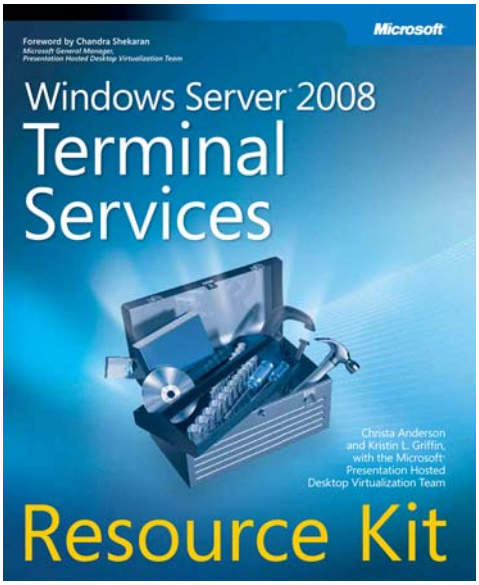


Windows Server® 2008 Terminal Services Resource Kit

Christa Anderson and Kristin L Griffin with the Microsoft Presentation Hosted Desktop Virtualization Team

To learn more about this book, visit Microsoft Learning at http://www.microsoft.com/MSPress/books/12716.aspx

9780735625853

Table of Contents

Chapter 4

Creating the User Work Environment

In this chapter:

After you have a terminal server installed, you can set up the user work environment so that users can be productive. This chapter and the next several chapters describe how to do this. In particular, this chapter discusses configuring profiles and folder redirection to work with Terminal Services.

The basic elements of a user workspace are the configuration settings in the user's profile and the default locations to save data. After reading this chapter, you will understand the following:

- How roaming, local, and mandatory profiles work
- Best practices for storing and managing profiles
- How to use folder redirection to unify user default locations between local and remote applications
- The benefits and drawbacks of using mandatory profiles to maintain a consistent look and feel
- How to secure the desktop to prevent users from saving files to it and why this is important
- How to support profiles when the client operating system is Windows XP

How Profiles Work

Apart from being the thing you see when you look at someone who's facing 90 degrees away from you, a *profile* is a collection of settings and documents that define a user's work environment. While a user is logged in, the collection of settings is stored in HKEY_CURRENT_USER (HKCU) in the registry of the computer that user is logged on to; the documents are stored in the subfolders within the profile folder. How do these settings get into the registry and those files into the profile folder? Therein lies a tale—and that tale is good background for understanding some of the complications that arise in a terminal server environment.

Note There are three types of profiles: local, roaming, and mandatory. Local profiles are stored on and used from a single computer. Roaming profiles are stored on and used from a network share, so they're available to any computer that can access that particular network share. Mandatory profiles are usually centrally located like roaming profiles, but whereas local profiles and roaming profiles are read-write, mandatory profiles are read-only.

User Profile and the Registry

The registry is organized into sections called *keys* that align with a particular configuration option. For example, computer-wide settings are stored in HKEY_LOCAL_MACHINE (HKLM), whereas user-specific settings are stored in HKEY_CURRENT_USER (HKCU). Windows Server 2008 maintains user-specific settings in HKCU while that user is logged on to the computer. You can see how HKCU works and reflects changes to the user environment by following the process outlined in the following sidebar, "See How the Registry Reflects Changes."

See How the Registry Reflects Changes

One easy way to watch how HKCU changes as you customize your environment is to make a change and watch the contents of the registry.

1. Run Regedit.exe and confirm that you want to run it when prompted.
2. Navigate to HKCU\Control Panel\Colors\Window. If you're using the default Windows Vista color scheme, the value of this entry should be 255 255 255. (Full saturation of red, blue, and green values show up as white on a monitor. Values of 0 for all three show up as black. If you ever had color theory classes, this is a demonstration of how black is the absence of color.)
3. Right-click the Desktop and choose Personalize from the context menu to open the Personalization window.
4. Click Window Color And Appearance. In the Appearance Settings dialog box, click Advanced to open the aptly named Advanced Appearance dialog box. From here, select Window from the Item drop-down list. Change Color 1 to light gray and click OK.

5. Click OK in the Appearance Settings dialog box. The screen will adjust for a minute and then the background color of windows will turn light gray.
6. If you examine the value of HKCU\Control Panel\Colors\Window, you'll see that it's now 192 192 192.

On Windows Server 2008 and Windows Vista, HKCU contains the subkeys explained in Table 4-1. (Even if you're logging on to a Windows Server 2008 terminal server from an older operating system such as Windows XP, the profile in the terminal session corresponds to the server platform, so these are still the registry keys that apply.) There may be more subkeys in this section—it depends on which applications you have installed.

TABLE 4-1 Subkeys of HKCU in Windows Vista and Windows Server 2008

Subkey	Description	Maps To
AppEvents	Sounds played on system events.	Control Panel\Sounds
Console	Command window settings such as window size, colors, and buffer size.	Command Prompt\Properties
Control Panel	User desktop appearance settings, mouse and keyboard settings, power policy, and accessibility.	Control Panel
Environment	Environment variable definitions.	Control Panel\System\Advanced
EUDC	Customized characters that end users install for viewing and printing documents when standard fonts don't support them. Applies to East Asian font sets.	Control Panel\Fonts
Keyboard Layout	Edits the keyboard layout. Useful if your operating system is displaying in one language but you want to use the keyboard layout of another one (for example, displaying in English but arranging the keyboard as though you were in Germany).	Control Panel\Regional and Language Options
Network	Network drive mappings and settings.	Control Panel\Networks
Printers	Printer connection settings.	Control Panel\Printers
Session Information	Information about the current session, such as how many applications are open.	Not stored—populated during the session
Software	Personal settings for all software installed for that user.	Individual applications
System	Contains the current control set for that user (drivers and services to run at startup).	Not stored—populated on startup

This information is in HKCU while the user it is associated with is logged on, but it can't stay there permanently; unlike HKLM, the current user settings are not persistent across logons. Most pieces of the registry are saved in files called *hives* and are loaded as necessary. When a hive file is opened, it's reloaded back into the registry. Therefore, HKCU is stored as a hive in a file called NTUSER.DAT. Each user logged on to the terminal server gets his own version of HKCU.

When you log on to a computer, the User Profile Service loads the hive file from the location specified in your user account properties and populates HKCU for that session. When you log off the computer, the hive file is written back to its storage location as NTUSER.DAT. If you happen to be logged on to more than one computer at a time, two copies of your profile will be open, populating the contents of HKCU on each computer.

Note Profiles may be cached on the terminal server to speed up logons if you set the corresponding Group Policy. However, even if you enable caching, when a user logs off the terminal server, the corresponding branch of HKCU is cleared out. We'll talk more about caching user profiles in the section titled "Caching Roaming Profiles," which appears later in this chapter.

In addition to loading HKCU with the contents of your profile, logging on to a terminal server updates two parts of HKLM, the computer-wide registry. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Profile List (Figure 4-1) contains a list of all currently logged on users and the profiles they're using. The users are identified by Security Identifiers (SIDs), but you can distinguish them by browsing the keys—they show the path to both the local cache (the ProfileImagePath key value shown in Figure 4-1) and to the roaming profile folder share (the CentralProfile key value shown in Figure 4-1), so it's not hard to map user names to profiles.

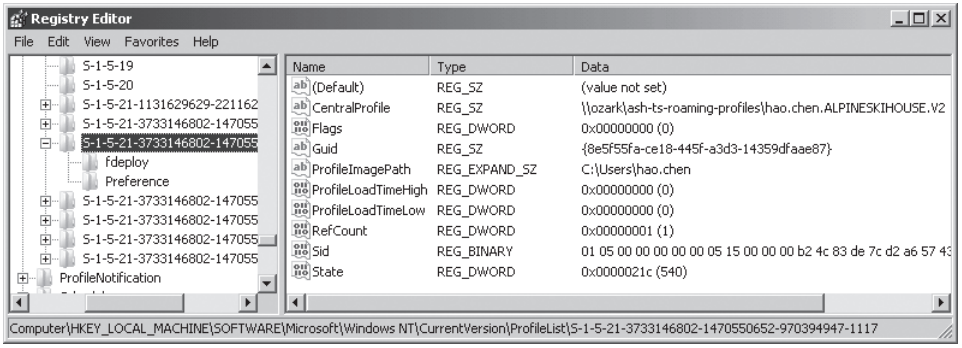


FIGURE 4-1 Loading a profile into a terminal session updates the Profile List key for the entire terminal server.

Another key in HKLM, shown in Figure 4-2, contains information about the Group Policy settings for that user. This registry key records the source of the Group Policy object (GPO) applied to this user, including its name and where it's stored.

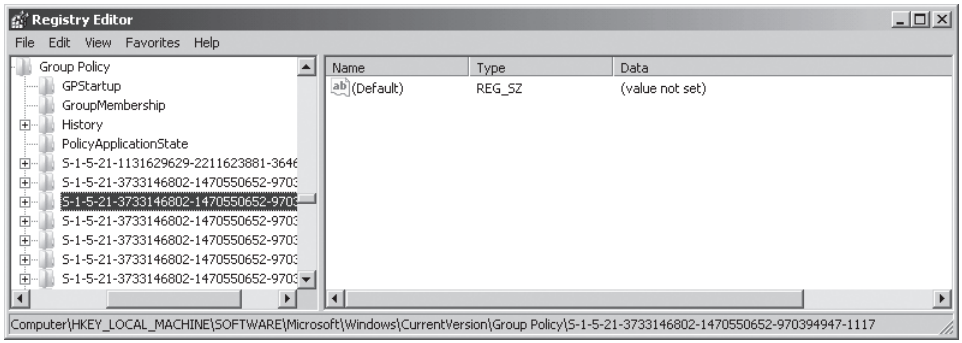


FIGURE 4-2 Logging on to a terminal session updates the Group Policy key for the terminal server.

When you log off from a terminal server, the two keys with your SID are locked. They don't actually go away, but if you attempt to open the key associated with a user who's currently logged off, you'll get an error message telling you that the system cannot find the file specified. Log on again, and the key with the same SID will be repopulated.

Although loading a profile adds two keys to the registry that never go away, most of the time it doesn't matter. As we'll discuss in the section titled "The Consequences of Deleting a Profile Folder from Explorer" later in this chapter, it *does* matter should you choose to delete a profile. Deleting the file doesn't delete the registry keys associated with it. Therefore, always use the correct tools to delete profiles.

How Profile Changes Are (Not) Merged

The operating system loads the contents of NTUSER.DAT into HKCU at logon and saves back to NTUSER.DAT at logoff, in the same way that you might open a Microsoft Office Word document when you log on, type in it for a while, and then save the document when you log off. This has some important implications for a terminal server environment.

As an example, imagine this scenario: You are logged on to two different computers and you open a new Microsoft Word document in each session. In Session 1, you type "Every Good Boy Does Fine." In Session 2, you type "All Cows Eat Grass." You save the file in Session 1 as Myfile.docx. Next you save the file in Session 2 as Myfile.docx in the same location, confirming that you want to overwrite the old file when prompted.

The next time you open Myfile.docx, the file will say only "All Cows Eat Grass." The phrase "Every Good Boy Does Fine" has been overwritten. In short, the files are not merged; they're written back to the save location, and the version last written to that location is the only one you'll see.

So it is with profiles, which are just another type of file. If you log on to two sessions, each of which is using the same roaming profile, you will have two copies of your profile open. If you make changes to the open profile, you'll see them at the time, but they won't be saved into NTUSER.DAT until you log off. (Unlike the Word .docx file, the file system won't ask if you want to overwrite the profile file.) As in the previous example, if you have a profile open in Session 1 and in Session 2, log off Session 1 and then log off Session 2, only the changes made to the Session 2 copy of the profile will appear when you log on again and reload that profile.

Note One implication of the way profiles work is that you shouldn't use the same profile for local sessions as you do for terminal sessions. If you do, then by definition every time you log on to your computer and then log on to a terminal server you will be opening two copies of your profile. You will almost certainly lose data this way.

You may be wondering whether opening two applications from a single terminal server opens one or two copies of your profile. In Windows Server 2003, you could create a Remote Desktop Protocol (RDP) session that would open a single application instead of displaying the entire desktop. (As noted in Chapter 1, "Introducing Terminal Services in Windows Server 2008," not many people did this because it wasn't terribly user friendly, but it was possible.) If you presented individual applications this way, then each time a user opened an application on the same server, she would open a separate session and therefore a separate copy of his profile. Windows Server 2008 improves on this design in two ways. First, it introduces RemoteApps. All RemoteApps launched from the same server run in the same session, so they only open a single copy of your profile. Second, when deciding where to route incoming connections to a terminal server farm, the TS Session Broker will check to see if a user already has an open session on a terminal server in the farm. If it does, then the user will be routed to that server to launch the application. End result: You have preference to the server where you already have an open connection, *and*, so long as you're only connecting to a single server, only one copy of the profile will be open.

Profile Contents External to the Registry

Not all parts of a profile are stored in HKCU. Folders for user data are stored in the profile folder, but separately from NTUSER.DAT. In Windows Vista and Windows Server 2008, the profile includes the folders listed in Table 4-2. (More folders may be available depending on which applications you have installed.)

TABLE 4-2 Folders Associated with a Windows Vista/Windows Server 2008 Profile

Folder	Description	Stored Separately in Windows XP
AppData	Default root location for user application data and binaries	No
Contacts	Used to store contact information and is also the address book for Windows Mail, the successor to Outlook Express	No
Desktop	All items stored on the desktop, including files and shortcuts	Yes
Documents	Default root location for all user-created files	Yes
Downloads	Default location for all files downloaded using Internet Explorer	No
Favorites	Bookmarked pages in Internet Explorer	Yes
Music	Default root location for all music files	Yes
Pictures	Default root location for all image files	Yes
Saved Games	Default location for saved games	No
Searches	Default location for saved searches	No
Videos	Default root location for all video files	Yes

As shown in Table 4-2, Windows Vista and Windows Server 2008 are a lot more granular about folder arrangements than Windows XP/Windows Server 2003 were. Rather than nesting folders, the operating system now organizes them at a top level. Unfortunately, this means that you can't use the same profiles for Windows Server 2008 terminal servers that you did for Windows Server 2003—the structure of the profiles doesn't match. We'll talk a bit later in this chapter about how to allow Windows Server 2003 and Windows Server 2008 profiles to coexist. (See the section titled "Sharing Folders Between Windows Server 2003 and Windows Server 2008 Roaming Profiles.")

Note Windows Vista folder arrangements generally are more granular than those of Windows XP, but in other places, Windows XP top-level folders such as Nethood, Printhood, and a few others have been moved inside the AppData folder in Windows Vista.

Although these document folders are stored by default in the user's profile folder (see Figure 4-3, which has hidden files visible), they don't have to be. In fact, it's best if they aren't.

First, keeping user data within the profile folder increases the profile size. Assuming that you're storing profiles on a central share instead of on individual terminal servers (and, for reasons we'll discuss shortly, this is a good assumption), this can slow logons. A large profile increases the time it takes for users to log on and log off (since the data in the profile must be cached on the terminal server). A large profile can also impact the ability of additional users to log on to a terminal server. If profile caching is enabled, when the hard disk where the cache is stored fills up, no one else will be able to log on.

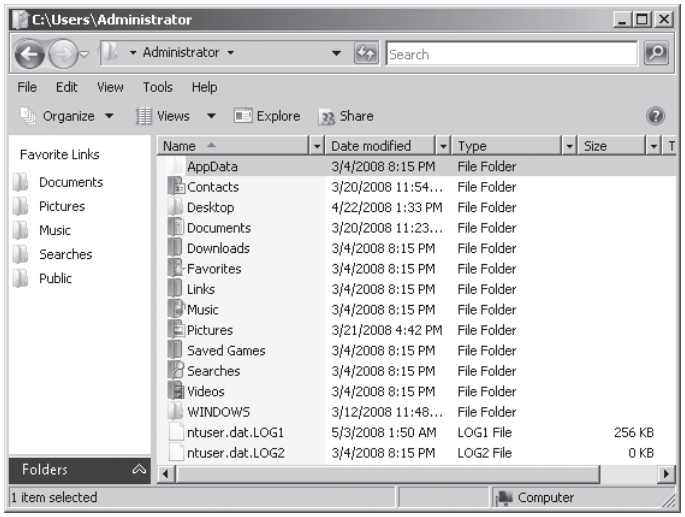


FIGURE 4-3 By default, a profile contains user data as well as user settings.

Second, if you're using mandatory profiles (more about these in the section titled "Choose Between Roaming and Mandatory Profiles" later in this chapter), and you don't redirect folders outside the profile folder, users will not be able to save files to the standard personal folders such as Documents. The files will look like they're saving, but they won't be saved. This will cause pain and agony and many unsolvable Help Desk calls.

Note In previous versions of Windows, the Recycle Bin was stored on a per-computer basis. In Windows Vista and Windows Server 2008, the Recycle Bin is a hidden file in the root of the profile folder. You can't redirect it, and even if you're using mandatory profiles, you will still be able to recycle files.

For these reasons, it's good practice to use folder redirection with Terminal Services. We'll talk more about this in the next section.

Design Guidelines for User Profiles

Each of the following has an impact on the way you save user-specific configuration settings and data for use with terminal servers:

- Local profiles aren't generally suited to deployments of more than one terminal server, because the user experience will become different on every terminal server.
- For centrally stored profiles, the larger the profile, the longer it can take to log on or log off. The User Profile Service must copy the files to the terminal server and then copy them back to the profile when they're no longer needed.

- Profile settings aren't stored granularly; they're stored as a flat file. If more than one copy of the profile is open, the settings in the copy that were saved and closed last will be the ones reflected in NTUSER.DAT.

The following sections explain how these facts will impact your design.

Choose Between Roaming and Mandatory Profiles

Local profiles aren't a good fit for terminal services deployments larger than a single server. Storing local profiles on terminal servers in a multi-server environment will:

- Lead to an inconsistent user experience and may create problems that are hard to troubleshoot because they're linked to logging onto a specific terminal server.
- Fill up a terminal server hard disk with duplicate copies of a profile (that is, the profile will be stored on each terminal server a user logs onto).
- Require that you back up the terminal server because it now holds user data.

You have two remaining choices: roaming profiles and mandatory profiles. Neither choice is always appropriate. The option you pick depends on the amount of control you want and have authority to implement.

Roaming profiles may be freely edited by their owners within the limits defined by Group Policy (discussed in Chapter 5, "Fine-Tuning the User Experience"). That is, if you've defined the wallpaper for a user group via Group Policy, that will be the wallpaper every time anyone in that user group logs on. If you haven't specified the wallpaper using Group Policy, anyone is welcome to change the wallpaper when he connects to the terminal server. (The choices of wallpaper on the terminal server are admittedly not great, consisting as they do of either a logo backdrop or flat colors, but if users mapped drives to their terminal session, they could add wallpaper from any pictures stored on their computer.)

Mandatory profiles differ from roaming profiles in that their owners can edit them, but any changes they make will not be saved to the profile. This can speed up logoff times, since nothing is written back to the network share where you've stored the mandatory profiles. More insidiously, mandatory profiles don't save any data to folders stored within the profile folder. You *must* use folder redirection if using mandatory profiles for users to be able to save data to their personal folders. In fact, that's worth highlighting in a cautionary note.

Caution If you use mandatory profiles, you must configure folder redirection in order to allow users to save files to their personal folders that are part of their profile.

The core choice between mandatory and roaming profiles is the tradeoff of flexibility versus control. Mandatory profiles make life easier for the terminal server administrator and eliminate the chance of a user erroneously making a profile configuration change that leads to

Help Desk calls (such as accidentally hiding the taskbar). Mandatory profiles also speed logoff times, but they don't allow users the degree of personalization that most have come to expect from Windows. More important, mandatory profiles don't allow other applications to save data to your profile either. This means that some security applications that require giving users a private key (the Encrypted File System is one) don't work with mandatory profiles. Your choice here will depend on your corporate culture, need to use applications that require private keys, and IT's ability to control the desktop.

Note One option to the choice between roaming profiles and mandatory profiles is to not choose. Use mandatory profiles and combine them with a mechanism that allows users to save selected settings and have them applied at logon. Windows Server 2008 does not include this functionality, but several Terminal Services ISVs or consulting partners do. You can find an example of this functionality—a tool named Flex Profiles—from the following link on the companion CD: *http://www.immidio.com/flexprofiles*.

Use Folder Redirection

Whether you're using roaming profiles or mandatory profiles, it's best practice to use folder redirection.

If you're using roaming profiles, you want to make sure that the profile isn't getting too big, because a large profile will slow both logon and logoff times. People don't want to wait to log on to their computers. The fastest approach is to use local profiles, but for reasons we already discussed, you don't want to combine local profiles with terminal servers.

If you're using mandatory profiles, then you want to use folder redirection—but selectively. Any folders that you keep in the profile folder will become read-only. For some folders, this is very bad news—people won't be able to save their documents or pictures in their personal folders—so you'll definitely want to redirect those folders. But for some folders, this is exactly what you want. If you don't want people to remove icons from the Start menu, leave its folder in the profile folder.

Prevent Users from Losing Files

The Desktop folder contains everything you can see on the desktop—files and shortcut icons. Many users like saving documents to the Desktop. This is acceptable if you're seeing the full desktop, but if you're using RemoteApps, this isn't a great idea, because people don't see their desktop in the terminal server session and therefore can't easily browse it. (They could still open the documents if they moved to that path when opening a file, but they'd have to know to do this.) If you keep the Desktop folder in the profile folder and use

mandatory profiles, then people can't save files to the Desktop . . . but if they try, it will appear as though they were able to do so. The file will be on the Desktop as long as they are logged on. Log off and log back on again, however, and the file will be gone.

You can use mandatory profiles to maintain a consistent look and feel for your users, prevent them from saving files to the Desktop, and give them an error message if they try. To do this, you'll need to:

- Redirect the Desktop folder to an external share.
- Set the permissions on this external share to read-only.

If you don't care if people save files to the Desktop (for example, if your users are connecting to a full desktop instead of to RemoteApps), then you can just redirect the Desktop folder.

Note For instructions on implementing folder redirection, see "Centralizing Personal Folders with Folder Redirection" later in this chapter.

Speed Up Logons by Reducing the Data to Copy

People are sensitive to the amount of time it takes to log on to a session. If it takes too long, you'll have problems with people leaving their sessions open rather than logging off. This is a security risk, has the potential to lock files that more than one person may need to edit, and keeps open processes on the terminal server.

To encourage people to log off, you must therefore make the logon process as painless as possible. We already discussed using folder redirection to keep a profile's size down. To speed things up, you can also use the Group Policy that applies to the way a computer loads profiles to configure the following settings:

- Cache roaming profiles.
- Define the amount of time a terminal server will try to get the user profile.
- Set an upper limit on the size of a user profile.

New to Windows Server 2008: Speeding Up Log*offs*

Speeding up logons is important, but when it's Friday afternoon and you want to get out of the office fast, logoffs are just as important. There are two ways in which Windows Server 2008 helps logoffs take less time.

You can limit the size of a profile using Group Policy (and help this limit by redirecting the folders out of the policy). This policy, Limit Profile Size, is set per user and is located in User Configuration | Policies | Administrative Templates | System | User Profiles.

Prior to Windows Server 2008, there was a nasty catch when it came to profile quotas in that previous versions of Windows were serious about enforcing this limit. If you made your roaming profile larger than Group Policy allowed, Windows would prevent you from logging off until you'd made the profile smaller. In Windows Vista and later versions, you can log off, but if the profile is larger than the size permitted by policy, the profile changes won't get written back to the roaming profile storage area.

Before Windows Server 2008, another issue that could delay logoffs (or prevent you from unloading your roaming profile altogether) was applications or drivers that left open handles to the registry (in other words, started to use it but never ended the connection to it). Microsoft had a separate tool called the User Profile Hive Cleanup Service (in an application called UPHClean) that checked for these open handles and closed them so users could log off. In Windows Server 2008, you no longer need to download this tool, because UPHClean functionality is handled by the User Profile Service.

Caching Roaming Profiles

To reduce the time it takes to log on to a terminal server, terminal servers cache the roaming profiles. Ordinarily, terminal servers attempt to retrieve the roaming profile from its central location. In cases when the network connection to the profile server is too slow or not working, however, being able to log on with a locally cached copy of your profile can at least speed things up. Caching stores a copy of the profile on the terminal server. This profile cache isn't used if the original roaming profile is available, but it can speed up logons in the case of slow or absent network connections.

Caching user profiles also means that you can use asynchronous processing of Group Policy, a policy processing model new to Windows Server 2008 that can speed up user logons. There are two ways that Group Policy can be applied. If you apply it synchronously (the default model for a server), logon doesn't complete until the Group Policy settings that apply to that user are applied. If you apply Group Policy asynchronously (the default model for a desktop), the user can log on while Group Policy is being applied. Asynchronous processing can lead to changes in the user environment after users have logged on but will speed up logon times if Group Policy processing is slowing things down.

All that being said, caching profiles does consume hard disk space on the terminal server. It can also prevent new users from logging on if the space allocated to cached profiles gets filled up. If you do cache profiles, make sure that you've got sufficient space for your user base and use the Group Policy and policy management tools described later in this chapter in the section titled "Removing Cached User Profiles on Terminal Servers" to delete profiles that aren't being used.

Caution Don't delete user profiles from the terminal server using Explorer or the delete command-line tools, because this does not clean up the registry entries associated with the profile and can affect the user's ability to log on again. The Delprof.exe tool does a complete job of cleaning up old user profile data. You can also configure the terminal servers using Group Policy to delete any profiles unused for a given period.

On the Companion Media To clean up old user profile data, download the Delprof.exe tool from the following location: *http://www.microsoft.com/downloadS/details.aspx?familyid=901A9B95-6063-4462-8150-360394E98E1E&displaylang=en*. This link is available on this book's companion CD.

Storing Profiles

By default, when you log on to a computer for the first time, you'll create a new profile in its local profile directory (%SystemRoot%*Users*). This profile directory will have your name as a logon alias; it will contain your folders and NTUSER.DAT (which is a hidden file, so you won't see it unless you've enabled viewing hidden files). If left alone, thereafter you'll store everything in that location. Documents will default to Documents, images will default to Pictures, and where music is stored by default is left as an exercise for the reader. All will be well . . . so long as that's the only computer you use.

If it's *not* the only computer you use, life gets somewhat more complicated.

Thus far, we've set up only a single terminal server. However, in Chapter 1, we alluded to it being best practice to have multiple terminal servers organized into a farm. (In Chapter 7, "Multi-Server Deployments and Securing Terminal Server Connections," we'll discuss how to do this.) When a user logs on to a terminal server farm, a special kind of terminal server called a Session Broker looks at the terminal servers in the farm, picks the one with the lowest number of active sessions, and sends the user there, as shown in Figure 4-4. Each time a user connects, the Session Broker decides anew which server the user should connect to based on the number of connections each server is actively supporting and whether or not the user already has a session open somewhere. The user connects to the server with the fewest active connections or the one where the user already has an open session. It is likely (and highly recommended) that users will log off when not using their terminal server session, so if you use local profiles for terminal server sessions, then over time a user will have local profiles on all the servers in the farm.

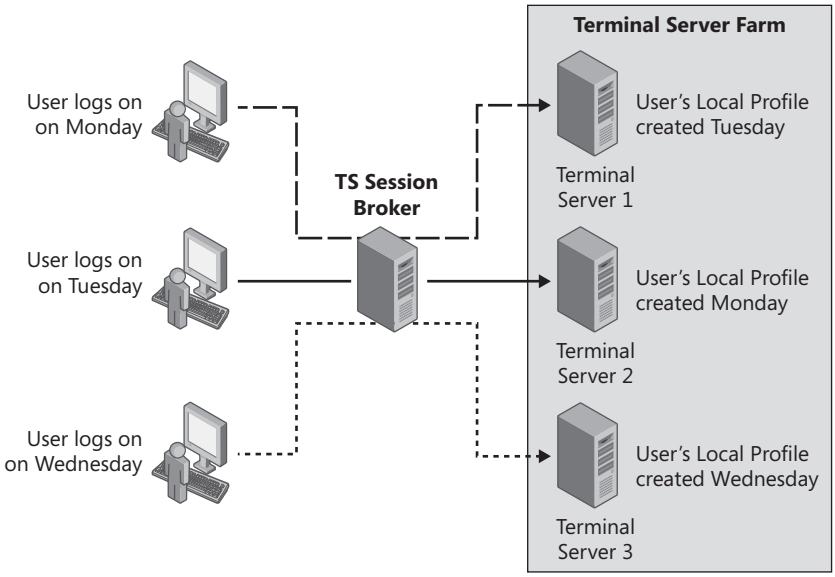


FIGURE 4-4 Over time, a user may have local profiles on every server in the farm.

This may not sound so bad. The user's logons will occur quickly, because the profile isn't loaded from the network but rather from the local computer. But when the user makes a change here and there, over time her desktop will look completely different depending on which terminal server she logs on to. (If user data is part of the profile—if you haven't redirected profile folders—the user will be even more confused, because the data she saved in one local My Documents folder won't be in another one.) If she makes a *bad* change, that change translates to a Help Desk call that can be tricky to figure out until you determine to which terminal server the user is connected. This is especially true because the problem might vanish if the user logs off and then logs back on and the Session Broker sends her to a different terminal server.

To avoid this scenario, all the terminal servers should use the same copy of the profile, which means that you need to use roaming profiles stored on a file share. When a user logs on, the User Profile Service looks at the user account properties to see where the profile reserved for terminal server sessions is kept and loads it from there.

When a user logs off, the profile is either deleted from the terminal server or retained in the local cache, depending on the Group Policy settings applied to the terminal servers. For faster logons, cache the profile but ensure that there's enough space on the hard disk holding the cache to support everyone who might need to cache their profile there.

Using Roaming Profiles with Terminal Services

This section discusses managing roaming profiles in a terminal server environment, including:

- How to convert an existing local profile to a roaming profile.
- How to use Group Policy to automatically set up the roaming profile storage area.
- How to create the Group Policy infrastructure that supports these policies, including security filtering and loopback policy.
- How to manage roaming profiles cached on the terminal servers.

Converting an Existing Local Profile to a Roaming Profile

In many cases, you won't start over with new roaming profiles but will have local profiles already in use that you must convert to roaming profiles.

Note It's very unlikely that you would convert a local profile that a user has been using on a desktop to be his Terminal Services roaming profile. The user may have administrative access to his personal computer, and could have installed numerous applications and made many customizations that don't apply to the shared (and more locked-down) world of terminal servers.

To do this, first you create a shared location to store Terminal Services user profiles. Give this folder the appropriate NTFS and share permissions. Tables 4-3 and 4-4 show the minimum share and NTFS folder permissions that need to be set.

TABLE 4-3 Share Permissions for a TS Roaming Profiles Storage Folder

User Account	Share Permissions
Everyone	Full control

TABLE 4-4 NTFS Permissions for a TS Roaming Profiles Storage Folder

User Account	NTFS Permissions
Creator owner	Full control, subfolders and files only
Local system	Full control, this folder, subfolders, files
User group that needs access	List folder/read data, create folders/append data, this folder only

Direct from the Source: How Profile Folders Are Named

The way that a user's profile folder is named depends on the circumstances in which it's created. The user My Name (with user name myname) with an account in Domain1 will store his profile in one of two places: \TS-Roaming-Profiles\myname or \TS-Roaming-Profiles\myname.Domain1.

The best case is that we add the domain name to the profile path; this disambiguates the path when there are two (or more) users with the same name living in different domains. For example, in a large corporate network, you might have Domain1\myname (that's me) and Domain2\myname (some other user). When Domain1\myname logs onto a legacy terminal server the profile created for him will be . . . \myname. If Domain2\myname later wants to store his profile on the same server, he will have a problem. That's why we added .domain to the profile path, so that users with the same name but from different domains would have different profiles. So ideally, we always want to add .domain to the profile path.

But then, what do we do with profiles that were created before we made this change and don't have .domain in the name? Leave them as is. But in this case, how do we know which user this particular profile belongs to? We use permissions to determine that. When the User Profile Service creates a new profile, it gives full control to the user whom this profile is created for. So, if Domain1\myname has explicit full control permission to the ...\myname folder, then this profile belongs to me and not to Domain2\myname. That's why we have this logic when creating profile names.

Here is the logic we use to create the profile path:

1. Attempt to locate the ...*username.domain* path. If it exists and the user has explicit permissions to it, then use it.
2. If the user does not have explicit Full Control access to ...*username.domain* or this folder does not exist, then try to access ...*username*.
3. If ...*username* exists and the user has explicit permissions to it, then use it.
4. If the user does not have explicit Full Control access to ...*username* or the folder does not exist, then use ...*username.domain*.

As you can see, by default we always create the folder with ...*username.domain*. Only when ...*username* folder exists and user has explicit Full Control access to it do we use it. Again, it's always best to include the domain name in the profile path so that two people with the same user name with accounts in different domains can store their profiles in the same central share.

Sergey Kuzin

Software Development Engineer II

To copy the local profile a user created on a terminal server to the designated file share, log on to the terminal server that contains the user's local profile using a domain admin account. Open the System Properties dialog box (in the Control Panel, or accessible by right-clicking Computer and choosing Properties). Click the Advanced tab and then click Settings under User Profiles, as shown in Figure 4-5.

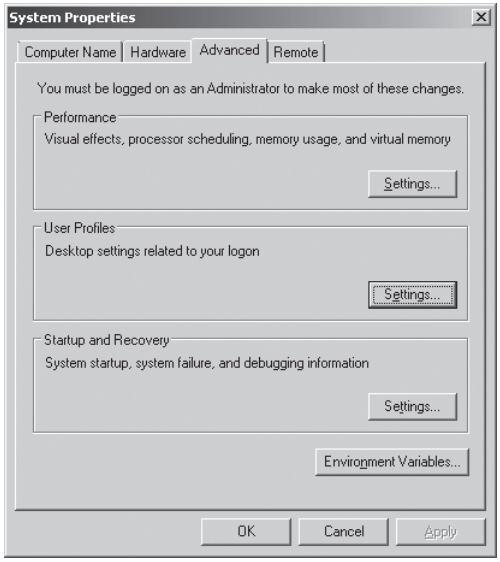


FIGURE 4-5 System Properties User Profiles Settings

Highlight the local user profile you want to make a roaming profile and click Copy To, as shown in Figure 4-6.

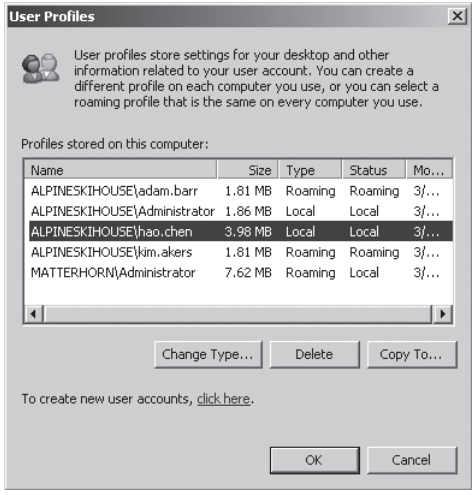


FIGURE 4-6 To move a local profile to a new location, highlight the user local profile and click Copy To.

You will see a dialog box like the one shown in Figure 4-7. Type or browse to the share location where you want to copy this profile.

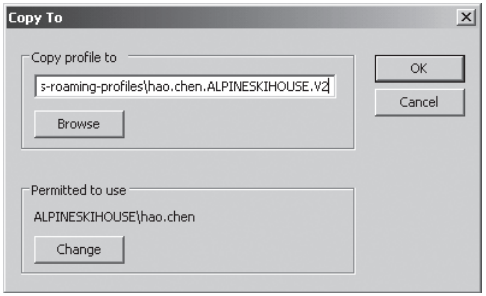


FIGURE 4-7 Enter the location to copy the user profile and give the user permission to use the profile.

The location path should take this form: *Servername**Sharename**username.DomainName*.V2.

Note Windows 2008 and Windows Vista profiles have a .V2 extension. Windows 2008 and Vista profiles are not compatible with Windows 2003 and Windows XP profiles.

To give the user permissions to use the profile, click Change and select the user's account from Active Directory. Click OK and then click OK again to exit. The profile will be copied to the designated location, with the folder name *username.DomainName*.V2.

Next, configure the user's Active Directory account to use this profile when logging into the terminal server. Open Active Directory Users And Computers and open the Properties dialog box for the user's account. Move to the Terminal Services Profile tab and type the Profile Path location using the format *servername**share name**%username%*.*DomainName* as shown in Figure 4-8.

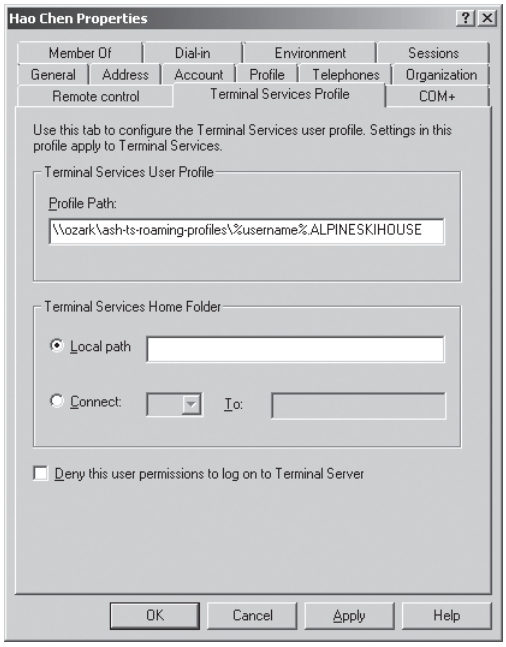


FIGURE 4-8 Type the Terminal Services User Profile path.

The variable %username% inserts the user account name into the profile path, so you don't have to customize the path for each person when adding new accounts manually or through a script. Nor do you need to add the .V2 extension to this path; it will be added automatically because the profile will be a 2008 version profile. The next time the user logs on to the terminal server, she will use her roaming TS profile.

On the Companion Media For tips on how to avoid the "duplicate link" problem you can introduce when converting a local profile to roaming, see *http://blogs.technet.com/deploymentguys/archive/2008/05/01/dealing-with-duplicate-user-profile-links-in-windows-vista.aspx*. You can find the link on this book's companion CD.

As you can see, converting an existing local profile to a roaming profile involves some work. If you start over with a new roaming profile for users using the terminal server, you can skip most of the steps. Just specify the Profile Path as explained previously and then:

- The User Profile Service will create a profile folder and profile in the specified path the first time the user logs on.
- The user will be the owner of the folder and will therefore be the only one to have access to it.

If you copy a local profile to the correct share path *before* the user logs on, the Administrator will be the owner of the folder—not the user—and will be able to access the profile contents. Although a user profile folder is for the user's convenience, it is also useful for administrators to be able to access the contents of the folder to delete a corrupted profile or perform other maintenance. To permit this, give the Domain Admins group full control NTFS rights to the parent folder, and pre-create TS roaming profile folders for each user in the TS roaming profiles share. Make sure that the user has full control of his profile folder, subfolders, and files and that the user is also the owner of the folder.

Direct from the Field: Managing Roaming Profiles Without Admin Access to the File Server

To use roaming profiles, you need a file server to store them on. In a smaller deployment, you may have administrative rights to the file server as well as the terminal servers, but enterprise deployments often segregate ownership. If you aren't an administrator of the file server, you can't directly manage the folders—you'll need to ask the file server administrator. Even the Group Policy setting Add The Administrators Security Group To Roaming User Profiles will not help if the terminal server administrator is not a member of Administrators group on the file server. You could lobby to become a member of the Administrators group on the file server, but this is counter to Least Privilege Access principles.

You can resolve this situation with a logoff script. Use Icacls.exe to include TS administrators to the user profile's permissions during logoff from user's security context. This works because the user has full access permissions to his profile, so she can add necessary permissions for TS Administrators. For example, the Logoff script might look like this:

```
Icacls.exe \\<profile root>\%username%.%userdomain%.v2 /grant <TS Admins group>:
F /T /Q
```

Add this script to each user through Group Policy: User Configuration | Windows Settings | Scripts | Logoff Script. Now you can manage that profile folder.

There are two reasons to do this at logoff, not logon. First, if the user is logging on for the first time, the profile folder may not yet exist, so the settings wouldn't apply until the second time. If the user never logged in again, you couldn't delete his profile without the help of the file server administrators. Second, if the profile is large, it takes some time for icacls to go through the whole tree. Users do not like long logon times, so why make them wait to start working? Let the script process permissions when they're done working and less concerned about the time.

Bohdan Velushchak

Operations Engineer, MSIT

If you have your terminal servers in their own organizational unit (OU), you can also create a computer GPO with Loopback Processing enabled and give administrators access to profile contents by enabling the following GPO setting: Computer Configuration | Policies | Administrative Templates | System | User Profiles | Add The Administrators Security Group To The Roaming User Profile Share. For more information on using Group Policy to create and manage TS roaming profiles, see the section titled "Using Group Policy to Manage Roaming Profiles" later in this chapter.

Direct from the Field: Choosing the Right Local Profile to Convert

The number one problem is that most administrators are scared of Roaming User Profiles. They don't understand how they work, how to properly set them up on a file server, or how to set up the GPO to apply them to users, so instead they just use local profiles on the terminal servers. Then when they add a second server, they don't know why the users are complaining about all their settings being lost. After setting up their profiles, the next time the users log on, they access the original server and find their Outlook nickname file is missing entries. After adding a third or fourth server, the cycle repeats itself.

Now they finally decide to implement Roaming Profiles. OK, which local profile do they copy to the profile share on the file server? The network administrator may wonder what to do.

Since most people would rate their Outlook nickname file as most important to keep, copy the profile that has the most recent date or the largest size.

Carl Webster

Senior Enterprise Engineer, SARCOM

The preferred way to specify Roaming Profiles to use in a Terminal Services session is to create a GPO that dictates the terminal services roaming profile location for everyone that logs into any terminal server in a farm. The next section explains how to do this and how to set up the Group Policy infrastructure you'll need.

Using Group Policy to Manage Roaming Profiles

To create a GPO that dictates the Terminal Services Roaming Profile location for everyone who logs on to any terminal server in the farm, it's imperative to set up the terminal server environment OU and create the GPOs correctly. This is the single most important part of successfully using roaming profiles with terminal servers.

Group Policy has many different uses, but it all comes down to making changes to many computers or many users all at once, instead of individually configuring those computer user settings. Computer settings are applied when a computer boots up; user settings are applied when a user logs on. Because the settings are applied at logon, they don't have to be saved as part of a user's account properties.

Because computer settings are applied before the user policies, when managing terminal server settings you'll use an additional GPO to enforce *loopback policy processing*. We'll talk about loopback policies in the section titled "The Ins and Outs and Ins of Loopback Processing" later in this chapter. For now, the most important thing to remember is that this policy reapplies the user-specific settings that are placed on the OU where Loopback Processing is enabled after the normal user GPOs are applied, so the settings placed on the terminal server OU will always take precedence in case of a conflict.

There's some overlap between the computer-specific and user-specific settings in Group Policy, but you'll generally find that you'll need both to configure the users' working environment. When setting up a terminal server environment, where it's important not just that you are logging on but that you're using a terminal server, you'll definitely need both.

Note The following explanations assume that you have permission to manage Group Policy for your terminal servers. If this is not the case, you'll need to provide the instructions to the administrator controlling Group Policy for your organization and let him fit them into corporate management policy. This is *one* way to organize your terminal server GPOs, but it is not the only possible model. GPO architecture is very individual to the particular situation. For example, for some organizations, blocking inheritance may not be an option for policy reasons. For more information on Group Policy modeling, see "Design Considerations for Organizational Unit Structure and Use of Group Policy Objects," located at *http://technet2.microsoft.com/windowsserver/en/library/2f8f18cf-a685-48db-a7be-c6401a8fb6341033.mspx?mfr=true*. You can find the link on this book's companion CD.

Creating Group Policy Objects to Work with Terminal Server Users and Computers

To manage terminal servers using Group Policy, first create an organizational unit (OU) and place all the terminal servers you want to manage together in it. All terminal servers in the same farm should definitely be in the same OU. Computers can be in only a single OU. To create a new OU, open Active Directory Users And Computers, right-click the domain, and choose New | Organizational Unit. Name it something descriptive such as Terminal Servers and then drag and drop the terminal server computer objects into the OU (see Figure 4-9).

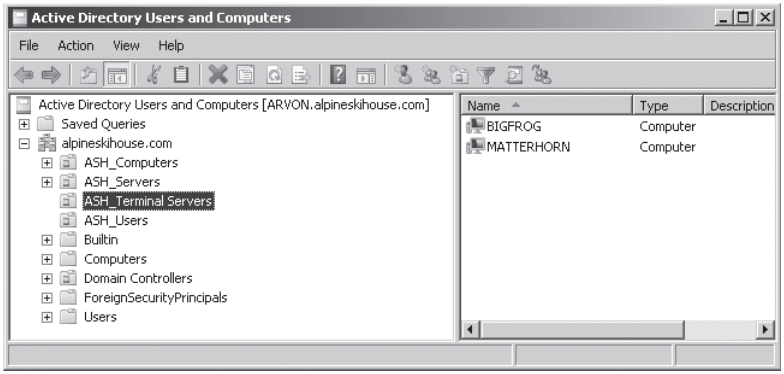


FIGURE 4-9 Create an OU for your terminal servers.

Next, block GPO inheritance for this OU so that only computer settings set by GPOs linked to this OU will apply to the computers in this OU, and only user settings set by GPOs linked to this OU will be applied to users logging on to the computers in this OU. Other GPOs set at the domain or site level will not be applied. To do this, open the Group Policy Management Console (Start | Programs | Administrative Tools | Group Policy Management), right-click the Terminal Servers OU, and choose Block Inheritance.

Next create two different types of GPOs: a computer GPO and a user GPO, as shown in Figure 4-10. Although one policy may contain both user-specific and computer-specific settings, it's best to isolate the two unless your environment is very small or your user base is very homogenous. This allows you to create a consistent model of terminal server management while still allowing you the flexibility to apply different policies to different groups of users.

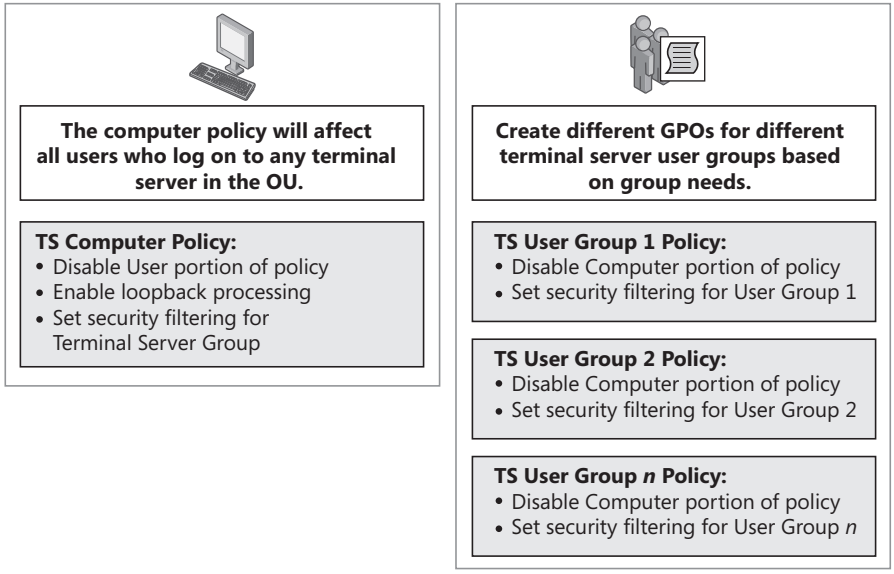


FIGURE 4-10 Creating separate user and computer GPOs for the Terminal Services environment

To create the GPOs for your terminal server environment, open the Group Policy Management Console (Start | Programs | Administrative Tools). Right-click the Group Policy Objects folder in the left pane, found under your domain folder, and choose New to show the dialog box in Figure 4-11. Name the computer policy something descriptive like TS Computer Policy.

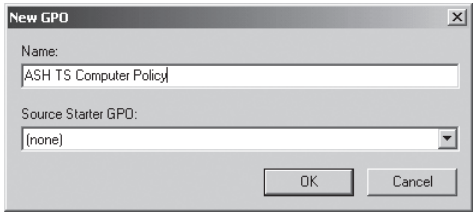


FIGURE 4-11 Create a terminal server computer policy.

Click OK, and you will be back in the Group Policy Management console, with a list of available policy objects—including the one you just created—in the right pane. When you click your Computer Policy, you will see a screen similar to the one in Figure 4-12.

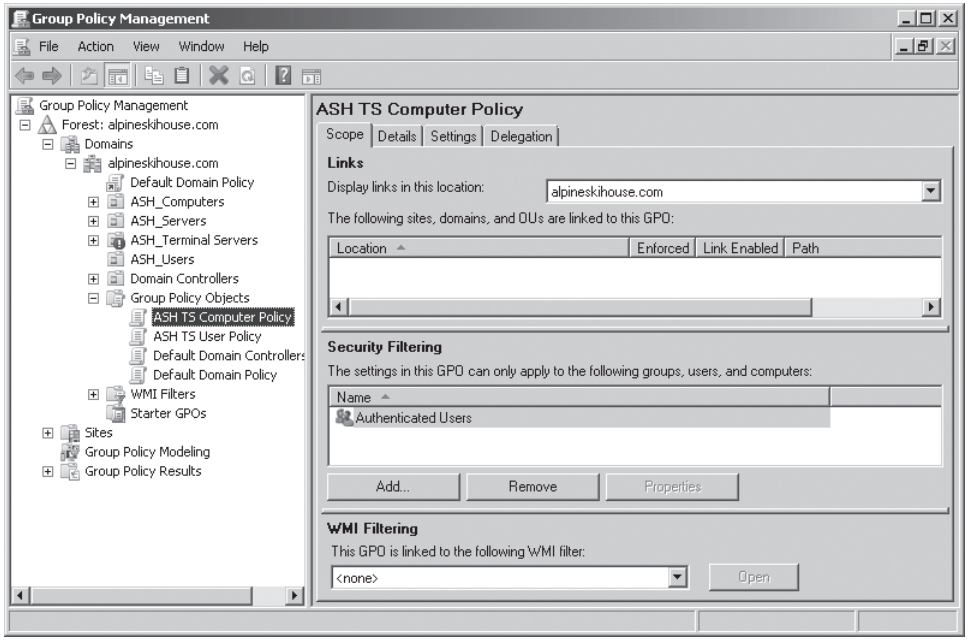


FIGURE 4-12 ASH TS Computer Policy default screen

Click the Details tab in the upper portion of the right pane. Here, there's a GPO Status drop-down list with four options: All Settings Disabled, Computer Configuration Settings Disabled, Enabled, and User Configuration Settings Disabled. To remove any user-specific settings from this GPO, select User Configuration Settings Disabled. This is important because you will

use loopback policy to apply user GPOs placed on the terminal server OU after user logon. Making sure no user policies inadvertently set in a computer GPO get applied will help you better manage your environment.

Note You can create and use multiple computer policies for terminal servers, but take special care to set the security on all computer GPOs exactly the same. Remember, the main goal here is to create a consistent environment across all terminal servers.

Follow the same process to create a new user-specific GPO. For the User Policy GPO (like the one shown in Figure 4-12), select Computer Configuration Settings Disabled from the drop-down menu on the Details tab. You can create more than one User Policy if you need to implement a different set of policies for different user groups.

Fine-Tuning GPOs with Security Filtering

A GPO works because by default anyone in the Authenticated Users group is allowed to use it—and Authenticated Users means "anyone who logged on to the domain." Computers actually log on to the domain, so they're members of this group.

To narrow the scope of to whom (or to what) these policies will apply, double-click the GPO in the Group Policy Objects folder and then turn to the Scope tab shown in the right pane. In the Security Filtering section on this tab, you can edit the users and groups to determine to whom the GPO will apply.

For your Computer Policy, you will want the settings to take place on all terminal servers. Add each terminal server computer object to the Security Filtering section (or if you have created a Terminal Servers group, then add it). Click the Add button to select the objects you wish to add and then click OK, as shown in Figure 4-13.

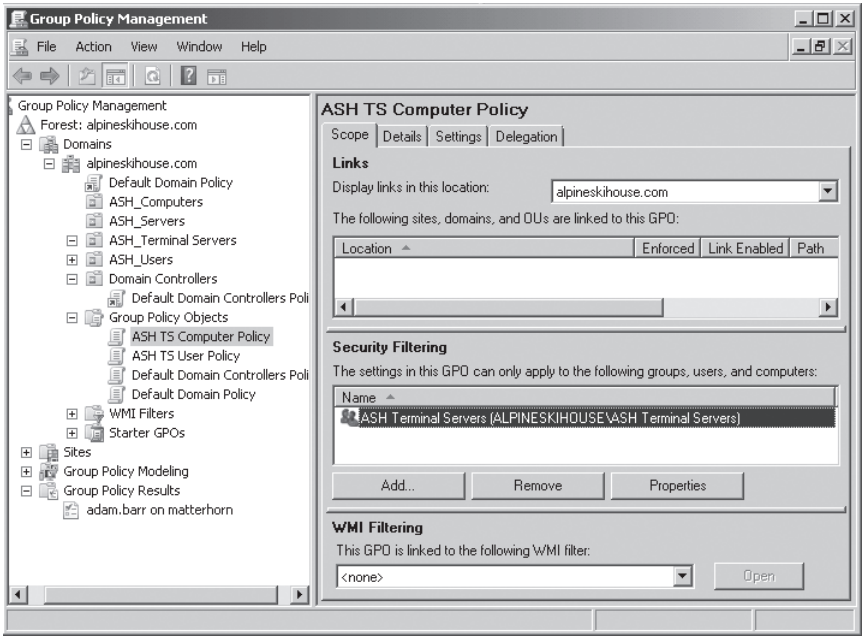


FIGURE 4-13 Add the terminal server computers group to the computer GPO security filtering.

Modify the Users Policy GPO Security Filtering to include the specific users group for which you want settings in the GPO to apply, as shown in Figure 4-14.

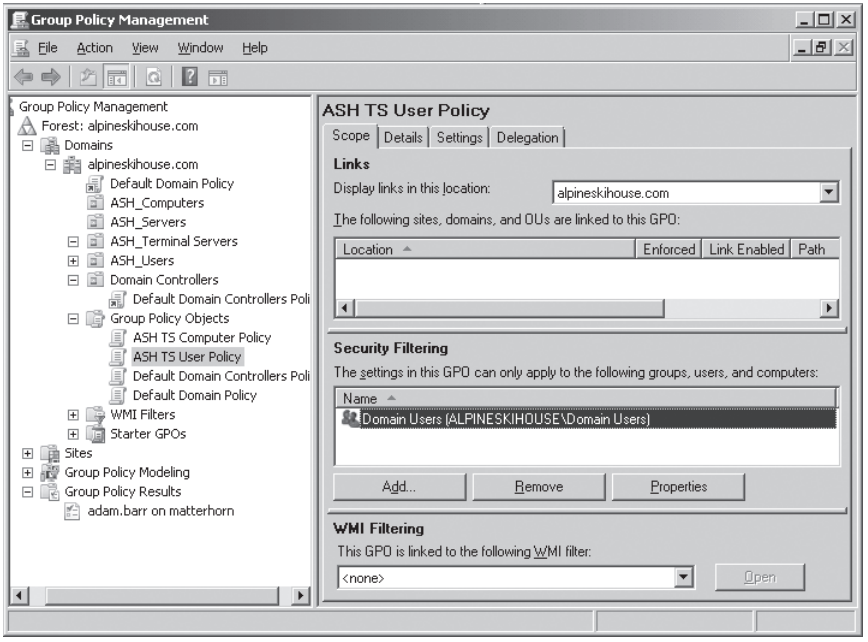


FIGURE 4-14 Add users to the GPO Security Filtering section of the ASH TS Users Policy.

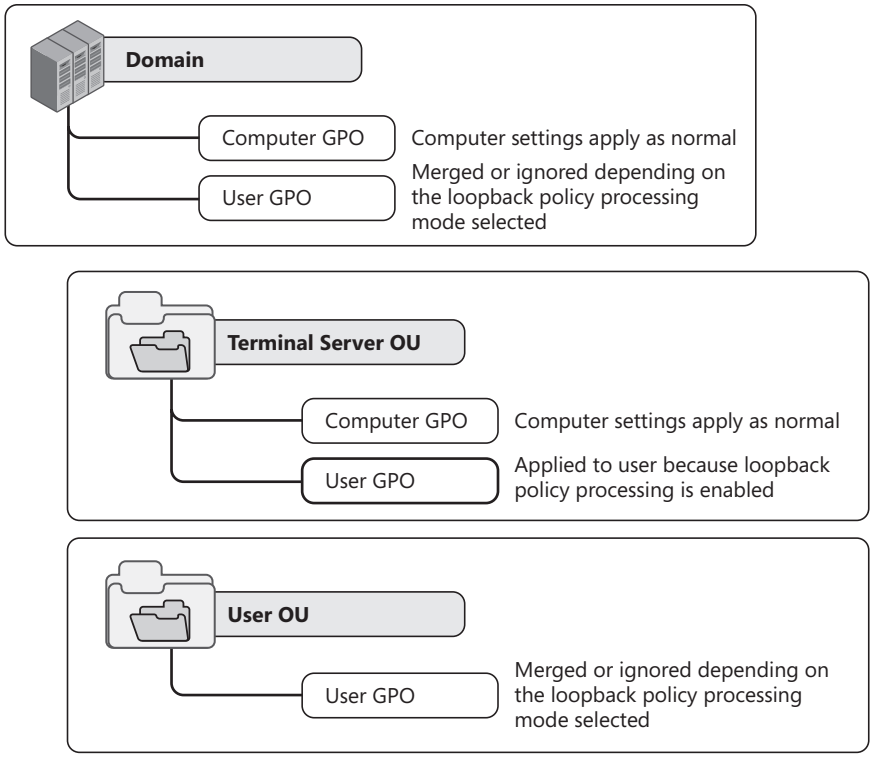
Figure 4-14 shows the Domain Users group added to the Security Filtering section, but you can add any group here.

The Ins and Outs and Ins of Loopback Policy Processing

Outside a terminal server environment, you apply a lot of Group Policy based on the persona of the user logging on. If you don't want Adam Barr to open Control Panel, for example, you probably feel much the same way about this whether Adam Barr is logged on to his desktop computer or his laptop. Similarly, if you don't care about him running Control Panel on the desktop, then you continue not to care whether he's logged on to his desktop or his laptop. It's his space—let him mess it up. (The Help Desk may feel differently about this, but that's another matter.)

Enabling Loopback Policy Processing changes the order in which policies are applied. Normally, computer GPOs are applied when the computer starts up. Then user GPOs are applied when a user logs on. Therefore, the computer policy will always be applied first, then the user policy. If a user policy and a computer policy conflict, and the user policy is able to override the computer policy, the user policy will always win because it's applied last.

On a personal computer, it's perfectly acceptable to have the identity of the person logging on define the final settings for Group Policy. But a terminal server is one of the location-specific or context-specific situations in which *where* you are matters even more than *who* you are. For example, you might decide that it's acceptable for users to use clipboard redirection when connecting to remote desktops, but for security reasons you don't want them using clipboard redirection when connecting to a terminal sever farm hosting sensitive data. You need policies applied based on which computer you are logged on to. In this case, you will apply loopback policy processing to tell the Group Policy engine to apply the user GPOs that pertain to the computer (that are applied to the Terminal Server OU) after (or instead of) applying the user GPOs that are normally applied during logon. With loopback policy processing enabled, GPO processing will now work like this:



When the terminal server boots, computer GPOs are applied. When the user logs on to the terminal server, user GPOs are applied to their session (or ignored if loopback processing Replace Mode is selected). Then, because loopback policy processing is enabled, user GPOs that are applied to the terminal server OU are applied.

To enable loopback processing, right-click the Computer GPO applied to the terminal server OU and choose Edit. The Group Policy Management Editor opens the GPO. Go to Computer Configuration | Policies | Administrative Templates | System | Group Policy and find the policy User Group Policy Loopback Policy Processing Mode node in the pane at right. Double-click it and you will see the dialog box shown in Figure 4-15.

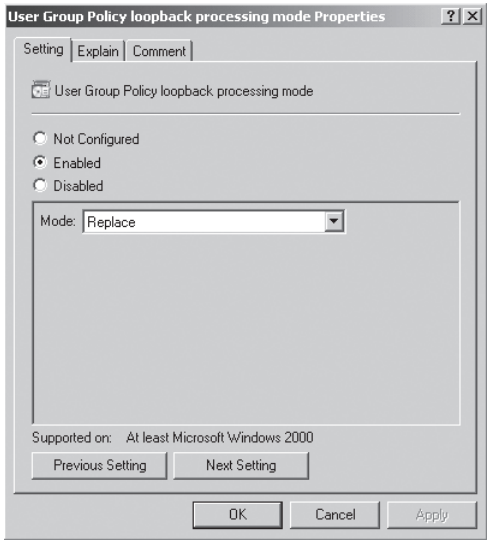


FIGURE 4-15 The User Group Policy Loopback Processing Mode Properties dialog box

How It Works: Applying Loopback Policy

Loopback policy can apply to users in one of two ways: Merge Mode and Replace Mode.

- In Merge Mode, Loopback Policy Processing will apply the user GPOs placed on the Terminal Server OU along with the normal user GPOs assigned to the OU where the user account resides. If there is a conflict, then the user GPOs applied to the terminal server OU will override.
- In Replace Mode, the Group Policy engine ignores the user's GPOs placed on the OU where the user account resides and applies only the user GPOs that apply to the terminal server.

Merge Mode or Replace Mode?

Whether you choose Merge Mode or Replace Mode (see the previous sidebar, "How It Works: Applying Loopback Policy") depends on your goals and how you've set up the rest of your environment.

If users are using the same GPOs to log on to the terminal servers and to their local desktops, their user settings may not mesh well with a shared environment. If that's the case, then you'd pick Replace Mode. If you want the user experience to be as similar as possible for both local and remote logons, then Merge Mode may be more appropriate for you, because it will preserve user-specific policies. The main thing you'll need

to watch out for is that GPO settings from the GPOs applied to the user do not cause problems for your user when she is logged on to a terminal server. Using Merge Mode is more work, because it requires a lot of considering of individual policies and their effect on a remote workspace scenario.

Using gpupdate /force

Active Directory does not immediately send Group Policy changes down to the computers to which they apply. The Group Policy Engine on the computer (in our case the terminal server) actually pulls the GPO changes from Active Directory at specific intervals, called the *refresh interval*. By default, the refresh interval is 90 minutes (plus a random time ranging from 0–30 minutes). To immediately see the effects of changes you make to GPOs, you can force this refresh. Open a command prompt on your terminal server and type **gpupdate /force**. Rebooting the terminal servers has the same effect.

Using Group Policy to Define the Roaming Profile Share

After you have a Group Policy infrastructure set up, you can effectively create a policy to automatically create roaming profile folders in the proper folder share location.

The Group Policy setting to set the path for TS roaming profiles is in the Computer Configuration GPO folder. Right-click your TS Computer Policy GPO and choose Edit. Expand the GPO to Computer Configuration | Policies | Administrative Templates | Windows Components | Terminal Services | Terminal Server | Profiles. In the pane at right, double-click Set Path For TS Roaming User Profile, shown in Figure 4-16.

Note It may seem counterintuitive to set the TS roaming profile path for computers, not for users. But the terminal servers must know where to find the roaming profile so the User Profile Service can load it when a user logs on.

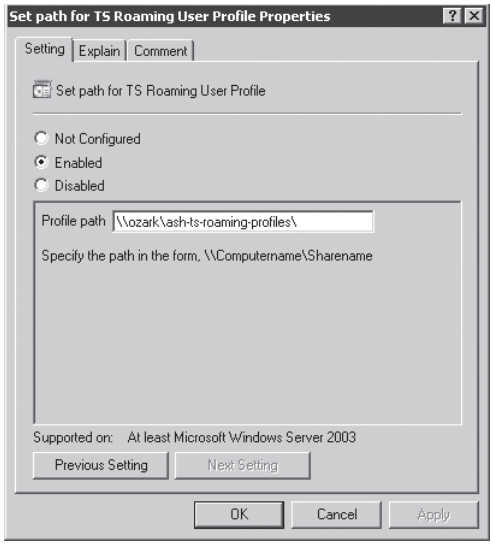


FIGURE 4-16 Set the path for Terminal Services Roaming User Profile storage.

Select the Enabled option and type the TS roaming profile share location in the Profile Path text box. If you use Group Policy to set the TS roaming profile path, then the profile folders that are created take the form of *username.domainname*.V2; you do not need to add the %username% variable, the domain name, or the .V2 extension. This is in contrast to defining the path to the Terminal Services profile folder by editing the user account properties through scripting or through Active Directory Users And Computers, where you must specify the *username* and *domainname* variables to create the folder properly.

Note If you already have profiles stored in the profile path and the profile folders do not include the domain name (perhaps they take the form of *username*.V2), change the names to include the domain name. Otherwise, the existing profile will not be seen, and a new one will be created in the format *username.domainname*.V2.

If the profile folders are created automatically when the user logs on, then he gets sole access to his profile and is also set as the owner of the profile folder. To permit administrators to access the profile, enable the following GPO setting: Computer Configuration | Policies | Administrative Templates | System | User Profiles | Add The Administrators Security Group To Roaming User Profiles. With this GPO setting enabled, the following permissions are placed on newly created user folders:

- User—Full Control, owner of folder
- SYSTEM—Full Control
- Administrators—Full Control (This is the local administrators group of the server where the profiles are stored, which also contains the Domain Admins group.)

You can also pre-create user profile folders and set permissions as required. For more information about profile folder permissions, see the section titled "Converting an Existing Local Profile to a Roaming Profile" earlier in this chapter.

With this GPO setting set, users accessing the terminal servers in this OU will now have a roaming profile created and stored in the designated share.

Speeding Up Logons with Small Profiles

One of the biggest tasks that IT professionals face in a terminal server environment is to provide and maintain a consistent and efficient user experience. Users want to log on quickly, work steadily, get their job done, and get out. If they find that they have to wait longer to log on than they like, the IT department will hear about it.

Roaming profiles provide a consistent user experience across all terminal servers, following the user to whichever terminal server they log on to, instead of the randomization that local profiles stored on the terminal servers will produce. The roaming profile is also stored in a central location, where it's easy to back up. Roaming profiles definitely have some benefits. But if they are not well controlled and well-maintained, they can cause problems. As profiles are used over time, they grow in size. Recall the kinds of folders that are stored in a user profile: Documents, Desktop, Favorites, and more. If users add files to any of these places (and of course they will), the profile gets bigger. Over time, they can—and usually do—get a *lot* bigger.

When a user logs on to a terminal server, her roaming profile has to be copied to that terminal server, and when she logs out, changes must be copied back to the roaming profile storage location—and not just the changes, because writing profiles to their storage space is not writing the delta between the starting point and the ending point, but the entire file. Imagine if one of your users saved 30 gigabytes (GB) of data in his Documents folder. He would log on to the terminal server and then go get a cup of coffee. Or take lunch. Now imagine if all of your users had that much data stored in their Documents folder. If they all come in at 9 A.M. and try to log on to the terminal server, logons could quickly consume all of your network bandwidth. Soon the water cooler or break room would be very popular, and no one would get any work done.

Profile caching also suffers if you experience profile bloat. *Profile caching* saves a copy of the user profile on the terminal server, so that if the network is slow to retrieve the saved profile from its file share, the user can still log on using the cached copy. (When you log onto a terminal server, a copy of your profile is saved there as a matter of course. If you enable profile caching, the profile just isn't deleted when you log off.) However, if the profiles in the cache are too large, the space allocated for them will fill up, and people won't be allowed to log on, because there's no room to store their profile.

To speed logons, you have to control profile size. There are a few ways to do this, and you'll likely end up with some combination of them:

- Limit the size of the profile by policy.
- Trim cached profiles not used for a certain period of time so you have room to cache the profiles you really need.
- Use folder redirection to limit the amount of data in the profile.

Limiting Profile Size

One way to reduce the impact of caching profiles on the terminal servers is to limit the size of the profiles. Although too many profiles can still fill up the hard disk, smaller cached profiles have less impact. To limit profile size, open your TS User GPO and browse to User Configuration | Policies | Administrative Templates | System | User Profiles. Locate the policy Limit Profile Size and enable it.

Note If you're redirecting folders, the size of the profile shouldn't be a major concern. NTUSER.DAT is a fairly small file. The exact size depends on the profile, but it's not much; check the size of one of your NTUSER.DAT files to adequately gauge the space needed to allocate space for profiles.

Removing Cached User Profiles on Terminal Servers

Another way to keep the size of the cache on the terminal server(s) from getting too large is to delete old copies of the user roaming (or mandatory roaming) profiles.

Using Group Policy to Delete Cached Profiles You can use two computer Group Policy settings to automatically delete unused cached profiles on terminal servers in the Terminal Server OU. Both policies are located in Computer Configuration | Policies | Administrative Templates | System | User Profiles.

- **Delete Cached Copies Of Roaming Profiles** Enabling this setting causes a user's cached profile to be deleted each time the user logs off. This setting ensures that the loaded profile is always the most recent. However, the cached profile provides a fall-back configuration to load if the actual profile isn't available due to network issues or an offline file server. If you delete cached profiles, then if the actual profile can't be loaded, the user will get a temporary profile and any changes they make to it will be discarded when the user logs off.
- **Delete User Profiles Older Than A Specified Number Of Days On System Restart** Enabling this setting deletes cached profiles older than a specified number of days. But beware; the cached profiles are only deleted when you reboot the server. So if you don't restart your terminal servers regularly, don't expect this setting to do much deleting.

Manually Deleting Cached Profiles Manually deleting cached profiles sounds too simple to bother explaining, but it's more subtle than it may appear. Cached profiles are kept in the %SystemDrive%\Users directory. However, the seemingly easiest thing to do—look at the profiles, check the dates, note that some profiles haven't been used in a while and delete them—will prevent the owners of those deleted profiles from ever being able to log on to the terminal server and load their roaming profile again, at least without some work from you. See the section titled "The Consequences of Deleting a Profile Folder From Explorer" later in this chapter, for more information.

The problem is that cleaning up old profiles isn't just a matter of deleting the directories. The registry maintains a list of profiles in HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList. Sort through that key (see Figure 4-17) and you'll see entries for everyone who currently has a profile cached on the server. Although the keys themselves are identified by the SID of the user account, you can see the name of the profile path by examining the contents of each key.

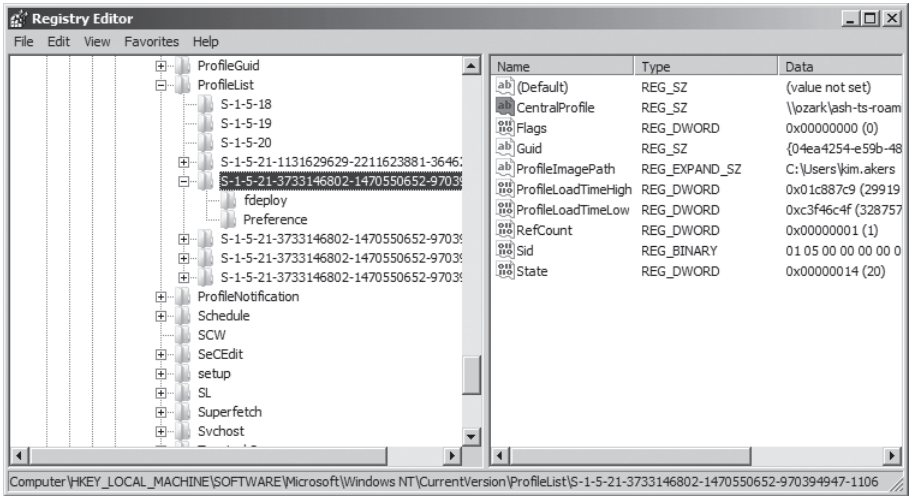


FIGURE 4-17 When you cache a profile on a server, it automatically creates a corresponding registry entry.

Note Examining this key can also help you troubleshoot profile problems. If someone seems to be getting their standard profile to log on to the terminal server, check the contents of CentralProfile (see Figure 4-17). If this entry is blank, that person is using a local profile.

To safely delete a profile, use the User Deletion Utility, Delprof.exe, currently available for download from *http://www.microsoft.com/downloads/details.aspx?familyid=901a9b95-6063-4462-8150-360394e98e1e&displaylang=en*. This tool both deletes the entire contents of the profile and cleans up the registry so that there aren't any orphaned entries causing problems later. The link to this tool is available on this book's companion CD.

You don't need to install Delprof.exe on the terminal server to clean up profiles on that terminal server. You can download and install Delprof.exe on another server or a workstation and run the tool from there. By default, Delprof.exe installs to C:\Program Files\Windows Resource Kits\Tools. To use it, open a command prompt with administrative privileges, navigate to this directory, and run **delprof** with the necessary parameters.

Note Add this path to your System Environment Path variable so you won't have to navigate to this directory each time you want to use the tool.

Table 4-5 lists the delprof parameter options.

TABLE 4-5 Delprof Parameters

Parameter	Description
/Q	Quiet, no confirmation
/I	Ignore errors and continue deleting
/P	Prompt for confirmation before deleting each profile
/R	Delete roaming profile cache only
/C	Remote computer name
/D	Number of days of inactivity

To delete the roaming profile cache on a specific server, run the command with the following arguments:

```
Delprof /R /C:\\servername
```

To be prompted to confirm the deletion, run the command with the following arguments:

```
Delprof /P /C:\\servername
```

You can also delete cached roaming user profiles from the User Profiles section of System Properties on the terminal server. Log on to the terminal server as a domain administrator. Go to Start | Control Panel | System and click Change Settings. The System Properties dialog box will appear. Move to the Advanced tab and then click Settings, located in the User Profiles section, to open the User Profiles dialog box shown in Figure 4-18.

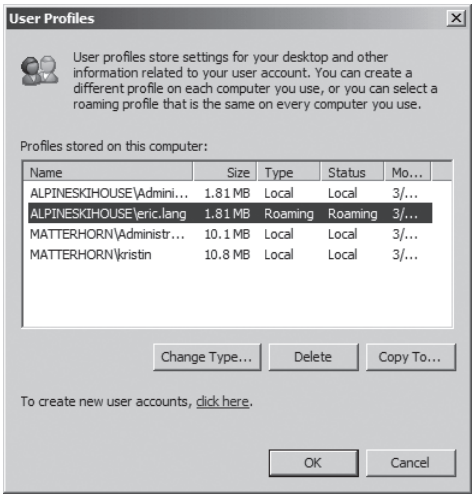


FIGURE 4-18 The User Profiles dialog box

Highlight the roaming profile you want to delete and then click Delete. When you see a dialog box confirming that you want to delete the profile, click Yes and the profile cache is deleted. Click OK.

The Consequences of Deleting a Profile Folder from Explorer

If you skip delprof or the graphical profile management tools and delete the unused profile folders from Explorer, the next time that user logs on, he will be unable to load his roaming profile. A temporary roaming profile will be created for him, and profile changes he makes will be discarded at log off. Event ID 1511 is logged in the Windows Application event log.

Note Event ID 1511 states that Windows cannot find the local profile and is logging you on with a temporary profile. Changes you make to this profile will be lost when you log off.

Deleting that directory caused a problem because you didn't completely clean up the cached profile. For each cached profile stored in %SystemDrive%\Users\%UserName%, the User Profile Service creates a registry entry for this profile at HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList, shown in Figure 4-19. This registry key is named according to the user SID.

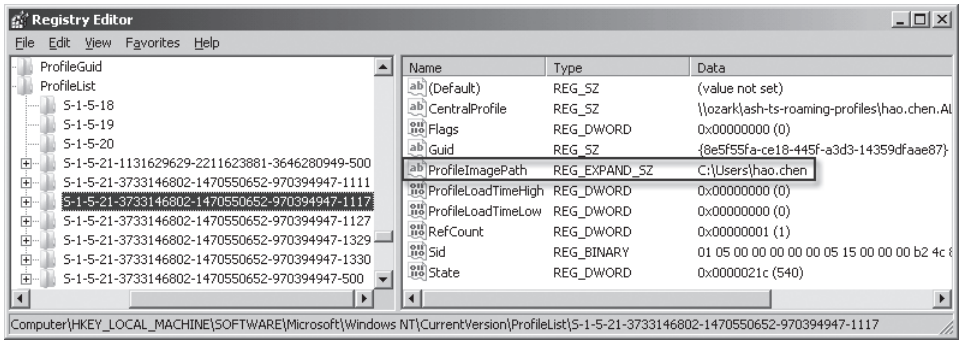


FIGURE 4-19 TS Roaming Profile cache registry entry for user hao.chen

The ProfileImagePath key in this folder indicates the cache location, by default in %SystemDrive%\Users\%UserName%. (The network location where the roaming profile is permanently stored is in the CentralProfile key.)

If you delete the user's locally cached profile folder and that user logs on to the terminal server, she will get a temporary profile. The registry entry corresponding to the user's cached profile is renamed. The SID part stays the same, but it is given an extension of .bak, and a new key is created in its place as shown in Figure 4-20.

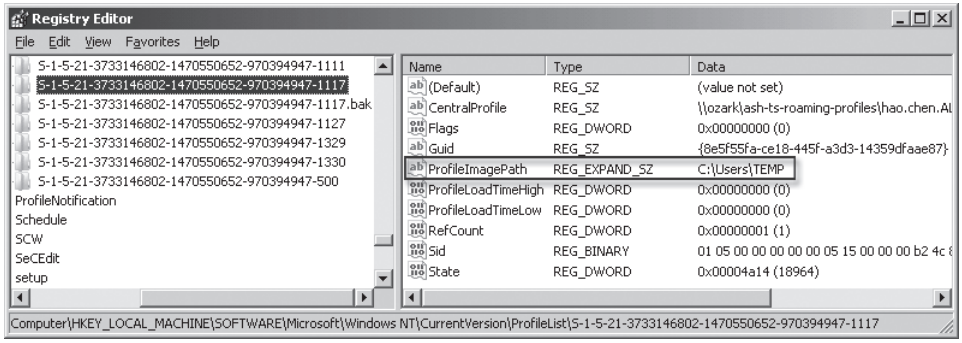


FIGURE 4-20 A new registry entry is created, but the ProfileImagePath key points to %SystemDrive%\Users\TEMP.

The newly created registry entry is named after the user SID just as before. However, the ProfileImagePath key inside the new folder now points to %SystemDrive%\Users\TEMP. So, the entry that used to work now has a .bak extension, and the one that is recognized is a temporary profile. When the user logs off, his temporary profile is not copied back to the central profile storage location on the fileserver. Delprof cannot help you here. It doesn't even recognize there is a problem with this user's profile now.

Deleting the rogue profile from the System Properties dialog box User Profiles section no longer works either. Most likely, the profile will not even be listed in the dialog box. If it is, it most likely means that the user has not completely logged off. If you do manage to select it and click Delete, you get the message shown in Figure 4-21.

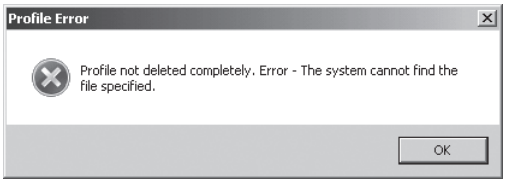


FIGURE 4-21 You can't use tools to clean up a partially deleted cached profile.

To correct this you must manually delete the abandoned registry entry that has the .bak extension. Only then can the user log on to the terminal server and have his roaming profile correctly cached once again on the server.

Centralizing Personal Folders with Folder Redirection

The biggest thing you can do to affect profile size is to not store user data in a user's profile. By default, user data folders such as Documents are in the profile, but they don't have to be. Instead you can create a pointer to a network share where the data actually lives. The user will still store files in their personal folders, but the user data won't be roamed so it will not impact the time required to load the profile to log on.

Not all profile folders can be redirected, but the ones with the biggest impact on profile size can be. These folders are:

- **AppData(Roaming)** Contains a user's application settings that are not computer specific and therefore can roam with the user.
- **Desktop** Contains any items a user places on his desktop.
- **Start Menu** Contains a user's Start menu.
- **Documents** Contains documents saved to the default location.
- **Favorites** Contains a user's Internet Explorer favorites.
- **Music** Contains a user's music files saved to the default location.
- **Pictures** Contains a user's pictures saved to the default location.
- **Video** Contains a user's video files saved to the default location.
- **Contacts** Contains a user's contacts saved to the default location.
- **Downloads** Contains a user's downloads saved to the default location.
- **Links** Contains a user's Internet Explorer Favorite Links.
- **Searches** Contains a user's saved searches.
- **Saved Games** Contains a user's saved games.

Before you redirect these folders, you need a place to redirect them to. Create a shared folder on the server where you want to store the redirected folders and set permissions on this folder according to the user profile folder permissions stated in Tables 4-3 and 4-4.

To redirect the folders to this share, open the Group Policy Management Console, create or select an existing user GPO, right-click, and choose Edit. Go to User Configuration | Policies | Windows Settings | Folder Redirection, shown in Figure 4-22.

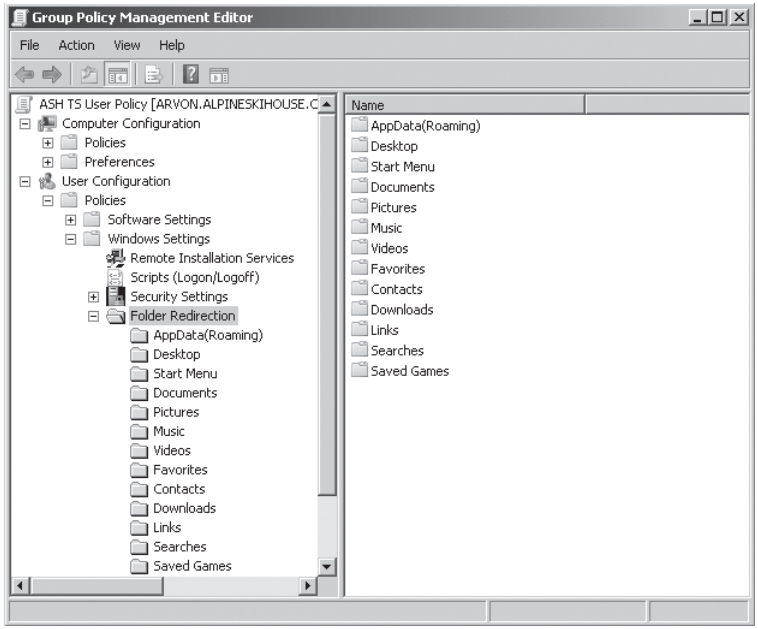


FIGURE 4-22 Setting the folder redirection policy

Right-click the AppData(Roaming) folder and choose Properties to open the dialog box in Figure 4-23.

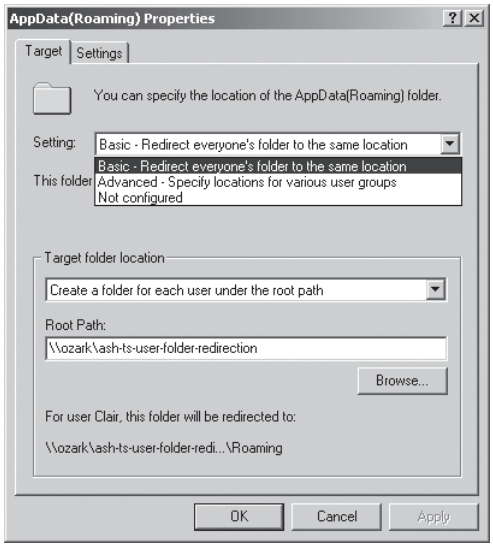


FIGURE 4-23 AppData(Roaming) folder redirection properties

To specify the location of the AppData(Roaming) Folder, choose between two options in the Setting drop-down menu.

- **Basic – Redirect Everyone's Folder To The Same Location** This means just what it says; all AppData(Roaming) folder data for every user will go to the same location.
- **Advanced – Specify Locations For Various User Groups** To store user data in different locations based on user group membership, choose this option.

Depending on which option you choose, the choices below that area change to adhere to your Setting choice. If you choose Basic, then you get a Target folder location drop-down menu with three choices:

- **Create A Folder For Each User Under The Root Path** Choose this option to put each user's profile data into a folder under the root path named according to their user name. In the Root Path text box, specify the location of your designated folder redirection share.
- **Redirect To The Following Location** Choose this option to redirect all user data to the same location. Do not choose this option if you want all users to retain their own settings. If you do, then the first user's data will get saved to the chosen location as expected, but subsequent users will attempt to save to the same location—unsuccessfully, since the first user will be the owner of the folder. Event error ID 502 will be logged in the Application event log, telling you that the specified path is invalid. However, this option does have a good purpose, as you will see in the section titled "Creating a Safe Read-Only Desktop" later in this chapter.
- **Redirect To The Local Profile Location** Your profiles roam, and you want your profile folders redirected to the network share, so do not choose this option.

Click the Settings tab shown in Figure 4-24.

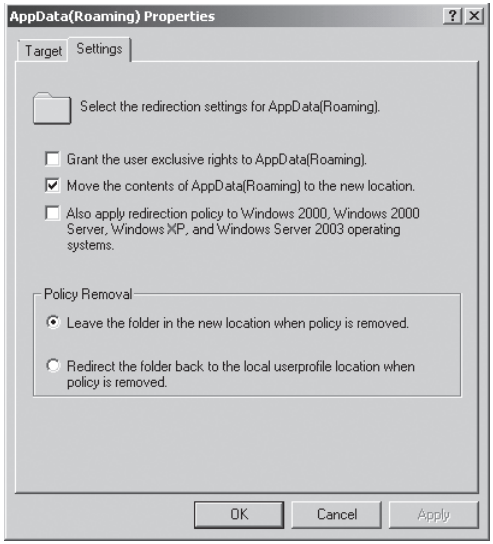


FIGURE 4-24 Clear the box for the option Grant The User Exclusive Rights To AppData(Roaming) to let administrators manage the redirected folder.

By default, Grant The User Exclusive Rights To AppData(Roaming) is enabled. If you leave it this way, then the user will own this folder and only she will be able to access this data. To enable managing this folder, clear this box so that the rights from the parent folder will be inherited. For example, if you give Domain Admins full control of the parent folder, then this group will have access to the redirected user folders as well.

If your users already have these folders before you set up folder redirection, then you must set up the existing folders in one of two ways, or else folder redirection will fail:

- The user needs to be the owner of the folder and can be granted exclusive rights to the folder.
- If the user does not need to be the owner of the folder, clear this box.

All of the folders listed in this GPO section have the same choices to pick from, except for the Pictures, Music, and Video folders. These folders have an extra setting that you can choose for the location of the folder: Follow The Documents Folder. This means that these folders will be stored in the user's Documents folder, wherever that folder is redirected to.

Sharing Personal Folders Between Local and Remote Environments

Because the TS RemoteApps in Windows Server 2008 are designed to blur the line between the remote computer and the local computer, it may make sense for you to help this along by using the same folder to store user-specific documents. This eliminates the problem of having to remember whether you were saving a file from a local or a remote application to know where the file would be stored.

Sharing Folders Between Windows Server 2003 and Windows Server 2008 Roaming Profiles

Note that 2003 profiles and 2008 profiles are not compatible. So, if you have some active 2003 terminal servers, you will need to keep two sets of profiles for your users—one to log on to the 2003 servers, and one to log on to the 2008 servers. However, folder redirection can be used to bridge the gap. Not all 13 folders that can be redirected in Windows Server 2008 can be redirected in Windows Server 2003—but some can. You can share the data in these folders between the 2003 profiles and the 2008 profiles. On the Settings tab of each folder in the Folder Redirection container is a check box option called Also Apply Redirection Policy To Windows 2000, Windows 2000 Server, Windows XP And Windows Server 2003 Operating Systems. For some folders, this option is available. On others (the ones that will not redirect for downlevel operating systems), it appears shaded and is unavailable. Table 4-6 shows which of the folders can be redirected for Windows 2000/XP/2003.

TABLE 4-6 Profile Folder Redirection Capabilities for Windows 2000/XP/2003 Operating Systems

Folder	Can the Folder Be Redirected for Downlevel Operating Systems?	Details
AppData(Roaming)	Yes	The following folders within AppData(Roaming) folder for 2000/XP/2003 will not be redirected: Cookies, network shortcuts, Printer Shortcuts, Recent, SendTo, Start Menu, Templates.
Desktop	Yes	
Start menu	Yes	In Windows Server 2003, the contents of the Start menu are not copied to the redirected location. It is assumed that the Start menu has been pre-created. Therefore, if you do not pre-create the Start menu and place it in the redirected location, the default Start menu located in the user's Windows Server 2003 roaming profile location is used instead.
Documents	Yes	
Pictures	Depends	If the check box is selected for Documents, this folder will follow the Documents folder for legacy operating system profiles. If Documents is not redirected, then this folder cannot be redirected for legacy operating system profiles.

TABLE 4-6 Profile Folder Redirection Capabilities for Windows 2000/XP/2003 Operating Systems

Folder	Can the Folder Be Redirected for Downlevel Operating Systems?	Details
Music	Depends	If the check box is selected for Documents, this folder will follow the Documents folder for legacy operating system profiles. If Documents is not redirected, then this folder cannot be redirected for legacy operating system profiles.
Video	Depends	If the check box is selected for Documents, this folder will follow the Documents folder for legacy operating system profiles. If Documents is not redirected, then this folder cannot be redirected for legacy operating system profiles.
Favorites	No	
Contacts	No	
Downloads	No	
Links	No	
Searches	No	
Saved Games	No	

On the Companion Media For more information on Windows Server 2003 Profiles and Folder Redirection, see *http://technet2.microsoft.com/windowsserver/en/library/06f7eebc-2ebb-47c5-8361-1958b58078cc1033.mspx?mfr=true*. You can find the link on this book's companion CD.

Setting Standards with Mandatory Profiles

One issue with roaming profiles is that users can change them. On the one hand, that's the point. On the other, change can cause problems. If users can change their profile, they can delete icons, accidentally resize their toolbar so that it disappears, add wallpaper that slows down their logon time, and so on.

One way to avoid this is to set policies controlling what users can and cannot do, and Chapter 5 explains how to do this. Another way to prevent users from making permanent changes to their profile is to make the user profile immutable. A user can change settings, but those settings will not be saved and will disappear with the next logon.

Profiles that don't change are called *mandatory profiles*. Mandatory profiles on a central store are copied to the terminal server at logon but are not copied back at logoff. Any profile changes that occur are discarded at the end of the user session. Many companies will not implement mandatory profiles because users find them too constricting, but combined with Folder Redirection, this option may give your users enough flexibility. All terminal server users can use individual profiles, or (since no one's writing to it) they can all use the same one. In this section, we'll show you how to support both scenarios.

Converting Existing Roaming Profiles to Mandatory Profiles

Setting up mandatory profiles is very similar to setting up roaming profiles using Group Policy. To convert a roaming profile to a mandatory profile, you first need to have roaming profiles working, either by setting the TS Roaming Profile path in the user's account properties in ADUC, or by using Group Policy. For information on how to set up roaming profiles, see the section titled "Using Group Policy to Manage Roaming Profiles" earlier in this chapter.

Assuming you have roaming profiles implemented, when a user logs on, her profile is stored in a subdirectory of the designated roaming profile share. To make the user's profile mandatory, in the user's profile folder, locate the file NTUSER.DAT and change its extension to .man (see Figure 4-25). The next time the user logs on, she'll be using a mandatory profile.

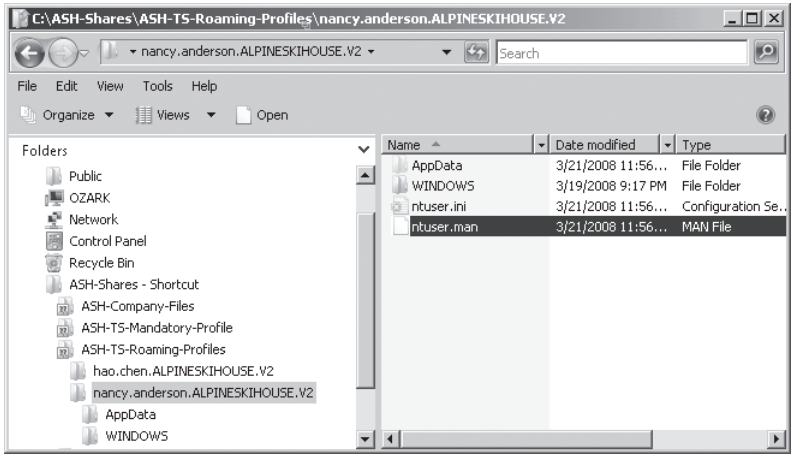


FIGURE 4-25 To convert a roaming profile to a mandatory profile, change its extension.

No changes the user makes to the profile will be saved. But combining mandatory profiles with Folder Redirection will give users some control over their TS environment and allow them to change their Favorites, Documents, Desktop, and so forth, without compromising the configuration data stored in HKCU.

Creating a Single Mandatory Profile

Mandatory profiles are easy to implement, but if you have many users, you probably won't want to manually convert each roaming profile to a mandatory one. To give everyone the same Terminal Services experience, you can create one mandatory profile for everyone as described in the following steps:

1. On a terminal server, log on as a local user with administrative rights. Use a local user account so that any Group Policy settings you have implemented on the Terminal Servers OU don't take effect. Customize the profile as appropriate and log off.
2. Create a network share to store the mandatory profile. Make sure the users who will use this profile have read access and SYSTEM has Full Control NTFS permissions. Administrators should be the Owner.
3. Set the GPOs. Edit the Computer GPO setting Set Path For TS Roaming Profile to point to the share created in step 2. Enable the Computer GPO policy setting Use Mandatory Profiles On The Terminal Server.
4. Run `gpupdate /force` on the terminal server(s) to update the policy.
5. Log on to a terminal server as a domain user. Log off. This will create a mandatory profile in the mandatory profile share inside of a new folder named .V2. Change the permissions on this folder to give users read access to the folder contents. Make Administrators the owner.
6. Log on to the terminal server used in step 1 as a domain administrator. Copy the local profile you created in step 1 to the .V2 folder created in step 5. Be sure to use the CopyProfile tool—do not do this manually, or it won't work. Set the permissions for the profile to be a group of users you would like to use the mandatory profile (a domain TS users group or domain users, for example).
7. After the profile is copied successfully, locate the NTUSER.DAT file in the .V2 folder in the mandatory profile share and rename it to NTUSER.MAN.

Creating a Safe Read-Only Desktop

One curious side effect to not being able to save anything to a mandatory profile is that any folders remaining in the profile (that is, not redirected) will not save changes either. For example, if you do not redirect the Desktop folder and if users save files to their desktops, those files will be discarded when they log off. There won't be any error and the file will be on the desktop during the session, but the files won't be there when the users log on again. To put it mildly, this could be confusing. However, if you're using TS Remote Apps, you don't really want people saving files to the Desktop, because not being able to see the Desktop will make those files hard to find.

To keep the Desktop read-only but make sure people know it is read-only, redirect the Desktop to a folder as described in the section titled "Centralizing Personal Folders with Folder Redirection" earlier in this chapter and make sure this folder is read-only. This will both prevent users from saving files to the Desktop (which you want) and alert them to the fact that they can't save files to the Desktop (which you also want). If they try, they will get an error. They still can't save anything to the Desktop, but at least they will *know* they can't.

Profile and Folder Redirection Troubleshooting Tips

Many people find the combination of terminal servers and profiles daunting. And it's true—things don't always work the way you expect them to. Table 4-7 describes some common errors, possible solutions, and the sections in the chapter where we discuss how to fix each problem.

TABLE 4-7 Profiles and Folder Redirection Troubleshooting Tips

Problem	Solution	Additional Information in This Chapter
Policies appear to be set correctly, but aren't being applied.	Force policy update via gpupdate or rebooting.	See the sidebar "Using gpupdate /force."
Folders are not being redirected to the proper location or roaming profiles are not being loaded.	Check event logs to make sure that share is available on the network and has appropriate permissions.	See "The Consequences of Deleting a Profile Folder from Explorer" and "Centralizing Personal Folders with Folder Redirection."
Group Policy settings aren't being applied to the right computers, groups, or users.	Check the security filters and make sure you've included the correct groups.	See "Fine-Tuning GPOs with Security Filtering."
Folders from downlevel profiles aren't redirecting properly, but Windows Vista profile folders are redirecting.	Make sure you've enabled downlevel folder redirection for that GPO.	See "Sharing Folders Between Windows Server 2003 and Windows Server 2008 Roaming Profiles."
Users cannot load their roaming profile when they log on and see a message that they will be logged on with a temporary profile.	You may have deleted the cached profile manually using Windows Explorer. Delete the old registry keys and use tools such as the profile management utility or delprof to delete profiles.	See "Removing Cached User Profiles on Terminal Servers."

Summary

Although roaming profiles (read-write or read-only) are the best model for storing user profiles in a terminal server environment, the complications involved in making them work well can be daunting. This chapter has explained how profiles work, including how the User Profile Service loads and saves configuration data. We've talked about best practices, including how to keep profiles manageable in size to speed user logons and how folder redirection and profile caching contribute to faster logons. We've explained how to set up Group Policy to enable automatic profile creation according to best practices and how to use security filtering and loopback policy processing to ensure that the policies are applied correctly to a terminal server environment. Finally, we've explained how to set up and use mandatory profiles with a terminal server environment and how to prevent users from losing files when using mandatory profiles.

Key points:

- Roaming profiles combined with folder redirection is generally the best way to store user data in TS environments. Folder redirection is very important for keeping logon times short and profile sizes small.
- Profiles don't merge, they overwrite. For best results, have open only one copy of the user profile at a time. For this reason, you should generally not use the same roaming profile for both local logons and terminal server logons.
- Implementing Group Policy correctly from the beginning is key to making roaming profiles work.
- Folder redirection is key to making profiles work properly.
  - Folder redirection keeps profiles small.
  - Using folder redirection, you can share folders between two profiles for better integration of the local and remote user experiences.
  - If using mandatory profiles, you must use folder redirection to allow users to save files to any of their normal document storage locations (e.g., Documents, Favorites, etc.).

Additional Resources

The following resources will extend your knowledge of topics addressed in this chapter. All links are available to you on this book's companion CD.

- For more information on user profile management (with or without Terminal Services), read the following:
  - "Managing Roaming User Data Deployment Guide," available online at *http://technet2.microsoft.com/WindowsVista/f/?en/library/fb3681b2-da39-4944-93ad-dd3b6e8ca4dc1033.mspx* and for download from *http://technet2.microsoft.com/WindowsVista/en/library/fb3681b2-da39-4944-93ad-dd3b6e8ca4dc1033.mspx?mfr=true*.
  - "Using User Profiles in Windows Server 2003," located at *http://technet2.microsoft.com/windowsserver/en/library/23ee2a30-5883-4ffa-b4cf-4cfff3ff8cb71033.mspx?mfr=true*.
- For more information about how to configure device redirection and how to lock down the server, see Chapter 5, "Fine-Tuning the Terminal Server Runtime Experience."
- For more information about application installation and publishing through TS RemoteApps and TS Web Access, see Chapter 6, "Installing and Publishing Applications."
- For more information about enabling terminal server farms with TS Session Broker and multi-server management, see Chapter 8, "Managing the Terminal Server Runtime Environment."
- For more information about how to enable secure access to the terminal server from inside the network—and from outside using TS Gateway—see Chapter 9, "Terminal Services Ecosystem Management."
- For more information about customizing the default profile (so that terminal server user profiles are customized upon creation), see *http://support.microsoft.com/kb/325364*.