders, synchronization problems occur because both Offline Folders and roaming user profiles try to synchronize at the same time. However, you can use Offline Folders with folders that you redirect, such as My Documents.
- Use Group Policy loopback policy processing in moderation if you’re also using roaming user profiles. Loopback processing enables you to apply different per-user Group Policy settings to users based on the computer they’re using.
- When redirecting the My Documents folder outside of a roaming user profile, set the home folder to the redirected My Documents folder for compatibility with applications that aren’t compatible with folder redirection.
- Disable fast network logon using Group Policy if you’re using roaming user profiles. This prevents conflicts that occur when user profiles change from local to roaming. For more information, see “Understanding Fast Network Logon,” later in this chapter.



More Info You can get a detailed explanation of loopback processing at <http://support.microsoft.com/default.aspx?scid=kb;en-us;231287>.

Managing Roaming User Profiles

Group Policy provides a number of policies that you can use to manage how Windows handles user profiles. You can configure these policies in a local Group Policy Object (GPO) or in a network GPO. Chapter 7, “Using Registry-Based Policy,” gives more information. For now, here’s a description of policies for user profiles:

- **Connect home directory to root of the share.** This policy restores the definitions of the %HomeShare% and %HomePath% environment variables to those used in Windows NT 4.0 and earlier.
- **Limit profile size.** This policy sets the maximum size of each roaming user profile and determines the system’s response when a roaming user profile reaches the maximum size. If user profiles become excessively large, consider redirecting the My Documents folder to a location outside of the profile.
- **Exclude directories in a roaming profile.** This policy enables you to add to the list of folders excluded from the user’s roaming profile.
- **Delete cached copies of roaming profiles.** This policy determines whether the system saves a copy of a user’s roaming profile on the local computer’s hard disk when the user logs off.
- **Do not detect slow network connections.** This policy disables the slow link detection feature.
- **Slow network connection timeout for user profiles.** This policy defines a slow connection for roaming user profiles.
- **wait for remote user profile.** This policy directs the system to wait for the remote copy of the roaming user profile to load, even when loading is slow. Also, the system waits for the remote copy when the user is notified about a slow connection, but the user does not respond in the time allowed.
- **Prompt user when slow link is detected.** This policy notifies users when their roaming profile is slow to load. Users can then decide whether to use a local copy or to wait for the roaming user profile.
- **Timeout for dialog boxes.** This policy determines how long the system waits for a user response before it uses a default value.
- **Log users off when roaming profile fails.** This policy logs a user off automatically when the system cannot load the user’s roaming user profile.

- **Maximum retries to unload and update user profile.** This policy determines how many times the system will try to unload and update the profile hive. When the number of trials specified by this setting is exhausted, the system stops trying. As a result, the user profile might not be current, and local and roaming user profiles might not match.
- **Add the Administrators security group to roaming user profiles.** This policy adds the Administrators security group to the roaming user profile share. The default behavior prevents administrators from managing individual profile folders without taking ownership of them.
- **Prevent Roaming Profile changes from propagating to the server.** This policy determines if the changes a user makes to his or her roaming profile are merged with the server copy of their profile. This is a policy-based method for implementing mandatory user profiles.
- **Only allow local user profiles.** This policy determines if roaming user profiles are available on a particular computer. By default, when roaming-profile users log on to a computer, their roaming profile is copied to the local computer. If they have already logged on to this computer in the past, the roaming profile is merged with the local profile. Similarly, when the users log off this computer, the local copy of their profile, including any changes they have made, is merged with the server copy of their profile.

The first three policies in this list are per-user and the remaining are per-computer policies; Figure 12-5 shows them in Group Policy Editor. All of the policies are administrative policies in System\User Profiles under User Configuration and Computer Configuration.

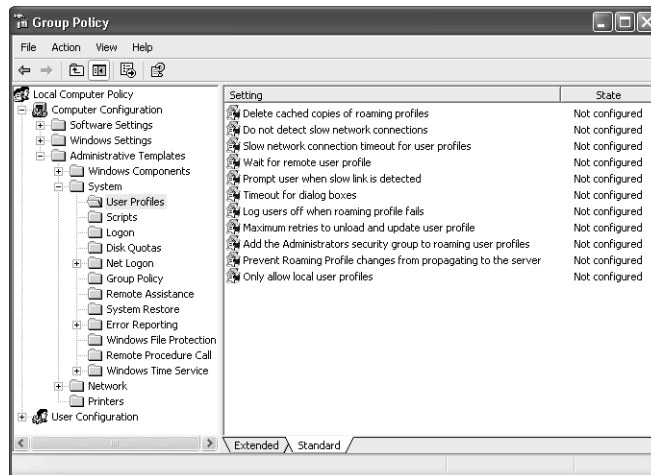


Figure 12-5 These policies give you management control of how Windows uses profiles.

Understanding Fast Network Logon

Windows doesn't wait for the network to start before displaying the Logon To Windows dialog box. This substantially improves start time over Windows 2000. Users who've previously logged on to the computer get to their desktops faster because the operating system uses cached credentials and loads Group Policy in the background after the network becomes available. Although fast network logon improves perceived performance, it has effects that you should understand. The most important fact to understand in this section is that Windows doesn't use fast network logon if you use roaming user profiles.

Because background refresh is the default behavior, users might have to log on to Windows up to three times for Group Policy extensions such as Software Installation and Folder Redirection to take effect. Windows must process these types of extensions in the background without any users logged on to it. Also, because advanced Folder Redirection is based on group membership, users must log on to Windows three times: once to update the cached user object and group membership, a second time to detect the change in group membership and require a foreground policy application, and a third time to apply folder redirection policy in the foreground. The operating system might require users to log on two times to update the properties of other Group Policy objects.

Another thing to keep in mind is the effect that fast network logon has on Windows when users' profiles change from local to roaming. When the operating system uses fast network logon, it always uses the locally cached copy of the profile. By the time the operating system detects that the user has a roaming user profile, it's already loaded the local profile hive and changed its time stamp. The result is that if users log on to multiple computers, the operating system can replace newer profile hives with older ones. To handle this scenario, Windows treats the change from local to roaming as a special case. First the operating system checks the following conditions:

- Is the user changing from a local to a roaming profile?
- Is a copy of the user profile on the server?

If both these conditions are true, then Windows merges the contents of the local user profile with the server copy, without the profile hive NTUSER.DAT. Then the operating system copies the server copy of the profile to the local copy, regardless of the profile hives' time stamps. After the user's profile becomes a roaming profile, Windows always waits for the network so that it can download the user profile. In other words, fast network logon and roaming user profiles don't work together.



Caution Considering the changes that Windows makes to roaming user profiles, if you remove the roaming profile path from a user in Active Directory, you should remove the profile folder from the server. If you reconfigure the user to use roaming user profiles and you use the same path, the user will receive the older server copy of the user profile.

Understanding the New Merge

Many IT professionals are reluctant to use roaming user profiles because they have experience with the merge algorithm that Windows NT 4.0 uses. That algorithm assumes that there is a single master copy of the user profile. When the user logs on to the computer, the operating system assumes that the master profile is on the local computer, and when the user logs off the computer, it assumes that the master profile is on the server. It mirrors the entire profile from the local computer to the server and vice versa, completely replacing the profile at the target location. This works perfectly well when people use a single computer, but it creates havoc when they use multiple computers.

The merge algorithm in Windows is more advanced; it merges user profiles at the file level. In other words, it's a real merge, not a wipe-and-load. The merged profile then becomes a superset of the files in the local and server copies of the user profile, and when a file exists in both copies, the operating system uses the most recent version of the file. New files don't turn up missing, and updated files are not replaced—both of which are symptoms that occur with the merge algorithm in Windows NT 4.0. In the case of the Windows NT 4.0 merge, if a profile changes on two computers, only the last profile copied to the network persists.

Behind the new and improved merge algorithm is the time stamp that Windows saves in the `ProfileList` key. When a user logs on to the computer, the operating system saves the current time in `ProfileList`. When the user logs off the computer, the operating system uses the time stamp to determine which files have been added or removed from the server's copy of the user profile. For example, if a file named `Example.doc` is in the server copy of the user profile but not in the local copy, the time stamp helps Windows determine whether the file was added to the server copy or removed from the local copy. If the time stamp of the file is later than the time stamp of the local user profile, the file was added to the server copy. The result is that Windows doesn't touch the file when it merges the local profile into the server copy. If the time stamp of the file is earlier than the time stamp of the local user profile, the file was removed from the local user profile. The result is that Windows removes the file from the server copy of the profile when the operating system merges the local copy into it. With Windows, if a profile changes on two computers, both of them are merged file by file into the server copy.



Note There is another issue that keeps many IT professionals from using roaming user profiles. Roaming user profiles are terrific when configurations are similar from desktop to desktop. When users log on to different computers with different sets of applications, screen sizes, power management requirements, and so on, roaming user profiles are cumbersome and users' experiences aren't very good. Roaming user profiles are great in scenarios such as call centers and other environments in which configurations are standardized, but they are not very useful when configurations are not standardized in an organization.

Deploying Default User Profiles

Deploying default user profiles is one of the easiest ways to deploy settings to new users. You can't use default user profiles to deploy settings to existing users, however, because they already have user profiles. These aren't settings that you want to manage. They're defaults that you want to establish for users while allowing users to change them when necessary. Essentially, deploying default user profiles is like modifying the default settings in Windows. If you want to define a setting that users *can't* change, use policies. Chapter 7, "Using Registry-Based Policy," contains more information about managing settings.

To deploy a default user profile, follow these steps:

1. Create a template account.

You can use a local or a domain account, but the user profile is generally cleaner if you use a local account on a computer that's not joined to a domain. (Because I include network shortcuts in my profiles, I usually use a domain account to create default user profiles.) Also, for the template account, choose a name that you're sure is unique in the registry and is shorter than eight characters. You'll learn why using a unique name is important a bit later in this chapter.

2. Log on to the computer using the template account, and customize its settings. The section "Customizing User Settings," later in this chapter, describes settings that I usually customize.
3. Clean up the user profile to remove artifacts that you don't want to deploy. The section "Cleaning User Profiles," later in this chapter, describes how to clean the profile.
4. Copy the template account's user profile folder to a new location, and name it Default User.

Don't replace %SystemDrive%\Documents and Settings\Default User, however, because you might need to repeat the process a few times to get it right and you'll want the original default user profile handy. In the section "Creating Default User Folders," later in this chapter, I describe an alternative method for building the Default User folder that I think is more precise because it yields a cleaner default user profile.

5. Deploy the default user profile.

You can put the Default User folder in %SystemDrive%\Documents and Settings on disk images and then deploy them, or you can put the Default User folder on the NETLOGON share of the server. I prefer the second method because it separates settings from the disk images, which allows me to update settings much more easily.

Alternatives to Default User Profiles

An alternative to customizing a bunch of settings in default user profiles is scripting. Create a script that configures Windows user settings per your company's requirements. This assumes that you have a specification, or at the very least, a list of settings that you want to customize for users. Then edit the NTUSER.DAT hive file in the disk image's Default User folder, adding the command that executes the script to the key `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce`. The NTUSER.DAT hive file in the Default User folder doesn't contain the `RunOnce` key by default, so you must add it. Then add a `REG_SZ` value to this key—the name is arbitrary—and put the command line that you want to execute in it. Each time Windows creates a new user profile, it executes the script to customize the user's settings.

Also, you can add a script that customizes the current user profile to `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`. Windows runs this script every time a user logs on to the computer. If you want to configure settings only the first time the user logs on to the computer, add code to the script that checks for a value in `HKCU` and runs only if that value doesn't exist. Then end the script with code that creates the missing value so that the script doesn't run the next time the user logs on to the computer. Chapter 11, "Scripting Registry Changes," shows you how to write scripts using Windows Script Host, and these are ideal for this scenario.

Customizing User Settings

Log on to the template account that you created in step 1 of the previous section and customize the account's settings. When customizing settings for a default user profile, less is more. Preferably, you'll work from a list of settings that you've examined with other members of the deployment planning team. The following list gives you an idea of the settings that I frequently target with default user profiles:

- Quick Launch toolbar
- Start menu
- Windows Explorer
- Internet Explorer
- My Network Places
- Search Assistant

- Tweak UI
- Control Panel, in particular:
 - Display
 - Folder Options
 - Mouse
 - Power Options
 - Printers and Faxes
 - Sounds and Audio Devices
 - Taskbar and Start Menu

You want to customize per-user settings because those are the only settings that are in the user profile. How do you know that a setting is per-user when you're customizing a user profile? You don't necessarily. That's why you must test the settings in your list ahead of time. Sitting down to construct a default user profile isn't the time to begin wondering whether a particular setting is per-user or per-computer. The easiest way to find out is to log on to a new account and customize the settings in your list. Then copy that user profile to a clean installation of Windows, and see which settings made it. The settings that didn't make it are per-computer settings, and you'll want to scratch them off your list. There are a small number of settings that are per-user but still don't work well in default user profiles, and there's generally little you can do about it except edit the profile to make them work. The most prominent example is desktop wallpaper. Including wallpaper in a default user profile requires you to include the wallpaper graphic file inside the profile folder and then edit the profile hive to point to the new location.

You might also want to include settings for applications that you're deploying, whether you include them on your disk images or deploy them using other methods.



Note Before you begin, here's a caveat: don't include settings for Windows Installer-based applications in a default user profile. Windows Installer provides superior methods for deploying settings. That means you shouldn't deploy settings for Office 2003 Editions using default user profiles. Instead, use tools such as Custom Installation Wizard and Office Profile Wizard. Both tools come with the Office 2003 Editions Resource Kit, and Chapter 17, "Deploying Office 2003 Settings," describes how to use them. Install other types of applications and customize their settings to your requirements just as you would customize Windows settings.

This last step is optional but I recommend it: remove artifacts from the user profile that you don't want to deploy. Artifacts include history lists and similar items. I have a preset route that I use to clean up a user profile. First I clear the Start menu and Internet Explorer's history lists. To do this:

- In Control Panel, launch Taskbar And Start Menu. On the Start Menu tab, click Customize. On the Customize Start Menu dialog box's Advanced tab, click the Clear List button.
- In Control Panel, launch Internet Options. In the Internet Options dialog box, click Clear History to remove Internet Explorer's history lists.

You don't need to worry about removing temporary Internet files because these are in the profile's Local Settings folder, and Windows doesn't copy them with the profile. If you opened Internet Explorer to customize it, however, you might clear out the cookies and AutoComplete lists. In the Internet Options dialog box, on the General tab, click Delete Cookies, and then on the Content tab, click AutoComplete, followed by Clear Forms and Clear Passwords.

After you're finished customizing and cleaning the account's settings, log off Windows. My last word of advice is to be cautious; don't open dialog boxes and programs that you don't intend to customize. Doing so keeps their settings out of the default user profile. For example, if you don't intend to customize Microsoft Windows Media Player, don't open the program.

Cleaning User Profiles

You cleaned the user profile a little bit in the previous section, but only to remove some artifacts from the profile hive. The next major step is to open the profile hive in Regedit and scour it for settings that you don't want to deploy or that you must change before deploying.

The most significant example is paths. User profiles contain references to the profile folder: %SystemDrive%\Documents and Settings*Name*. If you deploy the user profile to countless users, they'll all have different profile folders. When they try accessing the profile folder *Name*, Windows and programs will fail because the user doesn't have access to that folder. A more concrete example will make this clear. Assume you created a user profile using a template account named DefUser and deployed that profile to a user named Jerry. The user Jerry has access to %SystemDrive%\Documents and Settings\Jerry, but the folder %SystemDrive%\Documents and Settings\DefUser doesn't even exist. When the user Jerry runs a program that uses a setting containing the path to the DefUser user profile folder, the program causes an error. To correct this situation, follow these steps:

1. Log on to the computer containing the template user profile as Administrator.

2. In Regedit, load the NTUSER.DAT hive file from the template user profile folder. (See Chapter 2, “Using Registry Editor,” to learn about using hive files.)
3. Search the hive file for references to the template user profile folder. If the name of the folder is longer than eight characters, search for the long and short versions of the folder’s name.
4. Remove values that contain the path of the template user profile folder.
5. Unload the hive file, and restart the computer.

Restarting the computer is often necessary because Windows locks the file and you can’t copy it. Restarting the computer is the quickest way to force it to let go of the file.

When you remove values that contain the path of the template user profile folder in step 4, you’re assuming that Windows and other programs re-create missing settings. This isn’t always true. Some of my favorite applications fail to re-create missing settings. You’ll learn which do and which don’t through trial and error. You can handle the problem easily, though. Rather than removing the value permanently, replace a `REG_SZ` value with a `REG_EXPAND_SZ` value of the same name. Then set the value to the original path, substituting `%USERPROFILE%` for the portion that is the user profile folder. For example, if you see a `REG_SZ` value named `Templates` that contains `C:\Documents and Settings\Jerry\Templates`, remove the value; then add the value `Templates` back as a `REG_EXPAND_SZ` value, and set it to `%USERPROFILE%\Templates`. Test these changes in your lab to make sure they work properly.

In the previous section, you cleared some of the history lists using the Windows user interface. Take this opportunity to further neaten your work by removing the keys listed in Table 12-4. These correspond to most of the history lists that Windows keeps, including the Search Assistant and common dialog boxes.

Table 12-4 History Lists to Remove

History List	Key
Internet Explorer’s address bar	HKCU\Software\Microsoft\Internet Explorer\TypedURLs
Run dialog box	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Documents menu	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Common dialog boxes	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Search Assistant	HKCU\Software\Microsoft\Search Assistant\ACMRU

Creating Default User Folders

The template user profile is ready to go. All you have to do now is copy it. To open the User Profiles dialog box, in Control Panel, launch System. On the Advanced tab, click Settings in the User Profiles frame. In the User Profiles dialog box, click the template user profile and then click Copy To. In the Copy Profile To text box, shown in Figure 12-6, type the path to which you want to copy the profile. To keep things simple, I usually copy the profile folder to C:\Default User. Just make sure that the folder doesn't already exist. Also, give the Everyone group permission to use the profile, which is appropriate for a default user profile: click Change, type **Everyone**, and then click OK. The default user profile is ready to deploy, which you learn how to do in the next section.

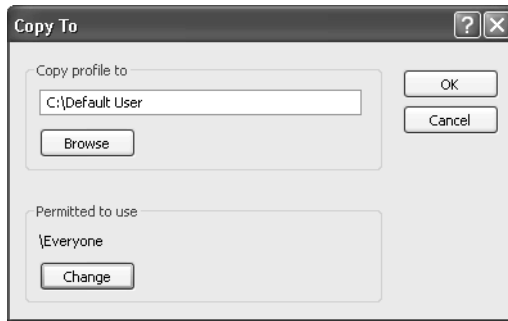


Figure 12-6 Copy the template user profile using this dialog box; don't copy the folder using Windows Explorer because doing so copies artifacts that you don't want in the profile.

The method that I just described is common for creating a default user profile from a template user profile. I don't like it because user profiles expand greatly in size and complexity after Windows loads and uses them. A default user profile created using the method that I just described contains more files and folders than necessary. To use the more precise method that I prefer, follow these steps:

1. Copy %SystemDrive%\Documents and Settings\Default User to another location, such as C:\Default User. You want to keep the original Default User folder, just in case you have to start over again.
2. Copy the NTUSER.DAT hive file from the template user profile to your copy of the Default User folder, C:\Default User.
3. Copy other files from the template user profile folder to your copy of the Default User folder, C:\Default User. I tend to copy files from the following folders, assuming they contain files that I want to deploy:
 - ❑ \Application Data\Microsoft\Internet Explorer\Quick Launch
 - ❑ \Desktop
 - ❑ \Favorites

- ❑ \NetHood
- ❑ \PrintHood
- ❑ \SendTo
- ❑ \Templates

Deploying Default User Folders

After completing the steps in the preceding section, you have a default user profile that's ready for deployment. You have two choices. If you're deploying Windows using disk-imaging techniques, you can include the default user profile on the disk image. Replace %SystemDrive%\Documents and Settings\Default User with your own Default User folder. After replacing the Default User folder with your own, clone and deploy the disk image. When new users log on to the computer, they'll receive your default user profile and thus your settings.

I don't like customizing the local Default User folder as my sole means of deploying default settings, however. I prefer to separate settings from configurations. What if I need to update a setting down the line? I don't want to update the Default User folder on each computer in the organization.

The alternative is to copy the customized Default User folder to the NETLOGON share of the server. As you learned earlier in the chapter, Windows looks first for the network version of the Default User folder and then the local version. The first time users log on to a computer, Windows gets my default user profile from the network. Of course, the benefit is that I can always update it later. The primary problem with this method is that if users log on to their computers locally, they still get the local default user profile. That's the reason that I prefer doing both at the same time. I replace the Default User folder on disk images and also copy the same folder to the NETLOGON share of the server.



Note An alternative to copying a default user profile to the NETLOGON share is keeping a user profile handy on the network and then copying it to users' network profile folders when you create new accounts. For example, stash away a default user profile somewhere on your server. Assuming that you're using roaming user profiles, copy the default user profile into new accounts' profile folders. The first time those users log on to Windows, the operating system downloads their roaming user profile, which you've already preconfigured. This is useful in one-off scenarios when you want users to have a profile other than the default. It's also useful in a heterogeneous environment, which often requires different user profiles for different versions of Windows.

Coexisting with Earlier Versions of Windows

Coexistence is an issue that affects roaming user profiles only. If you're not using roaming user profiles on your network, coexistence isn't an issue because you won't be deploying user profiles to different versions of Windows. In general, though, roaming user profiles are compatible between Windows 2000, Windows XP, and Windows Server 2003. Here are a few precautions that you can take to minimize problems:

- Try to ensure that users with roaming user profiles are logging on to the same version of Windows on each computer. That means you should choose your rollout units so that you're picking up all the computers that users can access.
- At the very least, make sure the same application versions are on each computer and that you've installed applications to the same path on each computer.
- If you're using roaming user profiles with Windows 2000, Windows XP, and Windows Server 2003, make sure that your %SystemDrive% and %SystemRoot% are the same. Also, make sure that profiles are stored in the same path. If you're using roaming user profiles with Windows NT 4.0 and Windows XP, you should move the location of user profiles that Windows XP uses by setting the `ProfilesDir` property in the `[GuiUnattended]` section of your answer file.

There's nothing in the documentation that says user profiles don't roam between Windows NT and Windows XP. However, I suspect that this scenario isn't workable. First, Windows XP converts Windows NT-based profiles. Second, having knowledge of both versions of the registry, I suspect that subtle differences between the two are likely to cause configuration problems in the long run. If anybody suggests that you can use roaming user profiles with any combination other than Windows 2000, Windows XP, and Windows Server 2003, ask for more information and test these scenarios carefully in a lab.

Migrating User Settings to Windows

Default user profiles give settings to new users, but what do you do about users who already have user profiles? You can let Windows migrate the user profile. Throw disk imaging into the mix, and you have a whole different bag of problems. One of the drawbacks of using disk imaging to deploy the operating system is that users lose their documents and settings. This doesn't have to be a barrier to deployment, though. A variety of third-party utilities are available to migrate users' settings. Also, Microsoft provides two tools, one for the user and one for the IT professional:

- **Files And Settings Transfer Wizard.** This tool is designed for the user. This wizard is also useful in enterprise environments when employees want to migrate their own documents and settings without the IT department's help.

- **User State Migration Tool (USMT).** This tool is designed for IT professionals performing large-scale deployments of Windows in an enterprise. USMT provides the same functionality as the File And Settings Transfer Wizard, but on a larger scale. USMT gives IT professionals precise control over the documents and settings that it migrates.

All these tools work roughly the same way. First you copy users' documents and settings off their computers and store them on the network. You install a new disk image to their computers, and then you reapply their settings. Users get to keep their documents and settings.

Files And Settings Transfer Wizard

Files And Settings Transfer Wizard is a fast and easy way for you to copy all your documents and settings from your previous configuration to Windows XP or Windows Server 2003. To start it, click Start, All Programs, Accessories, System Tools, Files And Settings Transfer Wizard. It migrates settings in four major groups:

- **Action.** This group includes settings such as the key repeat rate, whether double-clicking a folder opens it in a new window or the same window, and whether you need to double-click or single-click an object to open it.
- **Internet.** This group includes settings that enable you to connect to the Internet and control how Internet Explorer works. They include settings such as your home page URL, favorites, Internet shortcuts, cookies, security settings, dial-up connections, and so on.
- **Mail.** This group includes settings for connecting to your mail server, your signature file, views, mail rules, local mail, and contacts. The wizard supports only Microsoft Outlook and Outlook Express.
- **Application.** This group includes application settings such as Microsoft Office. The wizard migrates only application settings, not the applications. You must reinstall each after upgrading to Windows XP or Windows Server 2003.

Files And Settings Transfer Wizard also migrates your documents. It does so by type (*.doc), folder (C:\Documents and Settings\username\My Documents), or name (C:\Documents and Settings\username\My Documents\Jerry.doc). The wizard is pre-configured to copy the most common types of files and the most useful folders. It also gives you the option to change the folders, the file types, and the file lists.

User State Migration Tool

User State Migration Tool (USMT) is similar to the Files And Settings Transfer Wizard, but it also allows you to fully customize exactly what the tool migrates. USMT is designed for IT professionals only; individual users do not need to use USMT. The

tool is designed for large-scale migrations, and it requires a domain controller on which to store settings during migration.

USMT consists of two programs, ScanState.exe and LoadState.exe, and four migration rule information files: Migapp.inf, Migsys.inf, Miguser.inf, and Sysfiles.inf. ScanState.exe collects users' documents and settings based on the information contained in Migapp.inf, Migsys.inf, Miguser.inf, and Sysfiles.inf. LoadState.exe deposits this user state data on a computer running a clean installation of Windows. Both of these tools are on the Windows CD in the \Valueadd\Msft\Usmt folder. The shared set of INF files drive USMT. IT professionals can modify these files to customize the documents and settings that the tool migrates. In fact, during any real deployment project, you'll most likely have to modify the INF files to handle your unique requirements.



More Info The white paper "Step-by-Step Guide to Migrating Files and Settings" is a good guide for learning how to use USMT. This white paper is available on the Web at <http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/mgrtfset.mspx>.