realtimepublishers.com™

The Definitive Guide™ To

Windows Desktop Administration

SCRIPTLOGIC

Bob Kelly

Copyright Statement

Chapter 3: User Profile and Data Management

In the last chapter, we covered the deployment of new systems. With your baseline identified, tested, and deployed, the real challenge of desktop administration comes into play—satisfying your users. Your goal in this area is clear: provide your users with the software they need as well as helpful default settings to ease its use. If a user has to search for an application, configure the application, search for his or her data, then work to identify and install the nearest printer, they will not be productive (or happy) users. Even when users are fairly experienced in the use of Windows, searching for documents and printers can be a real headache. A well-implemented desktop can save users from these speed bumps, reduce Help desk calls, and increase user productivity. In this chapter, we will cover user profiles and various ways you can implement and control them (for an overview, see the sidebar "Group Policy, Scripting, and Third-Party Solutions"). We will also discuss what might be considered the most critical aspect of desktop administration—user data management.

Group Policy, Scripting, and Third-Party Solutions

Many of the issues covered with regard to desktop administration lend themselves to one of three primary solutions: Group Policy, scripting, and third-party solutions. Group Policy provides a specific set of solutions to certain problems; where appropriate, I've pointed out these capabilities throughout this chapter. Group Policy is popular with its users; however, as a result of Group Policy's strict requirements, a great many organizations can't take advantage of the benefits of this desktop administration solution. Group Policy requires AD, and its managed clients must be running Win2K or later—thus, Windows 9x, Windows ME, and other clients are out of luck in terms of using Group Policy.

Even if you use Group Policy on your network, this solution can't do it all. In environments in which you need to address specific requirements (for example, your network has legacy desktops), scripting is often the tool that will get the job done. In Chapter 7, we will explore how you can script solutions to several desktop administration issues.

Finally, if scripting isn't within your skill set or your needs are robust enough to demand a supported, documented, and evolving solution, third-party software is the choice for you. Although scripting your own solution is a viable option in many situations, developing and maintaining a very large and complex script can be expensive. In such cases, a third-party solution makes sense.

The problems you face will often direct you to the most reasonable solution for your scenario. My point is to show you that you have desktop administration solution options. Depending on the size and complexity of your network (and the complexity of the problems that you are sure to face as a result), it often makes sense to employ a combination of Group Policy, scripting, and third-party solutions to address all of your needs.

User Profiles

Many settings affect the entire system (and all who use it). For this reason, NT and later versions of Windows provide default security settings that restrict users with non-administrative permissions from modifying such items as system time, display resolution, and software installation, to name a few. (For information about Windows 9x support for user profiles, see the sidebar "Windows 9x Support for User Profiles.") Conversely, there are many settings that are user-specific, such as printer and drive mappings, software settings, desktop colors, shortcuts, and wallpaper. These types of items are stored in an area separate from those that users don't have permissions to change, and the user is given full control over these settings, which are referred to as the *user profile*. The user profile is made up of a directory structure identified with the root folder name of the user to which the profile belongs. This root folder also contains a file named User.dat or Ntuser.dat, which contains the HKEY_CURRENT_USER registry hive used to store settings specific to the user (see Figure 3.1). There are many ways to configure, modify, and even force settings within a user profile.

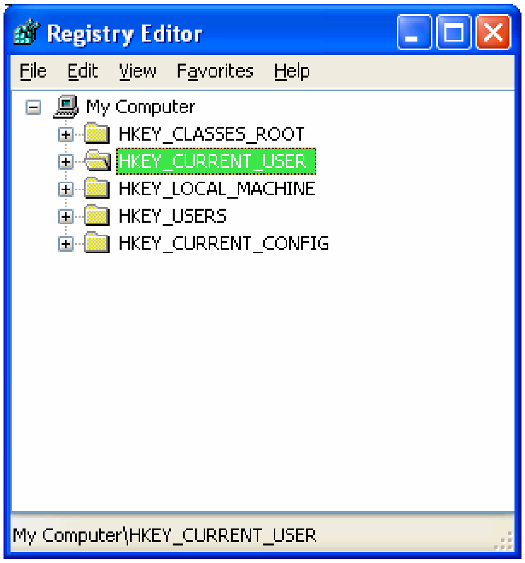


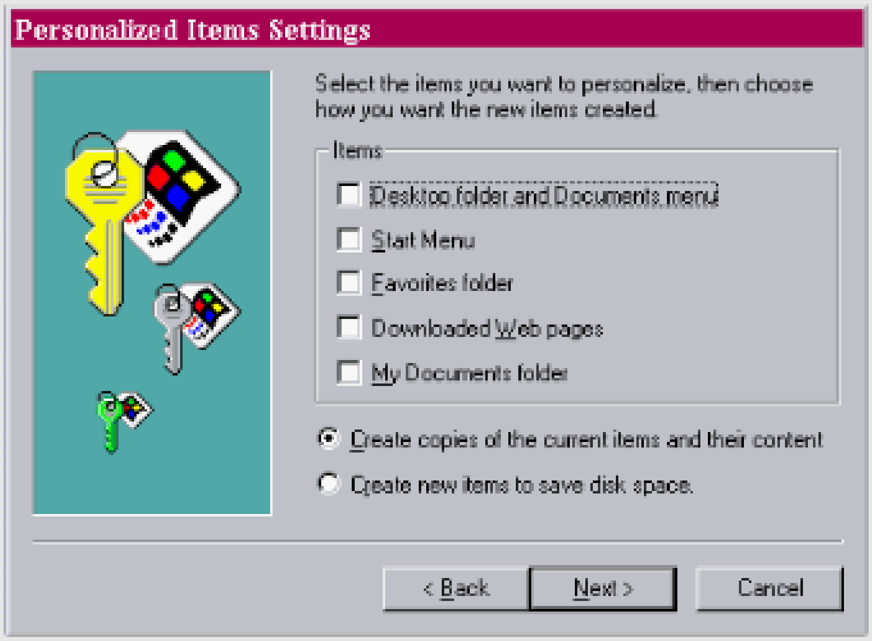
Figure 3.1: The user profile registry settings are loaded as HKEY_CURRENT_USER.

Profiles provide the ability for multiple users to work on the same computer. When each user logs on, the user has the same desktop settings as were available the last time the user logged off. Another key benefit is that customizations made to the desktop environment affect only that of the current user and not the environment of other users that might share the same computer. By implementing roaming profiles, such settings and data can be stored on a server from which it can be backed up and made available to users anywhere on the network.

Windows 9x Support for User Profiles

Although NT and later versions of Windows provide automatic support for user profiles, including the capability of restricting access to them, Windows 9x provides limited support. In Windows 9x, roaming profiles are stored in the user's home directory (as specified in the user's user profile) as opposed to the user's "profile" directory. Because file security is not a feature of these versions of Windows, no restrictions for accessing profiles exist locally. Additionally, you can configure Windows 9x to copy only shortcut (.lnk) and program information (.pif) files in the user profile.

To enable roaming profiles on Windows 9x systems, you must configure Windows 9x to make use of user profiles via the Control Panel's Passwords applet. Further, you may customize what is included in a Windows 9x profile by clicking the Change Settings button in the Users Control Panel applet (see Figure 3.2).



Select the items you want to personalize, then choose how you want the new items created.

Items

□ Desktop folder and Documents menu
□ Start Menu
□ Favorites folder
□ Downloaded Web pages
□ My Documents folder

● Create copies of the current items and their content
○ Create new items to save disk space.

Figure 3.2: Windows 95 personalized settings wizard.

When logging on to a Windows 9x computer, the user profile is copied from the user's home directory to the local machine (or the user is prompted to create a new profile if none exists). When logging off, the user profile is then copied back to the user's home directory. The home directory is set in the user's account profile on the server. This path must be in the Universal Naming Convention (UNC) format (\\*server name**share name*) and must be created beforehand. In addition, Windows 9x offers no support for a centrally stored default user profile and no support for common groups. Also, Windows 9x supports different files for the registry portion of user profiles. The User.dat file in Windows 9x is not interchangeable with the Ntuser.dat file found in NT later user profiles.

As a means of profile recovery, Windows 95 uses a file named User.da0 and NT 4.0 uses a file named Ntuser.dat.log. Although these files are similar, they provide slightly different functionality. Windows 95 writes a copy of User.dat to User.da0 each time the user logs off as a simple backup copy. NT uses the Ntuser.dat.log file as a transaction log file, which allows for fault tolerance in the event that a user profile must be recovered.

📖 See “Using Profiles with Multiple Versions of Windows” at the end of this chapter for information about the use of roaming profiles when logging onto multiple versions of Windows.

Windows provides four types of user profiles: local, roaming, mandatory, and temporary. In the following sections, we will discuss the purpose of each as well as considerations for local and roaming profiles to help you identify which implementation makes the most sense in your environment.

Local Profiles

The first time a user logs on to an NT or later system, a local profile is created and stored locally based on the default user profile (discussed later in this section). Changes made by the user are saved and subsequent logons will make use of this same user profile (if it exists). Table 3.1 provides the default locations for user profiles.

Windows Version	**Default Location**
Windows 95	\Windows\Profiles\username
Windows 98	\Windows\Profiles\username
Windows NT	\WinNT\Profiles\username
Windows ME	\Windows\Profiles\username
Windows 2000 * (English Language)**	\Documents and Settings\username
Windows XP * (English Language)**	\Documents and Settings\username

* If the installation is an upgrade from NT, user profile folders are stored in the same location as in NT.

** The localized base profile path can be determined by reading the registry

Table 3.1: User profile locations by Windows version.

Where a roaming profile is not found, local profiles are created and stored on each computer a user logs onto. The settings remain for use next time the same user logs on. To have the same settings available to users logging onto multiple systems, you must implement roaming profiles.

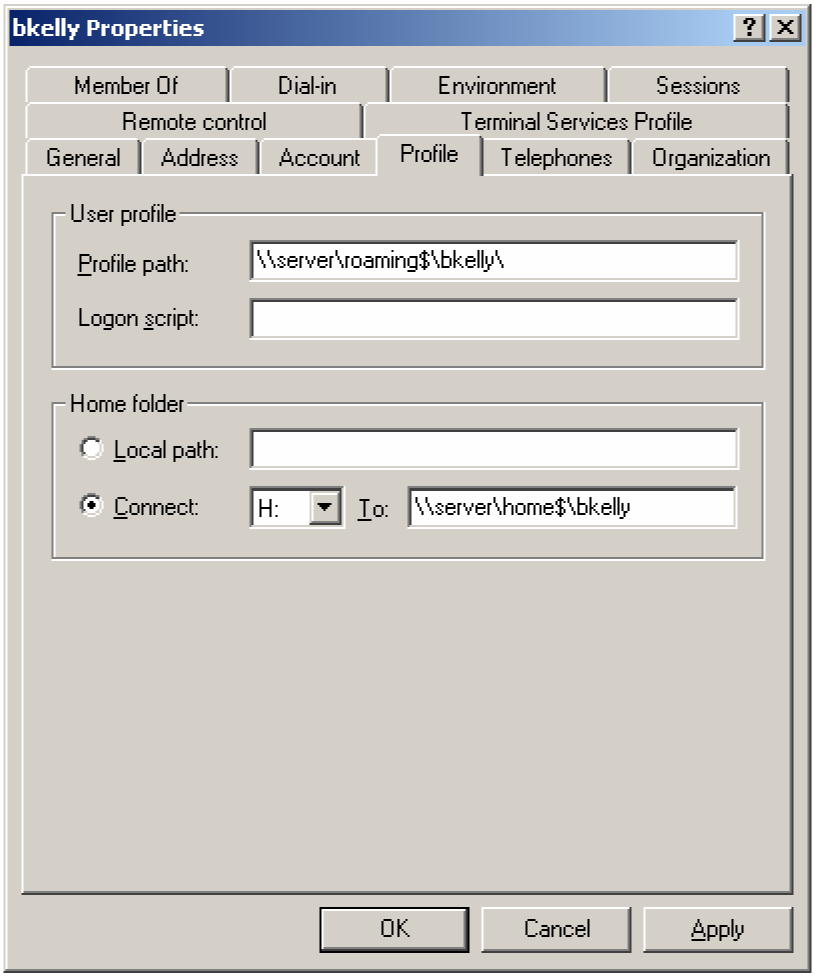
Roaming Profiles

Roaming profiles are copied down from the server (to the location as indicated in Table 3.1). When a user who is using a roaming profile logs off, the profile is copied back up to a specified share on the network.

The copying of the local profile to the network is determined by the file and object timestamps. Any files or objects in the local copy of the profile that have a different timestamp from the corresponding file on the network are copied back to the target profile server location. At a minimum, the Ntuser.dat and Ntuser.ini files are copied up to the server because the act of logging on and off the system will cause modification (and therefore a timestamp update) of these files.

The following steps walk you through the procedure for managing users on a Win2K server. NT provides very similar functionality as it pertains to configuring roaming profiles through its User Manager for Domains utility.

1. Set up and share a folder on a server.
2. Open the Active Directory Users and Computers snap-in, and navigate to the container in which the user account exists.
3. Right-click the user's name, and select Properties.
4. Select the Profile tab (see Figure 3.3).
5. For the profile path, input the path to the network share where the user profiles will be stored (for example, \\ServerName\ShareName\UserName).



User profile

Profile path: \\server\roaming$\bkelly\

Logon script:

Home folder

○ Local path:

● Connect: H: To: \\server\home$\bkelly

Figure 3.3: The Profile tab in Win2K Active Directory Users and Computers.

To create the roaming profile share, create and share a folder as the root folder for storing user profiles. Append a dollar sign ($) to the share name if you would like it hidden from users browsing the network (\\server/roaming$). Set the NTFS and Share level security to allow all users access to the share (the default security will be to allow full control to the Everyone group). In the user profile, enter the share path using the local path to the share and entering the username as the folder (for example, \\server\roaming$\bkelly). The roaming user profile directory will be created when the user first logs onto the domain (as opposed to user home directories, which are created at the time they are specified).

✎ The profile share can be stored on any system. The process of downloading the profile is controlled by the client computer—all the client needs is the correct path. However, it is strongly recommended that you use a server as opposed to a workstation for this purpose. One big reason is that NT Workstation, Win2K Professional, and Windows XP all have a limitation of 10 inbound network connections. However you may use a network attached storage (NAS) device or UNIX server share.

☞ You should not specify the same location for the user's profile and home directory. If you do so, all files that the user stores in his or her home directory will be copied up and down from the server in the profile copy process. If you want to use the same share, specify the roaming profile (as opposed to the root of the share) as a subdirectory in the user's home share to avoid this situation.

When logged onto more than one system at a time, it is the system you last log off of that will dictate the contents of your roaming profile. To demonstrate this idea, the following steps walk you through an example scenario. In addition, Figure 3.4 helps to illustrate the situation.

1. On COMPUTER1, you install software while logged onto both COMPUTER1 and COMPUTER2. This software installs required registry keys in your profile (such as licensing information).
2. You log off of COMPUTER1, and your profile information is copied to the server as expected.
3. You now log off of COMPUTER2, the registry entries and other profile changes that might have been made during the software installation on COMPUTER1 are lost when COMPUTER2 copies its version of the user profile over the profile copied up by COMPUTER1.
4. You log onto COMPUTER1, and the copy of your profile that does not know about the software installation is copied down to the local machine.

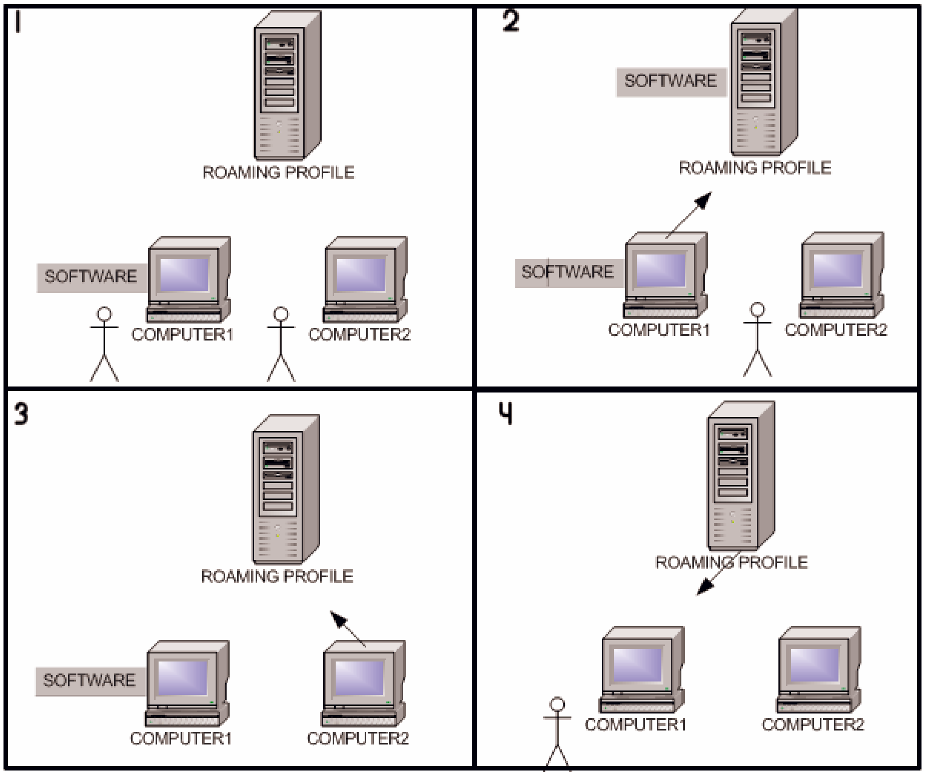


Figure 3.4: Multiple logons and roaming profiles can be a troublesome combination.

Additionally, roaming profiles do not work well over slow network links. In fact, Microsoft does not recommend using roaming profiles across a slow network link at all. Aside from extending logon and logoff periods, the risk of unsynchronized profiles increases.

One example of how slow network links can be trouble for roaming profiles occurs when a user logs on via a network connection that is slow enough to cause Windows to time out during the logon process. Windows instead uses the local profile (if the user doesn't have a local profile, one is created using the default user profile). If the remote server becomes available when the session ends, Windows will copy the local profile up over the roaming profile on the server.

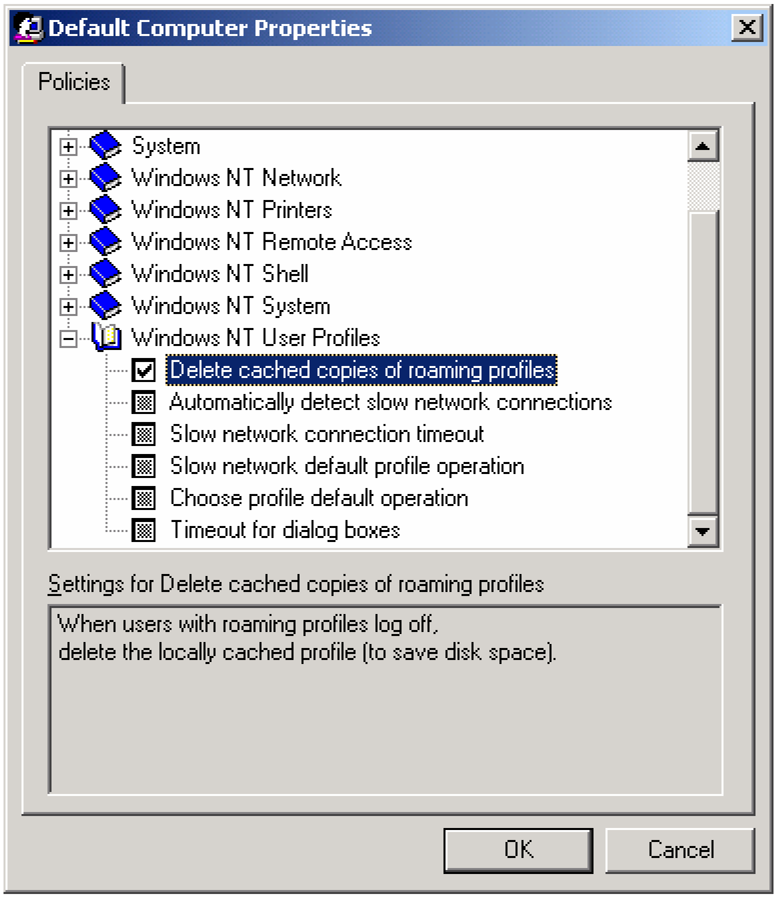
☞ NT and earlier versions of Windows detect slow links by measuring the time it takes the server to respond to a request for the file attributes of the profile. This action is timed and compared with the value determining a slow network.

Win2K and Windows XP determine whether there is a slow link by measuring the response time from a sequence of TCP/IP pings from the client computer to the server to determine the average transfer rate in kilobits per second. If the response time from any of the pings is less than 10 milliseconds, the link is not considered to be a slow one. Otherwise, the average transfer rate is calculated from three ping requests to the server with 2048 bytes of data. If this calculated average transfer rate is slower than the default (2000 milliseconds) or a value defined by the administrator, the connection is considered slow. The formula used in Win2K is

link speed=16000/(average ping for 2048 byte packet)

Roaming user profiles are not required to be stored on a server on which TCP/IP is an installed protocol. This method of pinging the server is attempted, and if the server is identified as not supporting the TCP/IP network protocol, it uses the method used by NT 4.0 and earlier versions.

By default, roaming profiles are stored on the system and remain until used again or manually deleted. You can, however, set policies to have roaming profiles removed from workstations if you desire using System Policies for NT and earlier (see Figure 3.5) or Group Policy for Win2K and later.



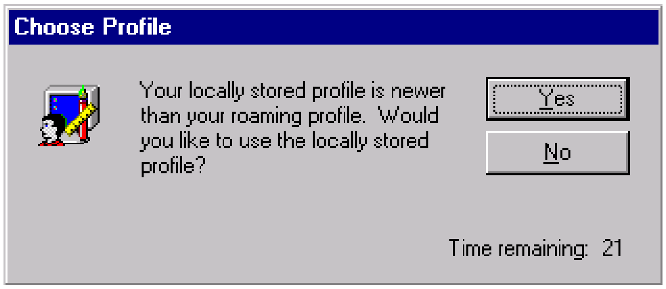
- System
- Windows NT Network
- Windows NT Printers
- Windows NT Remote Access
- Windows NT Shell
- Windows NT System
- Windows NT User Profiles
  - ☑ Delete cached copies of roaming profiles
  - ▨ Automatically detect slow network connections
  - ▨ Slow network connection timeout
  - ▨ Slow network default profile operation
  - ▨ Choose profile default operation
  - ▨ Timeout for dialog boxes

Settings for Delete cached copies of roaming profiles

When users with roaming profiles log off,
delete the locally cached profile (to save disk space).

Figure 3.5: The System Policy value for deleting roaming profiles.

When the copy of the user profile on the local system is newer than the one on the network, the user is presented with a choice of which to use, as Figure 3.6 shows.



Your locally stored profile is newer than your roaming profile. Would you like to use the locally stored profile?

Time remaining: 21

Figure 3.6: Choice presented by Windows when the network profile is newer than the local profile.

By default, this dialog box is presented for 30 seconds and the default selection is made automatically. This choice can be confusing to users, and it is common for them to select the default option (which differs among the Windows versions) or panic long enough that the default option is selected for them. For NT, the default is to download the network profile; for Win2K and later, the default is to use the local copy. To specify your desired default, add or modify the following registry value:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	SlowLinkProfileDefault
Type	REG_DWORD
Data	0 or 1 (1 = Download Profile, 2 = Use Local Profile)

You can edit the registry or use System Policy to exclude desired directories from being included in a user's roaming profile. This capability was introduced with NT Service Pack 4 (SP4). To use the registry edit method, add or modify the following registry value:

Key	HKEY_CURRENT_USER\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
Value	`ExcludeProfilDirs`
Type	REG_SZ
Data	Directories to exclude, using relative paths from the user profile root separated by semicolons
Sample Data	`Temporary Internet Files;Application Data\Microsoft\Outlook`

To use System Policy to exclude directories from a user's roaming profile, follow these steps:

1. In System Policy Editor, load the templates Common.adm and Winnt.adm (usually found in the hidden c:\winnt\inf folder).
2. Create a new policy.
3. Open Default User, then expand Windows NT User Profiles.
4. Select the *Exclude directories in roaming profile* option.
5. In the text box provided, enter the directory names you want to exclude. Again, the directories must be relative to the root of the user's profile and semicolons must be used to separate multiple entries (the default value is Temporary Internet Files;Temp).

Mandatory User Profiles

Mandatory user profiles are roaming profiles that can be used to specify particular settings for individuals or an entire group of users. Only systems administrators can make changes to mandatory user profiles. A mandatory user profile will not save changes made to the desktop by users during their logon sessions. Users can modify the desktop settings of the computer while they are logged on, but none of these changes are saved when they log off. The mandatory profile settings are downloaded to the local computer each time a user logs on. You can designate any profile as a mandatory profile simply by renaming Ntuser.dat as Ntuser.man in the root of the desired roaming user profile directory. Win2K provides support for mandatory profiles in this way, but in environments in which AD has been implemented, it is recommended that Group Policy be used to provide a layered, and more granular, control of user profiles.

> ✎ Although mandatory profiles are supported for Windows 9x clients, mandatory profiles cannot be shared. You must create a separate profile for each user.

Temporary User Profiles

Available only on computers running Win2K and later, a temporary profile is issued any time an error condition prevents a user's profile from being loaded. Temporary profiles are deleted at the end of each session. Changes made by the user to his or her desktop settings and files are lost when the user logs off. When a temporary profile is to be used, users are presented with a message during logon that advises them of this condition.

Profile Security

Local access to profile directories is restricted on NT and later versions of Windows where NTFS is in use. On NT computers, profile directories are created with the user account, local system account, and administrator's group having full control.

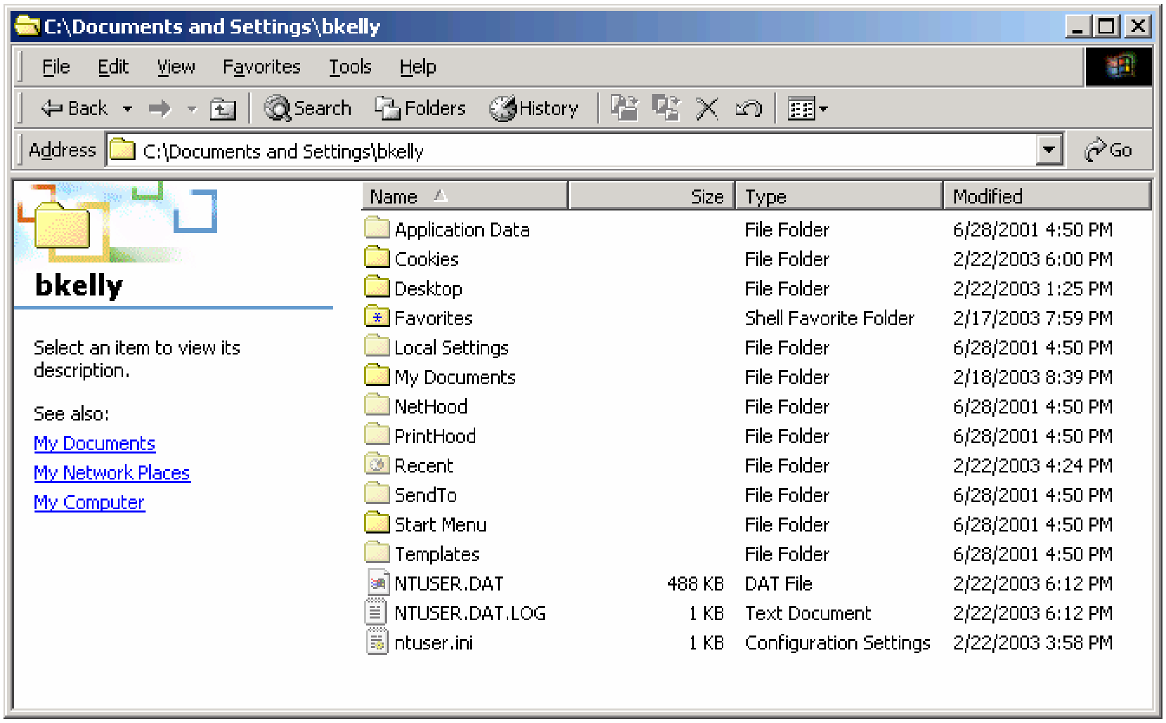
Directories containing roaming user profiles need at least add and read permissions for profiles to be read correctly. Because Windows looks for the existence of the folder first, having only add permissions will result in failure. For a roaming profile to be written back up to the server, the user must have at least change permissions. If a profile is mandatory, the user account must have at least read permissions on the network share on which the user profile is stored.

Contents of a User Profile

Several standard directories are included in a user profile, many of which are hidden. The following list provides the makeup of the settings and default directories included for a Win2K system (see Figure 3.7):

- Application settings—All user-specific application settings installed or generated by the user
- Windows Explorer file settings—All user-definable settings for Windows file explorer as well as persistent network connections
- Program groups and taskbar settings—All personal program groups and their properties, all program items and their properties, and all taskbar settings

- Printer settings—All network printer connections
- Control Panel settings—All user-defined settings made in the Control Panel
- Help bookmarks—Any bookmarks placed in the NT Help system
- Application data directory—Application-specific data, such as a custom dictionary for a word processing program; application vendors decide which data to store in this directory
- Desktop directory—Desktop items, including files and shortcuts
- Cookies—Internet Explorer (IE) cookies
- Local Settings—Application settings that do not roam with the profile; usually these settings are computer specific or are too large to roam effectively; the following subfolders are present by default: Application Data, History, Temp, and Temporary Internet Files
- Favorites directory —Shortcuts to program items and favorite locations
- NetHood directory—Shortcuts to Network Neighborhood items (hidden)
- My Documents directory—User data directory
- PrintHood directory—Shortcuts to printer folder items (hidden)
- Recent directory—Shortcuts to the most recently used items
- SendTo directory—Shortcuts to document storage locations and applications
- Start menu directory—Shortcuts to program items
- Templates—Shortcuts to template items (hidden)



Address: C:\Documents and Settings\bkelly

Select an item to view its description.

Name	Size	Type	Modified
Application Data		File Folder	6/28/2001 4:50 PM
Cookies		File Folder	2/22/2003 6:00 PM
Desktop		File Folder	2/22/2003 1:25 PM
Favorites		Shell Favorite Folder	2/17/2003 7:59 PM
Local Settings		File Folder	6/28/2001 4:50 PM
My Documents		File Folder	2/18/2003 8:39 PM
NetHood		File Folder	6/28/2001 4:50 PM
PrintHood		File Folder	6/28/2001 4:50 PM
Recent		File Folder	2/22/2003 4:24 PM
SendTo		File Folder	6/28/2001 4:50 PM
Start Menu		File Folder	6/28/2001 4:50 PM
Templates		File Folder	6/28/2001 4:50 PM
NTUSER.DAT	488 KB	DAT File	2/22/2003 6:12 PM
NTUSER.DAT.LOG	1 KB	Text Document	2/22/2003 6:12 PM
ntuser.ini	1 KB	Configuration Settings	2/22/2003 3:58 PM

Figure 3.7: Root directory view of a user profile.

User Profile Storage

There are situations in which duplicate profiles names are avoided by the system. For example, when a user named bkelly first logs onto the computer, a standard profile directory structure is created:

```
Documents and Settings/bkelly
```

On NT systems, a different user logging on with the same name would have a unique profile path created by appending a three-digit number to the UserID, starting with 000 and incrementing each additional time another duplicate name with a different user SID logs onto the computer:

```
Documents and Settings/bkelly.000
Documents and Settings/bkelly.001
```

On Win2K and later systems, when a second account with the same name logs on, the account domain name is appended to make it unique:

```
Documents and Settings/bkelly.APPDEPLOY
```

On Win2K and later systems, in situations in which further duplication might occur, a number is appended that increments each time the situation occurs:

```
C:\Documents and Settings\bkelly.APPDEPLOY.000
C:\Documents and Settings\bkelly.APPDEPLOY.001
```

NT 4.0 records which profile should be used by which user by placing registry keys for the user's security ID (SID) in the registry in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. Each user who has logged on to the local machine will have a SID recorded here in its own subkey with a value that contains the path to that user's local profile (ProfileImagePath). Should multiple users with the same account name log on to the network, separate distinct profiles are created for each.

Profiles Templates

When manually creating user accounts, you might choose to create and use multiple default user profiles that cater to the software and tasks appropriate for individual users or groups of users. Using this method, you might apply a tailored default user profile to users in order to provide them with a more customized starting point:

1. Create a new user account that will be used as a template for the preconfigured user profile.
2. Log on as the new user, then customize the desktop and install applications to configure this user's profile for the user profile template.
3. Log off, then log on as the Administrator.
4. Open the System applet in Control Panel.
5. On the Advanced tab, under User Profiles, click Settings.
6. Under *Profiles stored on this computer*, select the user that you created in step 1, click Copy To, and enter the path specified for the user's roaming profile.
7. In the Copy To dialog box under *Permitted to use*, click Change, and in the Select User or Group dialog box, select the user to whom you are assigning the profile.

Default Profiles

The default user profile is used as the starting point for new user profiles that are generated when a local or roaming profile is not available for a user logging onto the computer. To create a custom default user profile, follow these steps:

1. Log on to the system as Local Administrator, and create a new local user account.
2. For NT, use User Manager and for Win2K and later systems, right-click My Computer and select Manage, to start the Microsoft Management Console (MMC) snap-in that allows local user account creation.
3. Log off of the computer, and log on again using the newly created local user account.
4. Customize the system as you want default users configured.
5. Log off of the system when customization is complete, then log on again as the Local Administrator.
6. From the Control Panel, launch the System applet.
7. On the Advanced tab under User Profiles, click Settings (for NT, select the User Profiles tab), click the user profile that you just created, then click Copy To. In the Copy To dialog box, specify the location as <*local user profile path*>\Default User to create a custom local user profile or choose your network replication folder to create a network default user profile.
8. Under *Permitted to use*, click Change, and select Everyone. Finally, click OK to complete the process.

✐ If you want a domain-wide default profile, enter the path to NETLOGON\Default User on the domain controller. Doing so creates the default user profile for the domain. To create a network default user profile, specify the replication directory (the Netlogon share is a read-only share). For Active Directory (AD) environments, choose the share location from SYSVOL. In either case, the profile should be saved as Default User.

☞ Need to open System from a command line as an administrator? On Win2K and later, don't log off—instead type

```
runas/user:computername\Administrator"rundll32.exeshell32.dll,Control_RunDLLsysdm.cpl"
```

Keep in mind that you cannot copy or delete a user profile that belongs to the currently logged on user or any user whose profile is in use.

You can store the default user profile in either the Netlogon share of domain controllers or locally on each system. It is common to utilize both, but understand the precedence taken to determine when each is used: when available, the network copy of the default user profile will be used and not the local copy. In fact, unless the network is unavailable or you are dealing with a user logging onto the computer locally (not the domain), the default user profile on the local machine might never be used. The following list describes the order used to determine which profile is employed for a user:

- Is there a central (roaming) profile defined in User Manager for Domains? If yes, any profile created locally will become a roaming profile (otherwise the profile will be created as a local profile).
- If yes, does the roaming profile exist? If yes, use the roaming profile.
- If no, does this user have a local profile? If yes, use local profile.
- If no, does Default User exist on the Netlogon share of the validating domain controller? If yes, use the network default user profile to generate a new user profile.
- If no, does Default User exist in the local profile directory? If yes, use the local default user profile to generate a new user profile.

Manual Profile Modifications

To manually customize a user profile, you can manipulate the file structure or registry hive locally or from a network stored roaming profile. Keep in mind that if you are manipulating a roaming profile, it might be overwritten locally when logging on or the network copy might be overwritten if the user then logs off. To edit a user's registry entries, load the user's registry hive file as a new subkey, as Figure 3.8 shows.

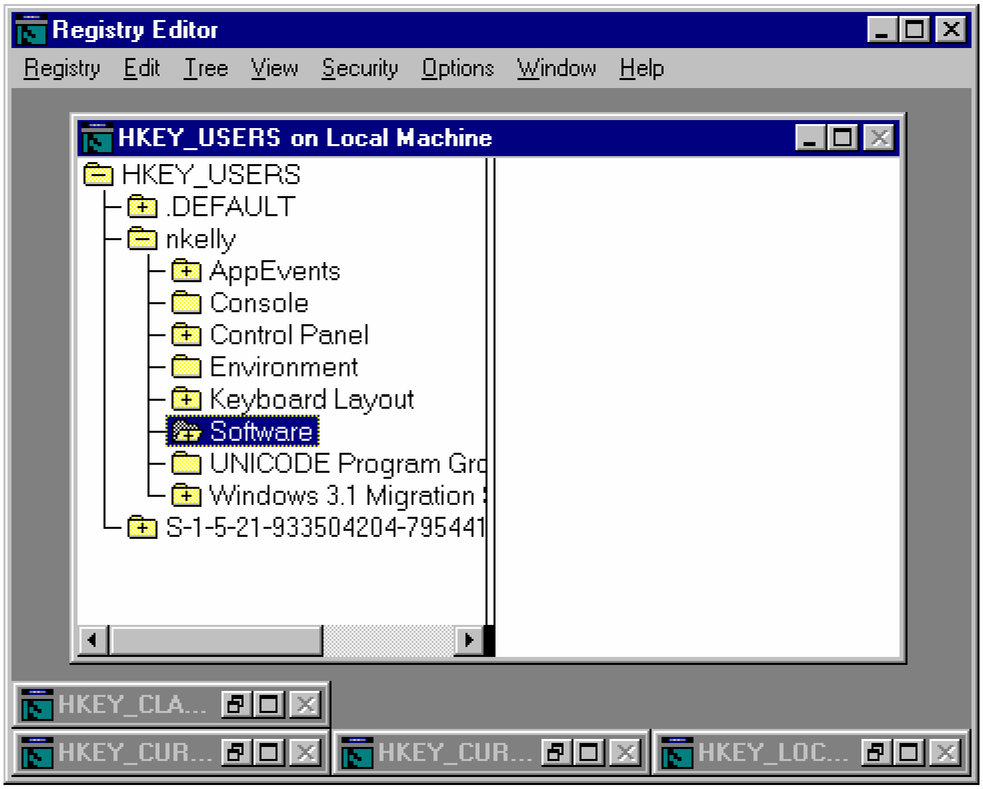


Figure 3.8: Loading another user profile as a new hive for manual editing.

1. Start regedt32.exe, and click on the root key of HKEY_USERS to highlight it.
2. From the Registry menu, select Load Hive.
3. Browse for the desired Ntuser.dat file to be manipulated.

4. A dialog box will prompt you to enter a key name. Enter the UserID to identify the profile being loaded, and click Enter.
5. Click Enter to add the profile registry hive as a subkey to HKEY_USERS, as Figure 3.8 shows (in this case, nkelly).
6. Edit the existing values as desired.
7. After completing the changes, highlight the root of the user's profile registry key, and from the Registry menu, select Unload Hive to save the changes to the user's profile.

Dictating Data Storage

Where do you want users storing their data? The answer to this question should be carefully considered. Once you decide, you need to determine how you'll enforce the storage policy—perhaps through written company policies or by denying users access to save to undesired locations. There are a handful of options that you can implement in several ways, as we will discuss in the following sections.

Network Share

Most environments prefer that user data be stored on a network share so that it might be easily backed up. You can create different shares to store data files by category or to share documents with other users in any specified group. Controlling who maps such drives and who should have access is often specified by group membership.

User Home Directory

You can specify the user home directory as a local directory or network share (see Figure 3.3). When a network share is specified, a drive letter to map the share to is also identified. During the logon process, the home drive is mapped to the designated drive letter.

The user home directory is created at the time it is specified in the user profile and its default security settings allow only the user assigned to the home directory to have access. Some administrators choose to create a separate share for each user; others choose to create a single share and include all user home directories within it. Either way, you can use file security to restrict unauthorized users from access.

> Having both a home directory and roaming profile set to the same path can result in all files in the home directory being deleted when a user logs off. However, it is acceptable to make the profile directory a subdirectory of the home directory (for example, \\Server\Share\UserHomeDirectory\Profile).

Single Share

For the single share method, create and share a folder as the root folder for storing user home directories. Append a dollar sign ($) to the share name if you would like it hidden from users browsing the network (\\server\homes$). Set the NTFS and Share level security to allow all users access to the share (the default security will be to allow full control to the Everyone group). In the user profile (see Figure 3.3 earlier in this chapter), enter the share path using the local path to the share and entering the username as the folder (for example, \\server\roaming$\bkelly). The home directory will be created at the time it is specified here.

On Win2K and later systems, you can use *deep mapping* support, which allows for drives to be mapped to a directory within a share. Particularly when dealing with user profiles, deep mapping is a very helpful feature. By mapping to, for example, \\server\roaming$\bkelly, a user sees his or her data directly within the user's mapped home drive. On NT and earlier clients, mapping directly to a subdirectory (*deep mapping*) is not supported. In this case, you could map to \\server\roaming$, for example, and the user would need to open the directory identified by his or her user name. Though security restrictions will keep users from accessing each other's home directories, in an environment with many users, digging for the proper folder can easily become a hassle. The alternative is to create a share for each user, as the next section details.

Individual User Shares

To use individual shares for each user, create a folder to hold all user home directories, then create subdirectories for each user. This step is typically done using the user name as the name of the folder for the corresponding user (for example D:\Homes\bkelly). Share each user folder and modify the default permissions to remove the Everyone group, then add the user account for whom the share is being created with Change permissions. Specify this location as the user profile directory in the Active Directory Users and Computers MMC snap-in.

> ☞ When the creation of a great number of home directories is on your task list, writing a script to do the job can be a real time saver. For a simple approach to automating this process, see the Microsoft Article "Batch Process to Create and Grant Access to Home Directories."
>
> Don't want to script it? There are a couple of tools to help you get the job done including AutoShare from ScriptLogic (http://scriptlogic.com/eng/Products/Autoshare/main.asp) and UserManagemeNT from Advanced Toolware (http://www.advtoolware.com/t4e/general/um_default.htm).

User Profile

Too much data in a roaming profile can result in extended logon and logoff times as well as increases the likelihood of corruption or impatient users powering off their computers during the copy process. For these reasons, it is best to limit the size of the user profile through implementation of drive quotas (discussed later in this section). Unless you manage the default location for the system and its applications, the user profile might well be where data is stored. Additionally, many novice users do not understand the difference between a shortcut and a folder. As a result, it is not uncommon for a user to copy or move a folder to his or her desktop for the sake of convenience.

Local Data Directory

Probably as the result of some past experience or paranoia, many users typically like to have their data stored on their local systems. Of course, if their machines suffer a drive failure or are re-imaged, their data could be long gone. In a small environment, network backups of local systems or scheduled scripts to synchronize the data with a network copy might be a sufficient solution to this problem. For larger networks, it is often policy not to allow users to save locally, which might be further enforced by restricting write access to the local hard drive. Generally, allowing users to store data locally increases the risk of loss and might restrict your ability to replace or upgrade systems in the future.

Setting Default Paths

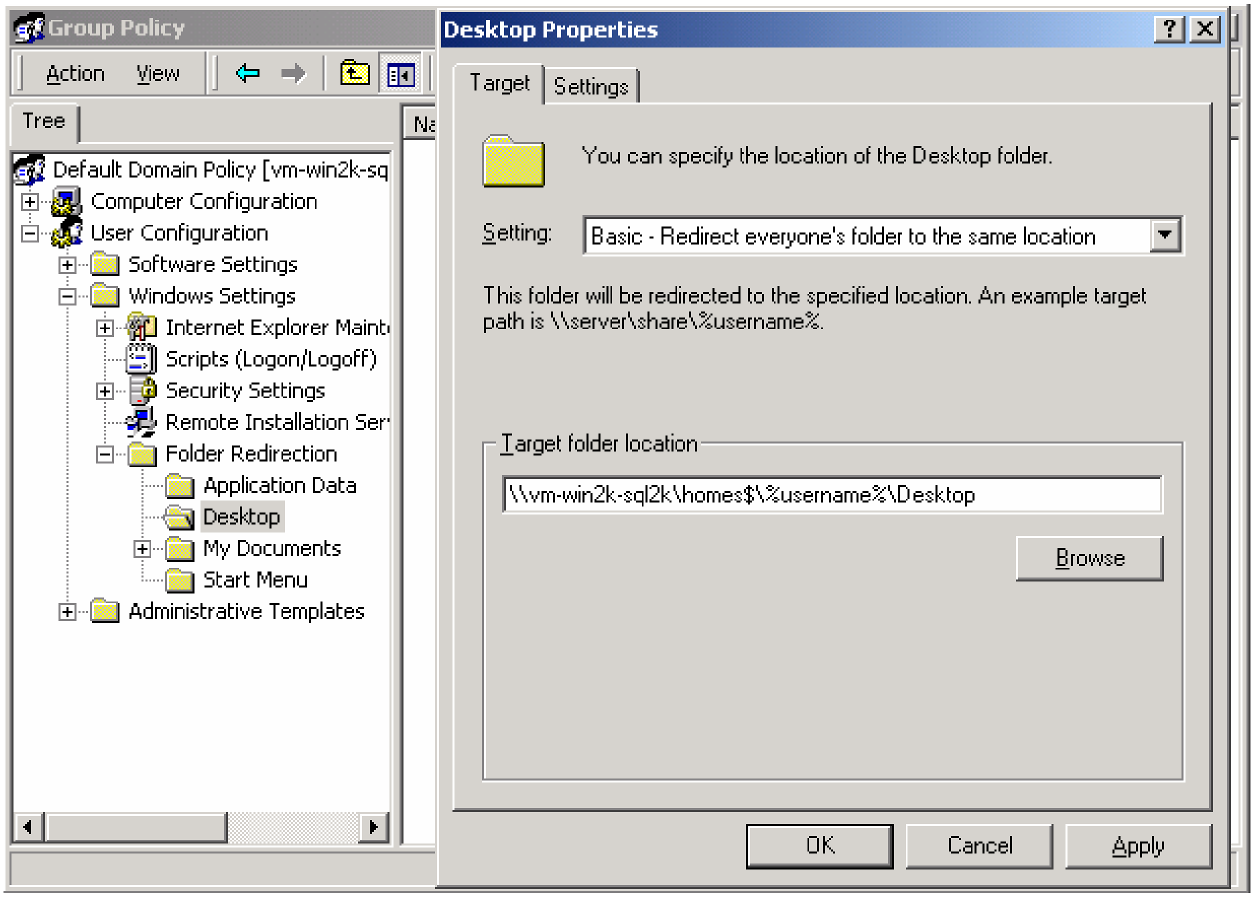
One common way to steer users away from storing data in their profiles is to specify desired locations as default for any deployed applications. Although Microsoft products are usually very good about documenting and providing settings for the location of templates and user data, not all applications are so friendly. You will need to examine each application used to generate user data in order to determine how (or if) you can specify the location of user data. As discussed, using the default user profile to configure these settings is often a means of providing a helpful starting point (this should include the setting of default paths). However, as applications are added and updated, managing this via the default user profile becomes less and less helpful over time (affecting only new users). You can further specify paths via registry edits using logon scripts or by using other tools designed to provide similar functionality. Remember, these are default paths—the users may browse to any location he or she has access to when saving data. Finally, you can use Group Policies and System Policies to enforce settings such as default data paths. Keep in mind that when setting paths using System Policy or Group Policy, the settings will be enforced at each logon, and therefore should only be used to *enforce* settings (not to provide defaults).

Folder Redirection

Folder redirection is a term used to describe the process of locating standard profile directories in alternative locations, typically a network share. Folder redirection can be used to significantly reduce the size of a user's roaming profile (avoiding long logon times and even corruption of data. Doing so can also be valuable in that you can trick applications and users by letting them work as they normally would, while the directories they are familiar with are actually located elsewhere. Group Policy provides the ability to implement folder redirection. You can also implement similar functionality by manually editing the registry.

> ✎ Ultimately, all folder redirection will end up being the result of the manipulation of particular registry values that inform the system where to find those folders. There are, therefore, several ways to achieve this result and manipulate these registry values (for example, manually, automatically via Group Policy, or automatically via a third-party solution). In the third-party solution category, utilities such as ScriptLogic (http://www.scriptlogic.com) and Enterprise Configuration Manager (ECM) from ConfigureSoft (http://www.configuresoft.com) include folder redirection in their arsenal of skills. In the freeware/shareware category, tools such as Multi-Remote Registry Change from Eytcheson (http://www.eytcheson.com) offer a solution for registry editing en masse (for links to additional registry editing tools, visit LabMice.net at http://www.labmice.net/Utilities/registrytools.htm).

For Win2K and later clients in an AD domain, you can utilize Group Policy to specify folders you want to have redirected. You can specify a single path for all users or common locations based on group membership. When specifying the same path for multiple users, you can use the %username% environment variable to personalize the path for each user, as Figure 3.9 shows.



You can specify the location of the Desktop folder.

Setting: Basic - Redirect everyone's folder to the same location

This folder will be redirected to the specified location. An example target path is \\server\share\%username%.

Target folder location

\\vm-win2k-sql2k\homes$\%username%\Desktop

Figure 3.9: Folder redirection properties for the desktop folder in a Group Policy Object (GPO).

If you specify a folder that doesn't exist, the system will create the folder when the user logs onto the network. It is customary to utilize folders in the user home directory for this purpose to increase the use of this managed location and to avoid storing user data in too many different locations.

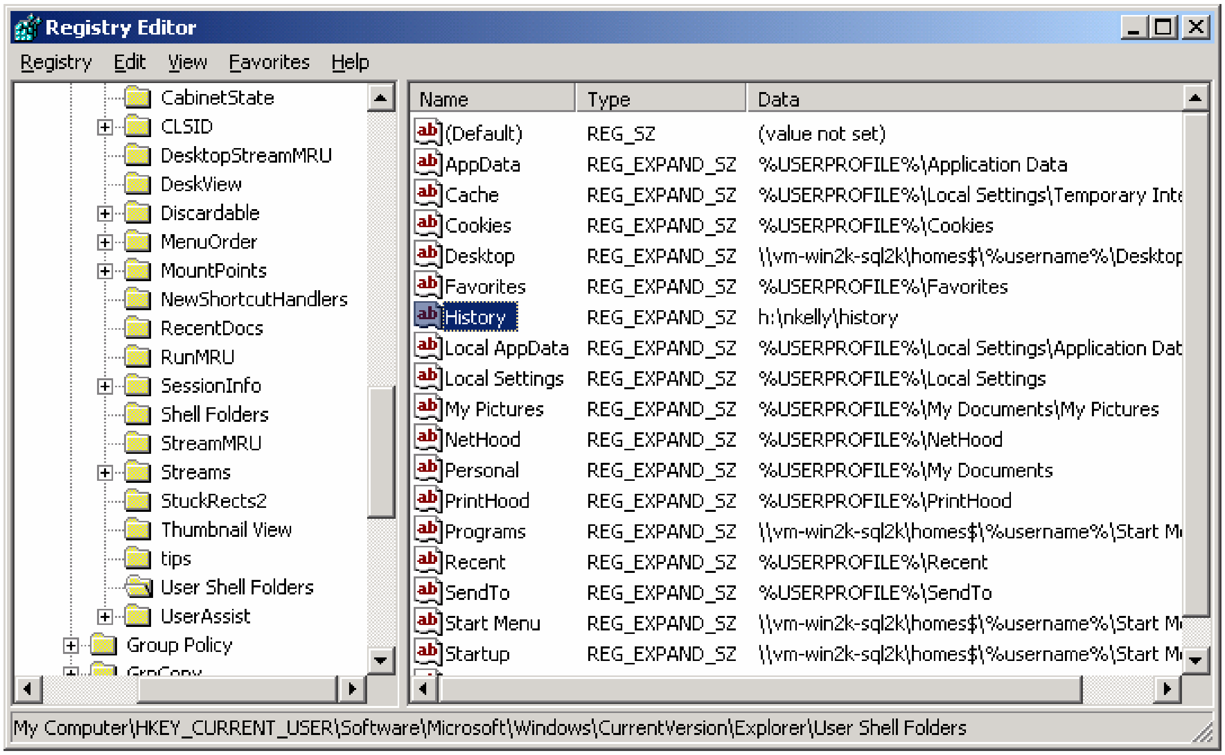
With the folder redirected, references made to the folder automatically interact with the redirected folder specified in Group Policy. For example, if the desktop folder is redirected (as in Figure 3.9), you will be able to see that any shortcuts created on the desktop are actually created in the redirected folder and not in the local user desktop folder. In fact, the local desktop folder normally found in the user profile will no longer be present.

The Start menu is another location that you might want to configure for folder redirection. For example, you might specify that all Domain Admins have their Start menus redirected to a common location where shortcuts to all administrative utilities are maintained.

Group Policies can only perform folder redirection on Win2K and Windows XP and later clients. For legacy clients such as Windows 9x and Windows ME desktops, you'll have to use a third-party tool or manually edit the registry to implement folder redirection.

Folder Redirection via Shell Folders

Alternatively, you can implement folder redirection by editing the *shell folder* registry entries. Even as far back as Windows 95, the location of several special folders (those normally located in the user profile) are identified in the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders. Even in an AD domain, you can use this method to specify redirected folders, as Figure 3.10 illustrates.



Name	Type	Data
(Default)	REG_SZ	(value not set)
AppData	REG_EXPAND_SZ	%USERPROFILE%\Application Data
Cache	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temporary Inte
Cookies	REG_EXPAND_SZ	%USERPROFILE%\Cookies
Desktop	REG_EXPAND_SZ	\\vm-win2k-sql2k\homes$\%username%\Desktop
Favorites	REG_EXPAND_SZ	%USERPROFILE%\Favorites
History	REG_EXPAND_SZ	h:\nkelly\history
Local AppData	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Application Dat
Local Settings	REG_EXPAND_SZ	%USERPROFILE%\Local Settings
My Pictures	REG_EXPAND_SZ	%USERPROFILE%\My Documents\My Pictures
NetHood	REG_EXPAND_SZ	%USERPROFILE%\NetHood
Personal	REG_EXPAND_SZ	%USERPROFILE%\My Documents
PrintHood	REG_EXPAND_SZ	%USERPROFILE%\PrintHood
Programs	REG_EXPAND_SZ	\\vm-win2k-sql2k\homes$\%username%\Start M
Recent	REG_EXPAND_SZ	%USERPROFILE%\Recent
SendTo	REG_EXPAND_SZ	%USERPROFILE%\SendTo
Start Menu	REG_EXPAND_SZ	\\vm-win2k-sql2k\homes$\%username%\Start M
Startup	REG_EXPAND_SZ	\\vm-win2k-sql2k\homes$\%username%\Start M

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Figure 3.10: Redirected folders registry entries set via GPO or by registry edit.

In addition to the User Shell Folders key, NT and earlier include a Shell Folders key. You can find both the User Shell Folders and the Shell Folders key in NT in either the current user or local machine hives of the registry. The order of precedence is as follows:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders *

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders *

* These keys are NOT used in Win2K and later.

This method of modifying the registry to achieve folder redirection works similarly to that of Group Policy but it is not quite as robust. Whereas Group Policy allows you to move the contents to the redirected location, manipulating the paths in the registry simply points the user to a second, new copy of the folder. You will need to move the contents yourself or the result might be duplicate entries (see Figure 3.11). In the following figure, the user's Programs folder location was modified in the registry, but the original still exists, resulting in two Programs folders.

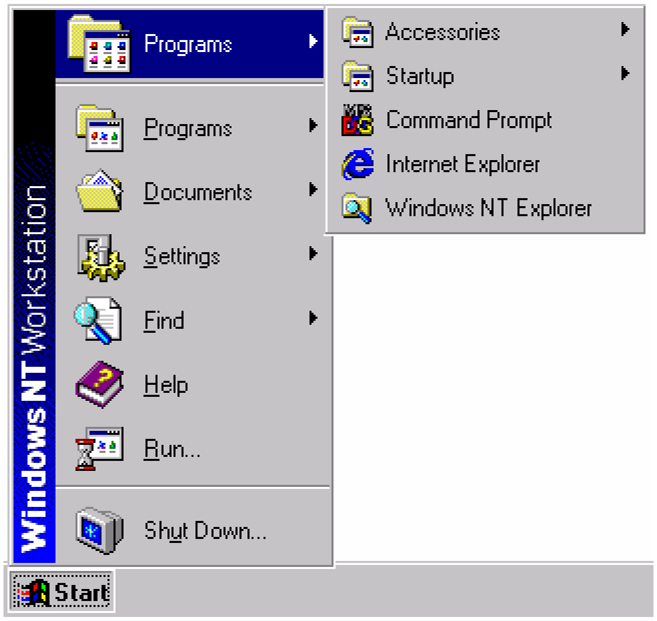


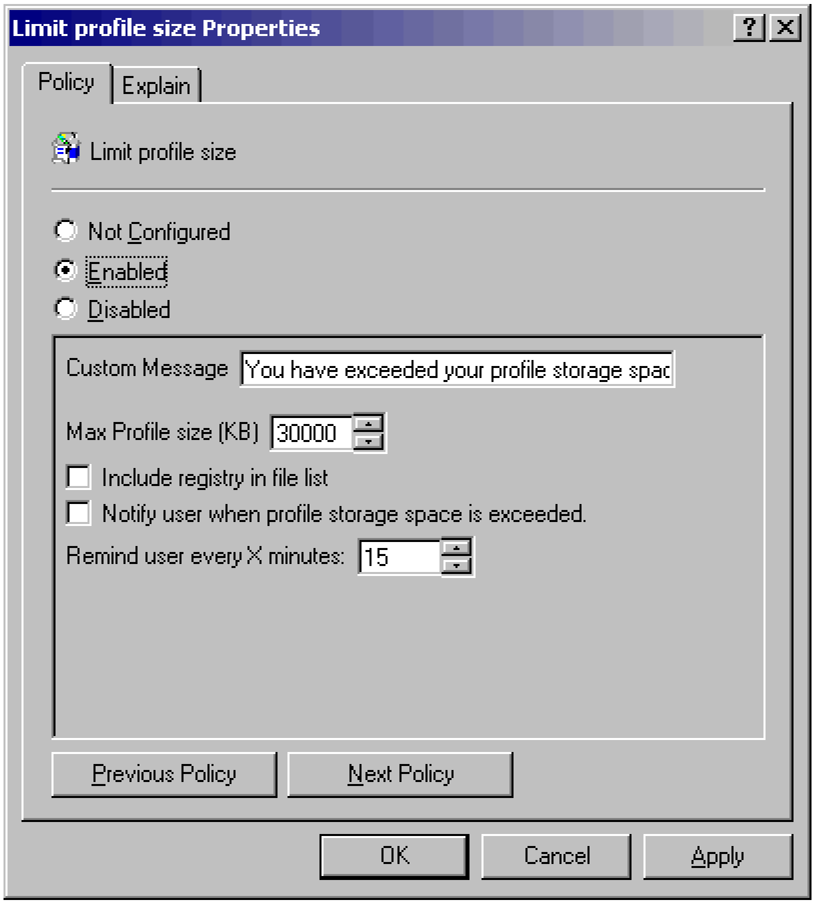
Figure 3.11: A redirected programs folder in NT results in two Programs folders.

If the original location is left, keep in mind that it is in no way linked to the redirected copy. Users might still navigate to the folder locally and any modifications will not be reflected in the redirected location.

☞ Like folder redirection via Group Policy, if a path is specified that does not exist, it is created when the user logs on.

User Profile Quotas

With the release of Win2K, built-in support for drive space quotas is now available. NT offers support for quotas via the ProQuota.exe utility (provided in SP4). You can prevent users from having roaming profiles that take up too much disk space or, more important, that are too large to be copied up and down from the network. When users' profiles exceed the limit defined in Group Policy (using the Limit Profile Size policy, as Figure 3.12 shows), they are presented with a message instructing them to reduce the size of their profile. Further, they are prevented from logging off until the profile has been reduced to a size less than that of the defined maximum size.



Limit profile size Properties

Limit profile size

○ Not Configured
● Enabled
○ Disabled

Custom Message: You have exceeded your profile storage spac

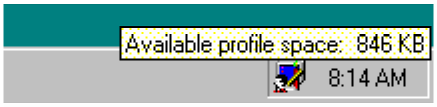
Max Profile size (KB): 30000

□ Include registry in file list
□ Notify user when profile storage space is exceeded.

Remind user every X minutes: 15

Figure 3.12: Win2K Limit Profile Size Policy.

With profile quotas in use, an icon is displayed that will show the available profile space when the cursor is placed over it, as Figure 3.13 shows.



Available profile space: 846 KB

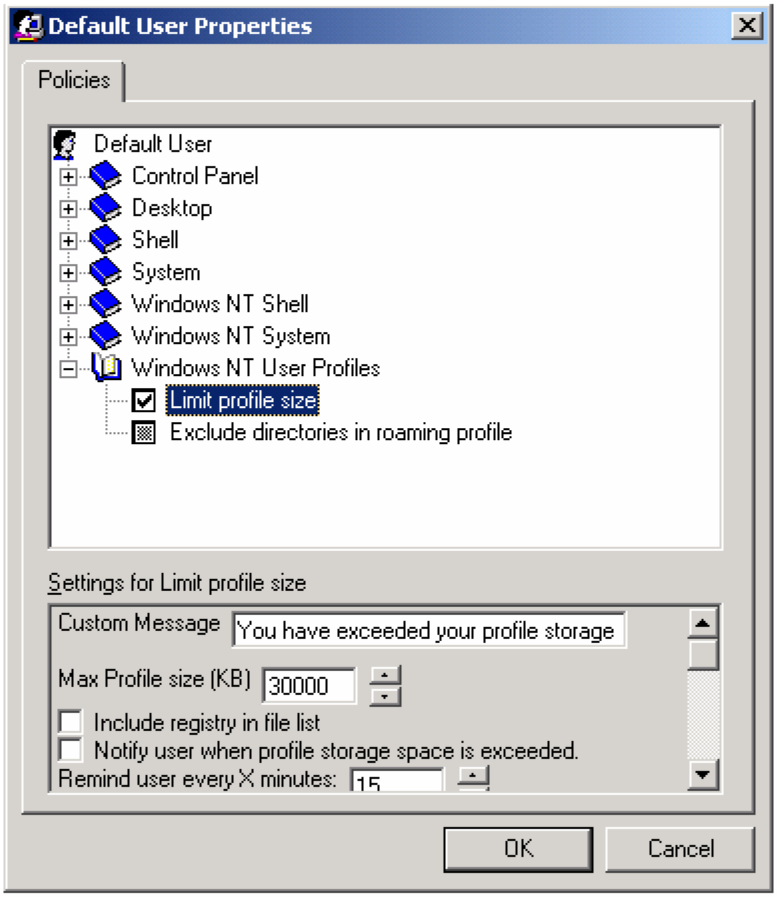
Figure 3.13: The Profile Quota icon.

To configure NT drive quotas, NT SP4 includes ProQuota.exe, which you can use with System Policies to enforce profile quotas. To configure profile quotas, perform the following set of tasks:

1. Ensure clients have the ProQuota.exe file installed. If not present, you can manually copy it to the %systemroot%\system32 directory.
2. Start the System Policy Editor (%windir%\PolEdit.exe).
3. Select Policy Template from the Options menu, and from the %SystemRoot%\inf directory, load the templates Common.adm and Winnt.adm.
4. Open Default User, and expand Windows NT User Profiles.
5. Select Limit Profile Size (see Figure 3.14), and specify the following values:

- Custom Message—This text will be presented to users when their profile size is exceeded.
- Max Profile Size—This field specifies the maximum size of a user's profile in kilobytes (the default value is 30,000Kb).
- Include Registry In File List—This check box specifies whether the Ntuser.dat file is to be presented to users in the list of user profile files that are currently in use (to help them determine which files can be removed from their profile). Obviously, you do not want a user removing Ntuser.dat, and whether you select the option to include it in the list or not, it cannot be deleted.
- Notify User When Profile Storage Space Is Exceeded—When this check box is selected, users will be presented with a warning message as soon as their profiles reach the quota size. By default, the message is only presented to users when they try to log off of the computer.

6. Save the policy as Ntconfig.pol, and store it in the Netlogon share (replication export directory on the Primary Domain Controller—PDC—for example, C:\WINNT\system32\Repl\Export).



☑ Limit profile size

▨ Exclude directories in roaming profile

Settings for Limit profile size

Custom Message: You have exceeded your profile storage

Max Profile size (KB): 30000

□ Include registry in file list

□ Notify user when profile storage space is exceeded.

Remind user every X minutes: 15

Figure 3.14: The Limit Profile Size policy.

✎ Users will not be able to log off if the user profile quota is exceeded. By default, small files (less than 2Kb in size) are not listed in the dialog box that displays the files contained in the profile. If IE is installed, there could be a great number of small files that will affect the size of the user profile in the Temporary Internet Files folder. This cache uses a small percentage of the total drive space, but can easily grow to be several megabytes in size. To delete these files, the user will need to empty the cache through the IE Internet Options dialog box.

💣 Be aware that a user can log off with an exceeded quota size by killing the ProQuota.exe process in Task Manager. Thus, defeating your imposed limitation.

Post Deployment Profile Configuration

A well-planned and tested default user profile is a good start for users, but over time any environment will undergo change: new printers, new software, new groups, and new shares. An implementation that dynamically dictates configuration and changes to settings will be best suited to handle these inevitable changes. Furthermore, the more that is taken into account dynamically, the less a default user profile is of any consequence.

Dictating Settings at Startup

A dynamic means of configuring machines or users, Group Policy provides centralized control of systems and can be easily modified for any or all users through its Startup and Shutdown script capabilities. By enforcing changes to a computer at startup, a potentially lengthy logon period can be dramatically reduced. However, changes made to the system at startup (and optionally, at shutdown) occur when no user profile is available for modification.

Despite this limitation, the more you work to customize your environment, the more you will realize a need to modify settings outside the user profile. Security settings, software installation, and changes to the All Users profile or HKEY_LOCAL_MACHINE hive of the registry are prime examples. Instead of working to bypass security and perform such actions during logon, changes might be more appropriately set to take place before a user even logs on.

Keep in mind that, like System Policies, Group Policy enforces settings. If your desire is to provide a default setting that might be modified by a user, policies are not the way to go. System Policies *enforce* settings at logon, and Group Policy *enforces* settings at startup and logon as appropriate. Further, Group Policy will reapply itself to the system at a specified interval. By default, this re-application occurs every 90 minutes, with a random offset time of as long as 30 minutes (to prevent all clients from requesting Group Policy at once).

Dictating Settings at Logon

Group Policy and System Policy can enforce settings at logon as well. Additionally, logon scripts run in the context of the user logging onto a system, providing the ability to modify the user profile. Typically implemented using scripting languages such as KiXtart, VBScript, or the DOS Shell, administrators can dynamically customize the user environment based on several criteria, including:

- Group membership
- Computer name
- IP address
- Windows version
- Organizational unit (OU—in AD)

Depending upon a user's location, you might want to map certain printers. Depending upon what group a user is a member of, you might want them to map a shared network folder. Depending upon the OU that the computer is in, you might want certain software configured. This customization can be a rather involved endeavor depending upon your requirements.

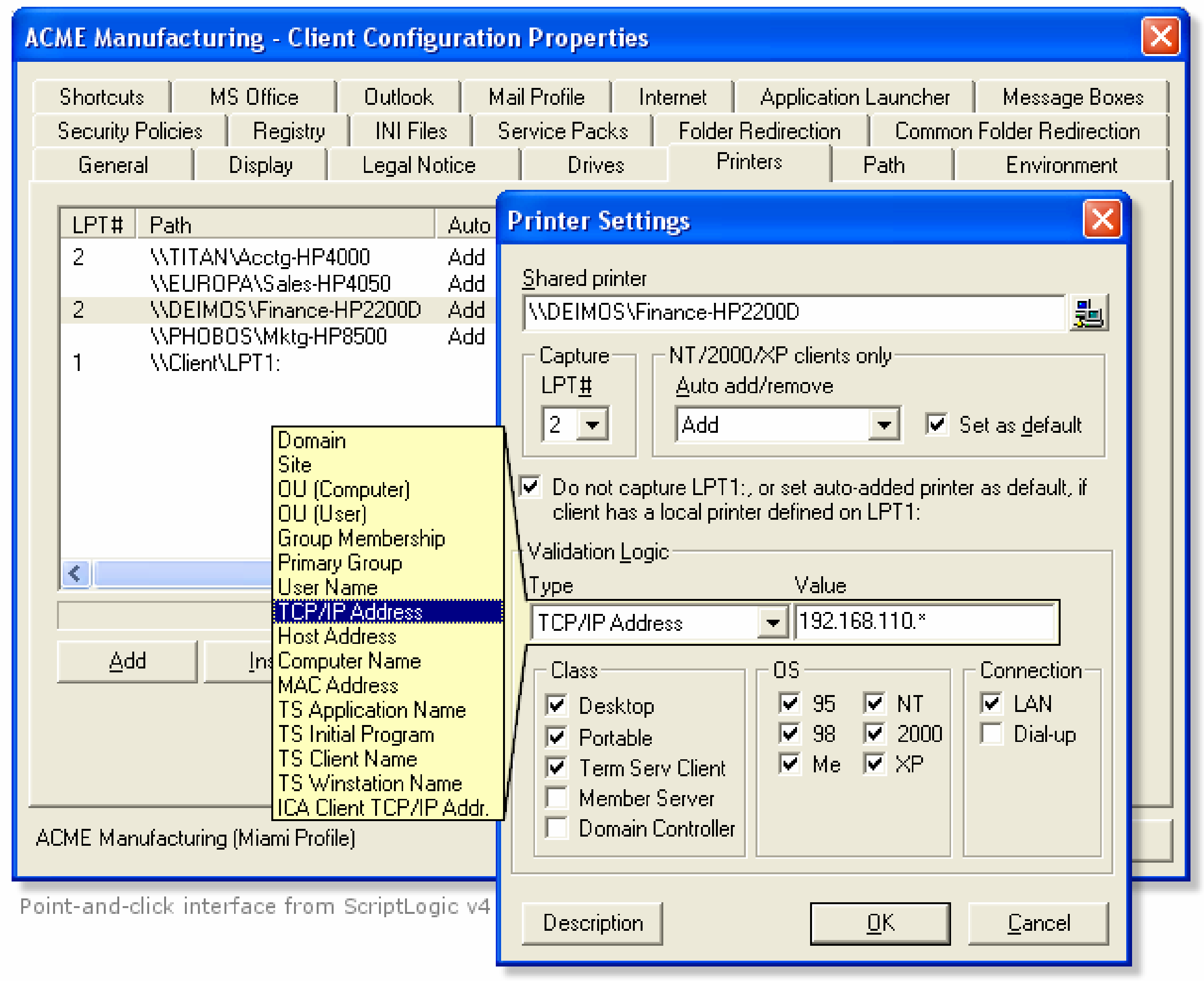
> 🕮 We will discuss custom scripting in more detail in Chapter 7.

Additional Tools

Third-party tools have been introduced to help administrators maintain control and configuration of user settings. Although a solution tailored specifically to your environment might be realized using scripts and other command-line tools, such an implementation can be challenging, complicated, and limited to the capabilities of your staff. In this section, we will touch on the capabilities of third-party tools designed to help employ a customized solution without the need to write scripts.

ScriptLogic

ScriptLogic provides a completely point-and-click interface for customizing a user's desktop environment based on a wide variety of conditions. Figure 3.15 shows the Printers tab, one of several items that you can customize.



LPT#	Path	Auto
2	\\TITAN\Acctg-HP4000	Add
	\\EUROPA\Sales-HP4050	Add
2	\\DEIMOS\Finance-HP2200D	Add
	\\PHOBOS\Mktg-HP8500	Add
1	\\Client\LPT1:	

Domain
Site
OU (Computer)
OU (User)
Group Membership
Primary Group
User Name
TCP/IP Address
Host Address
Computer Name
MAC Address
TS Application Name
TS Initial Program
TS Client Name
TS Winstation Name
ICA Client TCP/IP Addr.

ACME Manufacturing (Miami Profile)

Shared printer: \\DEIMOS\Finance-HP2200D

Capture: LPT# 2

NT/2000/XP clients only: Auto add/remove: Add ☑ Set as default

☑ Do not capture LPT1:, or set auto-added printer as default, if client has a local printer defined on LPT1:

Validation Logic

Type: TCP/IP Address Value: 192.168.110.*

Class: ☑ Desktop ☑ Portable ☑ Term Serv Client □ Member Server □ Domain Controller

OS: ☑ 95 ☑ NT ☑ 98 ☑ 2000 ☑ Me ☑ XP

Connection: ☑ LAN □ Dial-up

Point-and-click interface from ScriptLogic v4

Figure 3.15: Using ScriptLogic to customize a user's desktop environment.

The following conditions, for which actions can be based (as supported by ScriptLogic), provide a good example of how you can implement a truly dynamic configuration:

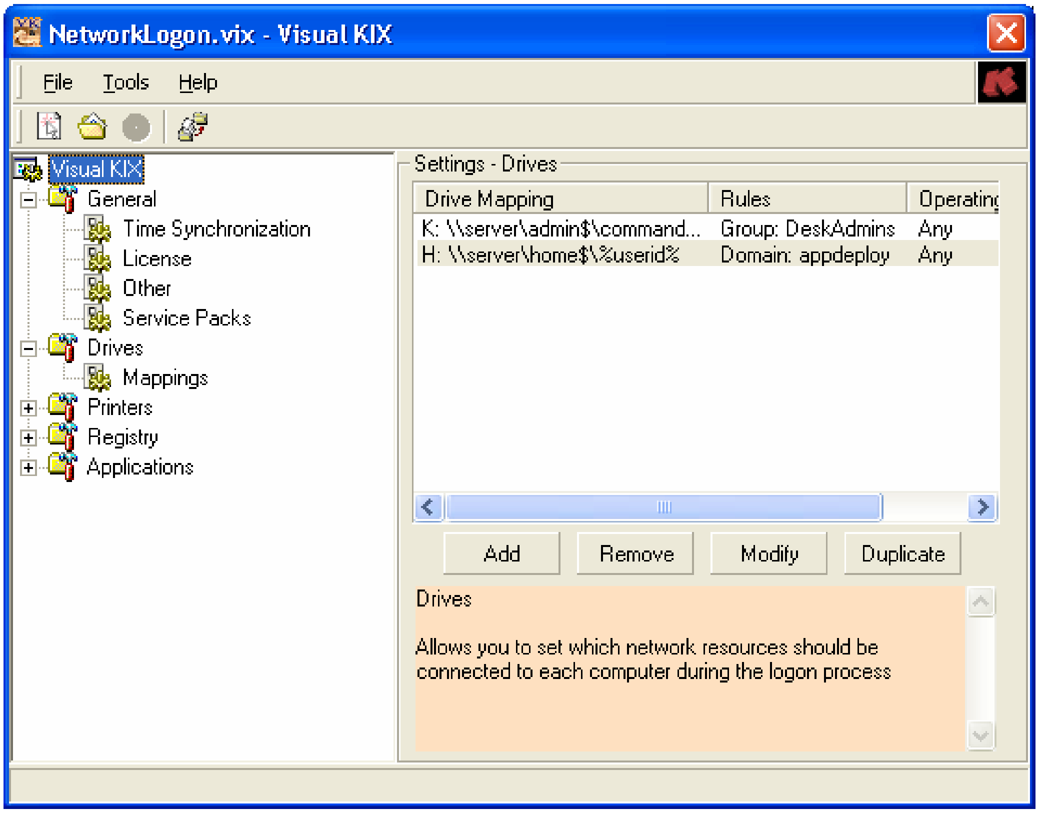
- Domain
- Site
- Computer or User OU
- Group membership
- Primary group
- User name
- TCP/IP address
- Host access
- Computer name
- MAC address

- Terminal Services application name
- Terminal Services initial program
- Terminal Services session name
- ICA client TCP/IP address

Additionally, you may focus actions on specific versions of Windows, connection types (LAN or dial-up), and class of systems (desktops, portable systems, Terminal Service clients, member servers, and domain controllers). It also provides the ability to run at logon or logoff (on all Windows platforms) and can use an alternative security context to perform actions that you might otherwise be unable to carryout within the user security context.

Visual KIX

Another solution for gaining the ability to customize and dictate configurations without writing scripts is Visual KIX. This tool provides the ability to accomplish many basic actions one would typically include in a logon script, including drive mappings (see Figure 3.16), registry changes, program launches, time synchronization, and the installation of service packs.



Drive Mapping	Rules	Operating
K: \\server\admin$\command...	Group: DeskAdmins	Any
H: \\server\home$\%userid%	Domain: appdeploy	Any

Drives

Allows you to set which network resources should be connected to each computer during the logon process

Figure 3.16: Visual KIX GUI.

Like ScriptLogic, Visual KIX also provides an automated method for replicating your final configuration to the network from which it is called through the normal logon script process.

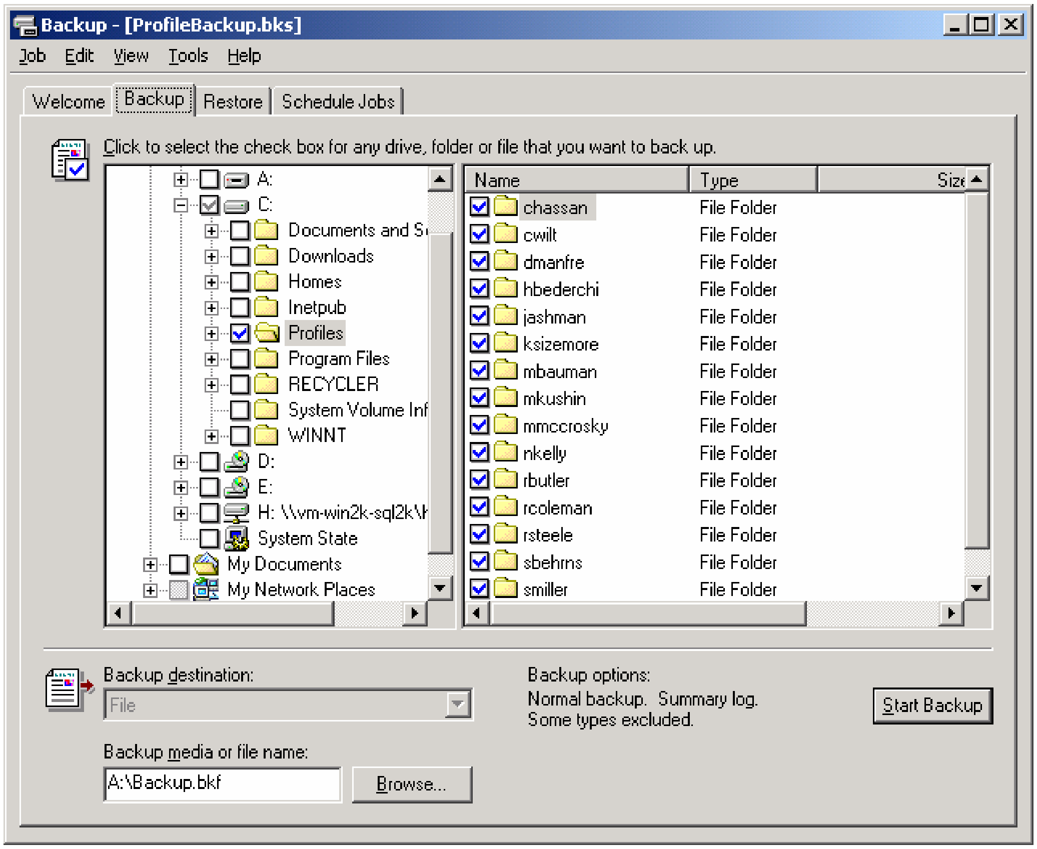
Both ScriptLogic and Visual KIX utilize the KiXtart scripting language as their core engine, which illustrates the power and usefulness of KiXtart as a Windows logon scripting language. For more information about KiXtart, visit http://www.KiXscripts.com, http://www.KiXtart.org, or http://scriptlogic.com/kixtart.

Backing Up and Restoring Profiles

By now, we have established that user profiles are certainly critical to users, especially considering the potential for the inclusion of data created by the user. It therefore stands to reason that you would want to back up user profiles.

Traditional Backup Systems

In environments in which roaming user profiles have been implemented, simply backing up the share to which they are stored is a simple and effective way of maintaining a backup. Scheduling a regular backup of your roaming profile share to occur daily or weekly is recommended for any network implementation of roaming profiles. Since the release of NT, backup software has been included as a utility within Windows. Win2K introduced a significant update to the backup software through its licensing of Veritas's backup software (see Figure 3.17). Most networks have a backup mechanism of some kind in place; simply ensure that roaming user profiles are included in the backup and (if possible) given special consideration for quick recovery.



Click to select the check box for any drive, folder or file that you want to back up.

- □ A:
- ☑ C:
  - □ Documents and S
  - □ Downloads
  - □ Homes
  - □ Inetpub
  - ☑ Profiles
  - □ Program Files
  - □ RECYCLER
  - □ System Volume Inf
  - □ WINNT
- □ D:
- □ E:
- □ H: \\vm-win2k-sql2k\I
- □ System State
- □ My Documents
- □ My Network Places

Name	Type	Size
☑ chassan	File Folder	
☑ cwilt	File Folder	
☑ dmanfre	File Folder	
☑ hbederchi	File Folder	
☑ jashman	File Folder	
☑ ksizemore	File Folder	
☑ mbauman	File Folder	
☑ mkushin	File Folder	
☑ mmccrosky	File Folder	
☑ nkelly	File Folder	
☑ rbutler	File Folder	
☑ rcoleman	File Folder	
☑ rsteele	File Folder	
☑ sbehrns	File Folder	
☑ smiller	File Folder	

Backup destination: File

Backup options:
Normal backup. Summary log.
Some types excluded.

Backup media or file name: A:\Backup.bkf

Figure 3.17: Microsoft Windows backup.

Scripted Copies

A scheduled script to perform a backup of user profiles to another folder or server share is another commonly employed method of maintaining backups of user profiles. Either copying a network share where roaming profiles are stored or remotely accessing each local workstation, keeping an online backup makes for quick and easy restore. The following text shows a simple example of how you can create a backup copy of your roaming user profiles:

```
Robocopy D:\Profiles \\BackupServer\Profiles /E /PURGE
```

This command line will copy all files from the local D:\Profiles folder to the \\BackupServer\Profiles share. The /E switch instructs Robocopy to include subdirectories, including empty ones, and the /PURGE switch instructs Robocopy to remove any files from the destination directory that do not exist in the source location.

Robocopy (Robust Copy) is available from in Microsoft resource kits (NT and later versions).

Migration Tools

There are several tools on the market to help in the migration of user data and settings from one system to another. These tools are geared toward those moving to a fresh new system who want to retain their desktop appearance and settings (including data files stored on the system identified by either directory or file extension). A fresh system is typically introduced via the deployment of a new OS or baseline deployment. With the exception of manual or scripted updates to the Windows OS, user settings and data are typically lost. User data may be taken out of the equation if folder redirection is in use, but settings must often still be taken into consideration. You can use third-party migration tools to migrate from one version of Windows to another or as a part of your desktop recovery process. Additionally, most of the imaging tools on the market today include a user settings and data migration tool.

You can find links, information, and reviews of the many migration tools on the market at http://appdeploy.com/tools/migration.asp.

Troubleshooting Profiles

Because profiles are a distinctly separate element of the user environment, they can be used in troubleshooting. When there is a problem with someone’s machine, some administrators promptly delete the user profile to see whether the problem goes away. Doing so can cause considerable trouble for users who have worked to define their default settings and even the appearance of their desktop. It might seem unimportant, but if users will spend time restoring these lost customizations, they are not doing there jobs—and as the one who deleted their profiles, it’s your fault!

Is there problem with an individual application? Try removing just these applications’ registry settings or try deleting the application data folder from the user profile. If you determine that it is necessary to delete a user’s profile, it is usually sufficient to simply delete the user’s registry settings (Ntuser.dat). Better yet, simply rename the file so that it can be easily recovered if it turns out not to be the problem.

Unable to Load Profile

If the problem is that a user is receiving an error and is unable to load the user profile, the troublemaker could be one of the following:

- Permission on the %SystemRoot%\Profiles directory has been modified; the Everyone group requires Full Control of this folder to load profiles.
- Not enough drive space or a registry size limit has been exceeded—a user profile will fail to load if either is true.
- If the local or roaming copy of Ntuser.dat (or .man) is corrupted, an error will occur and the profile will fail to load.

> ✎ Win2K and Windows Server 2003 include support for Microsoft Encrypted File System (EFS) but neither supports the use of EFS within roaming user profiles.

Troubleshooting Profile Problems with UserEnv.log

The UserEnv.log file is a very helpful tool for troubleshooting the process of loading and unloading user profiles. Each step in the user profile process is identified in this log file, including informational and error messages.

Support for logging is built into Win2K and later. Simply make the following registry edit to enable logging:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	UserEnvDebugLevel
Type	REG_DWORD
Data	10002 (Hexadecimal)

For NT, there is another version of the UserEnv.dll file, referred to as the "checked" version, which is identical to the retail version except that it contains debug flags that you can set and use with the kernel debugger. You can obtain the checked version of this file in either the NT Device Driver Kit (DDK) or the NT SDK. In addition to using this version of the UserEnv.dll, you must also set a registry entry. To enable UserEnv.log in NT, perform the following actions:

1. Rename the file UserEnv.dll in the %systemroot%\System32 folder to Userenv.old.
2. For the client machine to be debugged, copy the checked version of UserEnv.dll to the %systemroot%\System32 folder.
3. In the registry editor, add the following registry value and reboot the system:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	UserEnvDebugLevel
Type	REG_DWORD
Data	10002 (Hexadecimal)

The UserEnv.log file is created in the root directory of the C drive. This file is a simple text file that you can view using a text file viewer. On Windows XP systems, the log file is created at %WinDir%\Debug\UserMode\UserEnv.log.

Listing 3.1 shows a sample log output from UserEnv.log on a Windows XP Pro computer.

```
USERENV(298.d0) 20:38:49:639 PingComputer: Adapter speed 100000000 bps
USERENV(298.d0) 20:38:49:639 PingComputer:  First time:  0
USERENV(298.d0) 20:38:49:649 PingComputer:  Fast link.  Exiting.
USERENV(298.d0) 20:38:56:981 ProcessGPOs: network name is
mindspring.com
USERENV(298.d0) 20:39:04:252 ProcessGPOs: Computer Group Policy has
been applied.
USERENV(298.d0) 20:39:04:252 ProcessGPOs: Leaving with 0.
USERENV(298.d0) 20:39:04:262 EnterCriticalPolicySection: Machine
critical section has been claimed.  Handle = 0x110
USERENV(298.d0) 20:39:07:867 LeaveCriticalPolicySection: Critical
section 0x110 has been released.
USERENV(298.d0) 20:39:07:877 GPOThread:  Next refresh will happen in
105 minutes
```

Listing 3.1: Sample log output from UserEnv.log on a Windows XP Pro system.

Using Profiles with Multiple Versions of Windows

With roaming profiles, users are not restricted from logging onto computers running different versions of Windows. However, NT user profiles are not compatible with Win2K systems A Win2K server can act as a repository for any type of profile, even an NT profile, but the system will not load an NT user profile, nor will an NT system load a Win2K user profile. One way to maintain roaming profiles on a network that has both NT and Win2K systems is to provide different accounts for logging onto each system.

Windows 9x profiles are not compatible with NT systems At first glance, the folder structure might look similar, but the incompatibility lies in the registry structure contained in the registry hive (User.dat and Ntuser.dat) files. The registry structures are completely incompatible between Windows 9x and NT. It is recommended that profiles for each of these OSs be stored in their own location. This implementation is fairly easy to configure and manage as Windows 9x profiles are stored in the user home directory, and NT profiles locations are specified in the user account profile itself.

Hard-Coded Profile Paths

Since NT, the %UserProfile% environment variable has been available as a reliable means of addressing the user profile directory. Despite this, some applications look to the %SystemRoot%\Profiles folder for user profiles. Because this had been the location of the user profile up until Win2K, it was not uncommon for software developers to assume this location. As a result, situations might arise in which a user logs onto NT without problems, but when logging onto Win2K, encounter a problem as a result of a hard-coded, invalid path.

System and Group Policy Assignments

NT enforces settings across the domain through System Policies. These settings are cached as part of the user's profile. Win2K enforces settings across the domain using (GPOs), which are added to the user's registry settings at HKEY_CURRENT_USER\Software\Policies, and Windows looks to this location for settings to be enforced on a user (overriding what may be contradicting settings elsewhere in the registry). If users log onto an NT system and have System Policies applied, then log onto a Win2K system and have GPOs applied, no technical limitation exists to prevent such a situation. However, the inclusion of both settings in the user's registry settings might increase its size.

✎ By default, NT calculates the registry size as 25 percent of the paged pool. The default page pool size is approximately equal to the amount of RAM. The maximum registry size is 152MB (80 percent of the paged pool, which is limited to 192MB). With Win2K, the default registry size limit is 33 percent of the size of the paged pool with the same maximum of 80 percent of the paged pool allowed. In Windows XP and Windows Server 2003, the registry files are mapped in the computer cache address space. Therefore, regardless of the size of the registry data, it is not charged more than 4MB. There are no longer any explicit limits on the total amount of space that can be consumed by hives in paged pool memory and in disk space.

Summary

In this chapter, we have discussed the user profile—its use and benefits. We covered the multiple types of profiles and the configuration of a custom default user profile. I discussed problems to avoid when using roaming profiles as well as ways to reduce their size through quotas and folder redirection. In the next chapter, we will explore another major part of establishing your users' work environment: deploying and upgrading the applications themselves.