

Realtime
publishers

"Leading the Conversation"

The Definitive Guide™ To

Vista Migration

sponsored by



altiris®

*Danielle Ruest
and Nelson Ruest*

Chapter 8: Working with Personality Captures	209
Define your Profile Policy	211
Choosing the Profiles to Protect	213
Differences between Windows XP and Vista.....	214
Completing the Personality Protection Policy	217
Determine your Backup Policy	223
Prepare your Protection Mechanisms	224
Long-term Personality Protection Mechanisms.....	227
Relying on Vista's Folder Redirection	228
Enabling Folder Redirection with Roaming Profiles.....	232
Finalizing the Personality Protection Strategy.....	234

Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 8: Working with Personality Captures

Personality protection is probably the most important aspect of any operating system (OS) deployment project; not, of course, from the technician's point of view, but rather, from the end user's point of view. After all, while we, as technical IT professionals, view a computer as a system we need to build and maintain, end users view it as a necessary evil they need to work with to perform their job functions. And personalities—the collection of data, favorites, desktop settings, application customizations and more—are the most important aspect of any OS migration for them.

That's because users perceive their computer's personality as part of their workspace and many of them will spend considerable time optimizing it for the work they do. If computer personalities are not preserved in the course of a migration project, users lose productivity as they take time to either relearn or recreate the aspects of their old computer personality that they depended on to get their work done. For many users, losing printer settings, email configurations, Microsoft Word templates or even the placement of shortcuts on their desktop can compromise their comfort level and effectiveness with a new machine and/or operating system. This disorientation decreases productivity and increases the helpdesk workload because it leads to unnecessary end-user support calls and training.

Therefore, preserving the personal computing environment of each user is a critical step in mitigating the productivity impact of an OS migration and controlling its costs. As with the other engineering processes that are required to complete an OS migration project, this process includes several steps (see Figure 8.1).

- Begin with defining the administrative policy you will use to provide this protection. For this, you'll need to fully understand the differences between profile structures in Windows XP and their counterparts in Windows Vista since these profiles are *not* compatible with one another; profiles are the OS components that store personalities. Then, you'll need to determine which mitigation strategies you intend to use as well as how you will protect profiles once they are captured.
- Next, you need to perform an analysis of your network. You've already performed inventories to determine your hardware and software readiness status. Now, you need another inventory to determine how many profiles you need to protect and how much central storage space you need if you choose to copy the profiles you decide to protect to a network share.
- Then, once this is established, you can begin to prepare your protection mechanisms. Of course, this will be closely related to your tool selection as the tool you selected for this purpose will provide many of the features you'll require for this protection.
- Once the mechanisms are in place, you can move on to testing. Make sure you test this process fully and make sure you involve end users in the acceptance testing to guarantee that the level of protection you provide will meet and perhaps exceed their expectations.

- When everything is as you expect and you have approval from end users, you can sign off on the personality protection strategy and begin its integration into the overall migration process.

These steps form the basis of this chapter. Once again, they are mostly performed by the PC team with support from the server team if network protection and backup has been included in the protection policy.

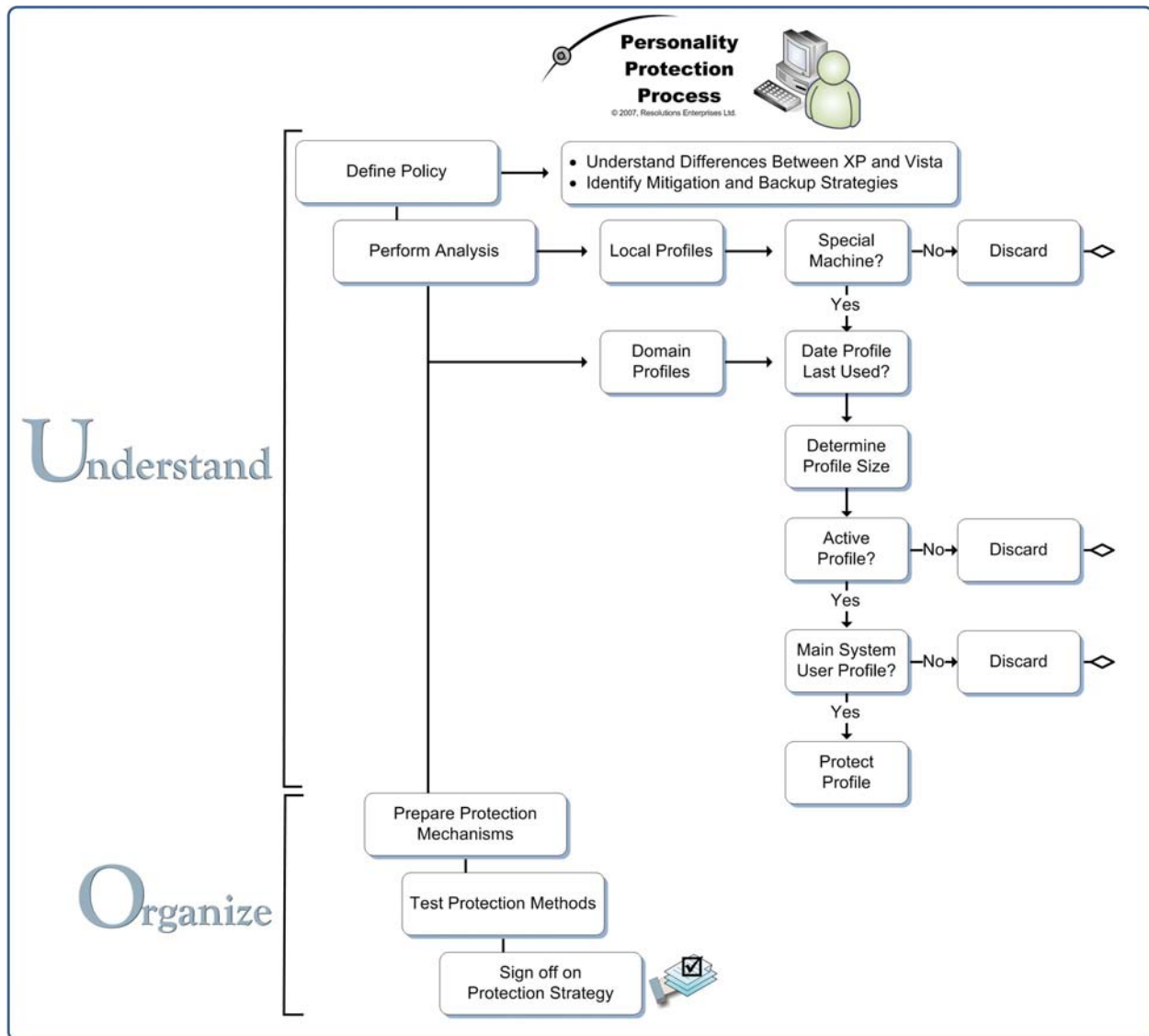



Figure 8.1. The Personality Protection Process

Define your Profile Policy

 This is part of the **Understand** phase of the QUOTE System (see Chapter 2 for more information).

In order to define your protection policy, you first need to understand personalities or profiles and how they work, and then you'll want to categorize the profiles in your network to help determine which you will protect (see Table 8.1). A profile is generated the first time a user logs onto a system. Basically, the first time the user logs on, the contents of the default user profile are copied and personalized for the user. The system automatically resets the security parameters of these contents so that the user has exclusive access to them. This is one reason why it is so important to properly manage the contents of the default user profile when you create your system image as discussed in Chapter 7. By creating one single default user view, you standardize how end users access and interact with the computer systems you deploy to them. Of course, they will make this profile evolve, but you can at least ensure that key elements remain common in all profiles.


Users can log on through a domain, relying on an Active Directory (AD) authentication, or through the local system, relying on the local security accounts manager (SAM) database that can be found on every Windows system. Each first-time logon will create a profile. This means that technicians who log onto a system for repair purposes will automatically generate a profile as will any other user logging on for other purposes.

Most local logons are volatile because few organizations run their network without a central authentication database such as AD provides. This means that in most cases, you can discard any local profiles from your protection strategy. That is, unless you have custom systems that operate in a workgroup only. Many organizations use such systems to monitor and maintain systems connected to a demilitarized zone (DMZ) such as those found in a perimeter network. You can evaluate the opportunity to protect such local profiles versus having administrators and technicians recreate them when these machines are upgraded. If your default user profile is properly created, the value of protecting any local profile will be minimal.

Therefore, your protection policy should concentrate on profiles that are generated through domain logins. If your network offers a single PC to a principal user, then you'll have it relatively easy since all you will need to do is identify the principal user's profile on a system, protect it and discard all other profiles. If your network uses shared computers, then it will be slightly more difficult. Domain login profiles can also be protected by other means such as roaming profiles—profiles that are stored on the network and downloaded to each PC as the user logs on—or folder redirection policies—Group Policy objects (GPO) that move the contents of local folders found in the profile to network locations. Your analysis will need to take these factors into account if you want a protection policy that will meet the needs of every user in your network.

Some organizations, especially those that must operate 24/7, will also have generic accounts in their network. Generic accounts are shared accounts that allow operators to share a machine without needing to log on or off at the end of their shift. There are two types of generic production accounts. The first deals with 24/7 operations and is required as mentioned above to run a machine without the need to log on or off. Operators share the password to this account and can thus change shifts without closing the session.

The second type is for environments that have a high personnel turnover. A good example of this is on naval vessels. Since officers and staff change almost every time the ship docks and crews are rotated, some organizations choose to use generic role-based accounts instead of named accounts. For example, a first officer would use the First Officer account instead of one named after him or herself. In this situation, the password may or may not be shared. It depends on the amount of effort the administrative staff is willing to undertake at each crew change. They can either reset the passwords of each generic account or not, as they wish. Obviously, a policy that would require either named accounts that could be renamed each time a crew member changes or password changes at each crew change would be much more secure than one where passwords are shared.

 With Windows Vista, organizations that are currently using generic production accounts can mostly do away with them because Vista supports Fast User Switching (FAS) even in a domain environment. Organizations that rely on shared accounts to run operations and machinery can now use named accounts because their operators can each be logged on personally while others are using the same machine. There is no downtime for the machine as shifts change and users each have their own account and a private password. This creates a much more secure environment.

If your organization decides to move from generic to named accounts during its migration, then your protection policy will have to support the capture of a shared profile and its restoration to multiple users, something few organizations face today.

Profile Type	Comments
Default User	Used to generate new profiles at first log on.
Network Default User	Stored on the network under \\domaincontrollername\Netlogon share. Used to generate new profiles on domain-joined computers.
Mandatory Profile	Read only profile that is forced on users. This profile is not saved at log off.
Super Mandatory Profile	Like the mandatory profile except that it will force log off if the profile cannot be loaded from the network.
Roaming Profile	Profile that is stored on the network and loaded at log on. Changes are saved at log off.
Local Logon	Profile generated when logging on to the SAM. Usually volatile profiles.
Network Logon	Profile generated when logging on to Active Directory. Usually permanent profiles.
Principal User Profile	Profile of the main user of a machine.
Generic Account (24/7)	Account used in 24/7 operations to ensure no log off is required at shift change.
Generic Account (Shared)	Account used in situations where there is high personnel turnover. Accounts are named by position and shared among users who hold this position.

Table 8.1 Different Profile Types.

Choosing the Profiles to Protect

You need to have the means to determine which profiles to protect. The best way to do this is to use a flowchart that identifies which profiles to protect and under which circumstances (see Figure 8.2). We've already discussed some of the reasons why you would or would not protect a given personality.

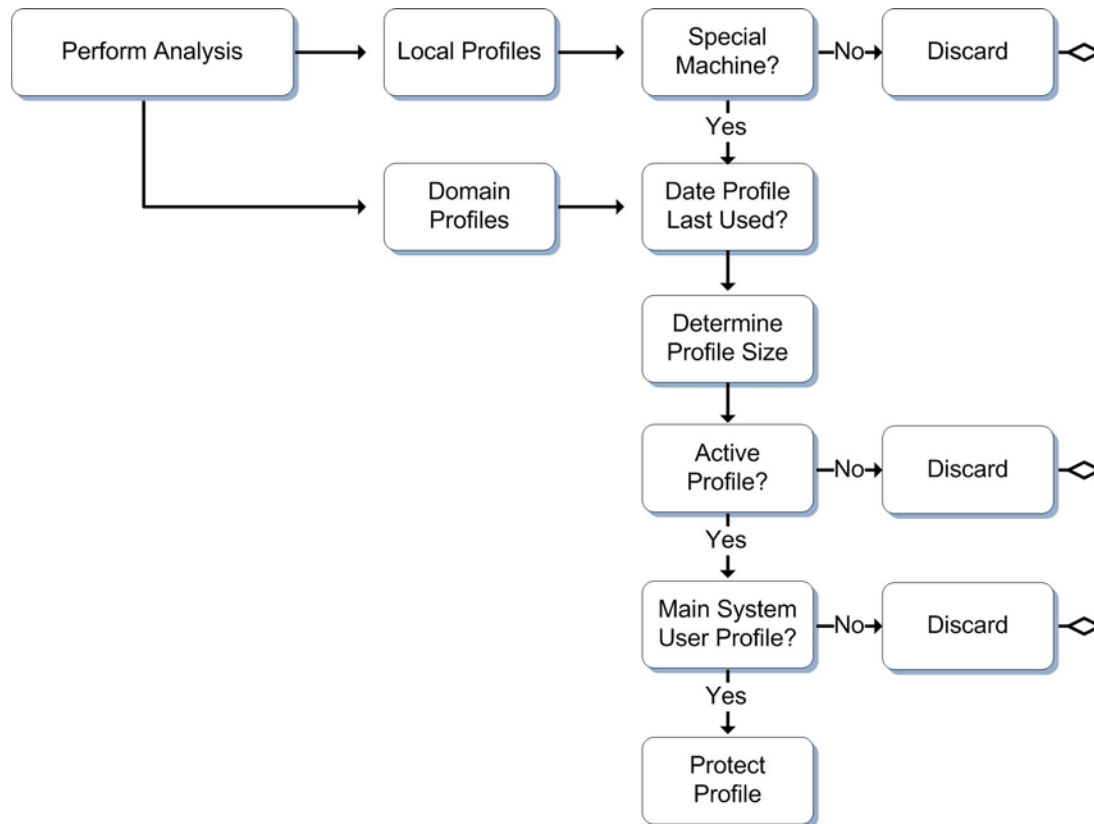


Figure 8.2. Using a Decision Chart to determine the Personality Protection Policy

This means your decision flow should include the following guidelines:

- Local profiles are only protected if they are situated on special machines that are not part of the domain and cannot be replaced by a custom default profile.
- Domain profiles are protected if they have been used recently and on a constant basis.
- Only profiles with actual content are protected (based on profile size).
- Only active profiles are protected.
- If your machines have principal users, then their domain profiles are protected at all times.

There are of course, other considerations, but these decisions should form the main crux of your personality protection policy.

Differences between Windows XP and Vista

Profiles are designed to store several different types of content:

- The first is user data which ranges from user-generated documents to desktop preferences to Internet favorites and more; basically, anything a user generates when they are working with their PC system.
- The second is user application data. This includes custom dictionaries, custom toolbars in applications, custom settings for one particular application and so on.
- The third is application data that applies to any user of a system. In XP, this system-wide data was stored in the All Users profile, a profile that was shared as its name suggests by all users. In Vista, the All Users profile disappears and becomes the **Public** profile.

Each data type has its own particularities and each requires a slightly different treatment. In addition, profile data is stored not only in the file system, but also within the Windows registry under the HKEY_USERS Structure. The profile of the user that is currently logged on is stored under HKEY_CURRENT_USER, a volatile registry structure that is designed to store in memory profile contents. Finally, profiles contain volatile information within a special profile file: NTUSER.DAT which is located in the root of the user's profile folder. This file contains the in-memory information related to a user's login session. Because of this, it is difficult to protect when in use. All of these elements must be captured to protect a given personality.



Many organizations use roaming profiles—profiles stored on a network drive and which are downloaded to the PC when the user logs in. This strategy is great for users that roam from one PC to the other in a network, but roaming profiles is an outdated technology because, depending on the profile size, it will take some time for the profile to be downloaded to a system and, should the network not be available, then the profile won't be either. In addition, profile changes are only saved at log off. If the user has not logged off from one machine but wants to use another, they will get an older copy of their profile.

XP roaming profiles are not compatible with Vista. You can however mix the use of roaming profiles with folder redirection as discussed further in this chapter. This reduces the contents of the roaming profile and increases roaming profile performance while giving users access to their profile anywhere in the organization. If, however, you choose to use a different strategy, you should turn roaming profiles off before the migration. If you do not use roaming profiles, then use the more traditional profile protection strategy discussed here.

But, the first place to start to make sure all information is protected is to take an in depth look at the differences in profile structures between Vista and XP.

There are seven major differences between Windows XP and Windows Vista profile structures:

1. Profile location is the first. In Windows NT, profiles were stored in the WINNT folder, allowing users read and write privileges to this most important folder. With Windows 2000 and Windows XP, profiles were moved to the Documents and Settings folder structure. Of course, with Vista, this has been changed once again (third time lucky?) to become the Users folder structure (see Figure 8.3).



Figure 8.3. The Evolution of the Profile Location

2. The User folder structure is the second. Several different elements of the User folder structure have changed and have been relocated for several different reasons, one of the main which is the need to provide better support for roaming users through a better structured profile folder structure.
3. Microsoft has now begun using *junction points* or redirection points which appear as proper folders but are there only for compatibility purposes (see Figure 8.4). Several different folders both within and without the User folder structure act as junction points and provide support for the operation of applications that are not Vista aware. Two types of junction points are included in Vista: per user and system junction points.

```

Administrator: Command Prompt
Directory of C:\ProgramData
04/09/2007 05:22 PM <DIR> .
04/09/2007 05:22 PM <DIR> Adobe
12/26/2006 11:58 AM <DIR> Adobe Systems
12/26/2006 11:58 AM <DIR> Apple Computer
04/03/2007 04:33 PM <DIR> Application Data [C:\ProgramData]
11/02/2006 06:00 AM <JUNCTION> Beta client
12/26/2006 11:58 AM <DIR> Desktop [C:\Users\Public\Desktop]
11/02/2006 06:00 AM <JUNCTION> Documents [C:\Users\Public\Documents]
04/18/2007 04:22 PM <DIR> DRM
11/02/2006 06:00 AM <JUNCTION> Favorites [C:\Users\Public\Favorites]
02/25/2007 03:32 PM <DIR> FLEXnet
12/26/2006 11:58 AM <DIR> InstallShield
01/03/2007 09:39 AM <DIR> Microsoft
01/18/2007 10:12 AM <DIR> Microsoft Corporation
04/18/2007 02:22 PM <DIR> Microsoft Help
12/26/2006 11:58 AM <DIR> Office Genuine Advantage
12/26/2006 11:58 AM <DIR> SBSI
12/26/2006 11:58 AM <DIR> SonicStage
12/26/2006 11:58 AM <DIR> Sony Corporation
11/02/2006 06:00 AM <JUNCTION> Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
12/26/2006 12:46 PM <DIR> Symantec
12/26/2006 12:46 PM <DIR> Symantec Shared
11/02/2006 06:00 AM <JUNCTION> Templates [C:\ProgramData\Microsoft\Windows\Templates]
12/26/2006 11:58 AM <DIR> VMware
12/26/2006 11:58 AM <DIR> Windows Genuine Advantage
01/18/2007 09:46 AM <DIR> WinZip
0 File(s) 0 bytes
  
```

Figure 8.4. Displaying Junction Points in the Command Prompt

More on junction points can be found in the **Vista Application Compatibility Cookbook** at <http://msdn2.microsoft.com/en-us/library/aa480152.aspx>.

4. The Application Data folder structure has also been modified. It is now comprised of a series of junction points along with actual folders (see Figure 8.5).

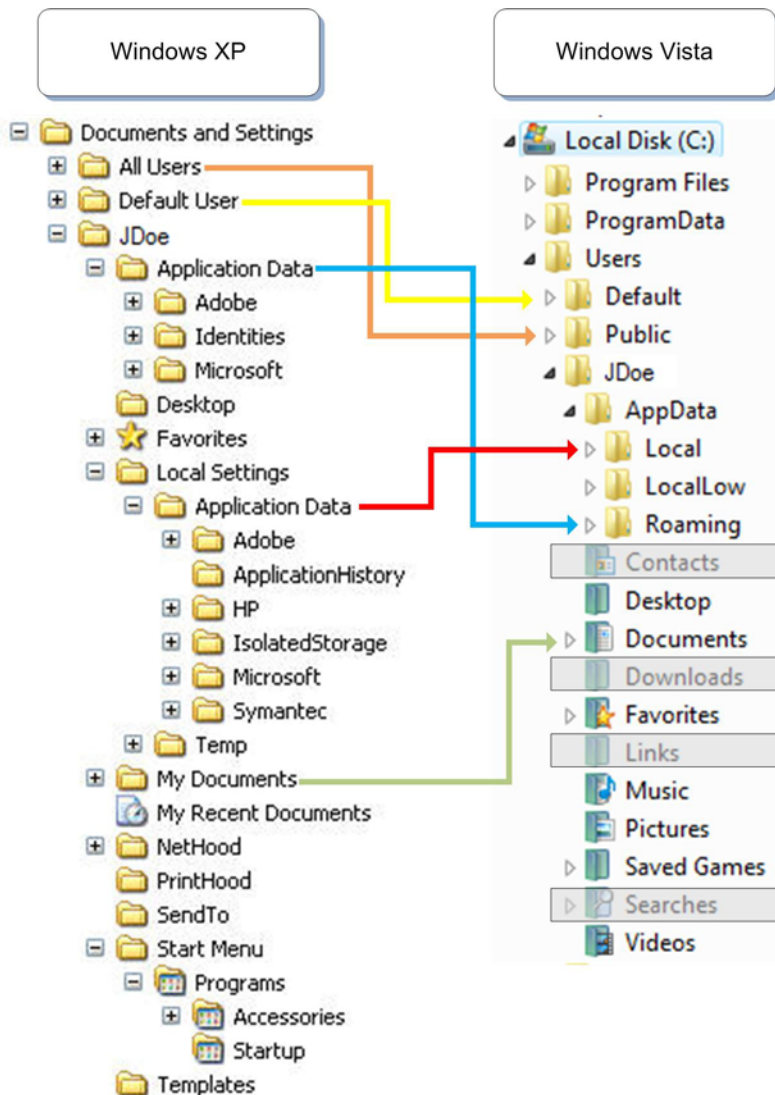



Figure 8.5. Linking the XP and the Vista Profile Structures—New Vista Folders are shown in boxes

5. A new ProgramData folder has been introduced. ProgramData works along with Program Files to store system-wide application information or what is also normally found under the HKEY_LOCAL_MACHINE registry hive with legacy applications.
6. As mentioned before, the All Users profile has now been renamed Public. In addition, the Default User's profile is now renamed Default.
7. Folder redirection, or the ability to control the location of a folder within the user profile structure through Group Policy objects (GPO), has been updated significantly and now provides real protection for all user data.

 Two new subfolders, Local and LocalLow are used to store application data that remains local at all times. Data in these folders is either specific to the machine itself or is too large to be stored on the network. For example, Outlook personal storage files (.PST) are located under the Local folder structure.

This is why it is important to supplement any folder redirection or roaming profile strategy with a full profile backup. This way, there is no possibility of data loss during machine upgrades.

Other changes are included deeper in the profile structure. For example, the Start Menu is now buried in the AppData\Roaming folder structure under the Microsoft, then the Windows folders (see Figure 8.6). This is where you will find other corresponding contents such as printer settings, recent documents, network connections and so on. These latter changes to the Vista profile structure were specifically performed to support the seventh element in the previous list, folder redirection.

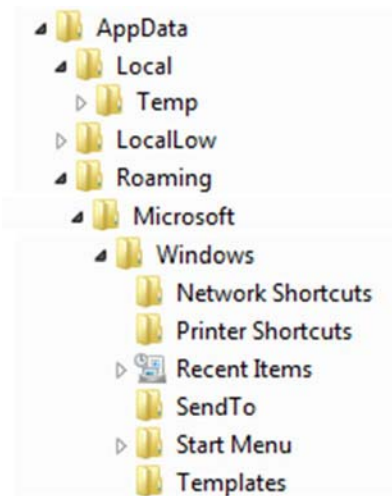


Figure 8.6. The Contents of Vista's AppData\Roaming Profile Structure

Each of these has an impact on the migration of personality content. For one thing, the tool you use for migration must support the conversion of a profile from Windows XP and perhaps earlier to Windows Vista.

Completing the Personality Protection Policy

Now that you are more familiar with the structure of the Vista user profile, you can complete your personality protection policy. Two items are left to complete:

- Identify the migration strategy
- Define the profile backup policy

The first will depend on the tools you selected. There are several tools on the market for personality protection. Hopefully, you elected to select a comprehensive tool that supports every part of the OS migration process and especially, one that has been upgraded to support Vista migrations. As far as profile migrations are concerned, your tool must support the translation of XP or earlier profiles to Windows Vista. In addition it should include several other features:

- Store the profile(s) to migrate either locally or remotely on a network share.
- Compress all profile contents to reduce space requirements, network traffic and migration time.
- Support a profile collection analysis to help determine how complicated your personality protection strategy will be.
- Support the application rationalization process through the migration of application settings from one version of an application to another.
- Support the creation of profile migration templates so that you can premap migration settings and therefore automate profile migration processes.
- Support the integration of the profile collection and restoration process to the overall OS migration process.

The degree of support your tool will offer for each of these elements will help determine the contents of your personality protection policy.

Profiles can be stored either locally or remotely. If you decide that you do not want to reformat disk drives during the OS migration, then you can store profiles locally. Remember that the Vista image-based setup (IBS) is non-destructive and supports proper upgrades.


Tools such as the Symantec Ghost Solution Suite and Altiris Deployment Solution support local profile storage even if a disk wipe is performed. Storing the profile locally will definitely save you time since profiles tend to be large and take time to transfer over the network. But, storing the profiles locally can be a risk to the project because there is no backup for them. If something goes wrong, you won't be able to go back and recover information from a locally stored profile. If, on the other hand, you choose to store profiles on a network share, you will then be able to back them up and protect them for the long term. Remember, as far as an end user is concerned, the protection of the personality of their computer is *the* most important aspect of the project for them.




During one of our migration projects, the project team lost a single profile out of more than 2,500. Unfortunately, it happened to belong to a developer who was in charge of the single, most important application the organization was running. It turned out this user had never backed up anything from his computer before and had never stored any single piece of code onto the network. More than five years of work was lost.


Your project will not face such a disastrous situation, but keep in mind that a protection policy for the data in every profile is critical to the perceived success of the project. Imagine losing any profile from upper management—these are the kinds of pitfalls that are really easy to avoid through proper preparation and structure.

If profiles are to be carried across the network, then you need to have them compressed as much as possible. This is one more reason why they should be cleared of all useless data beforehand. One good way to ensure this is done is through a pre-migration analysis of both profile contents and approximate profile sizing. Use the flowchart in Figure 8.2 to help determine what you are looking for in this analysis. Your objective is to make the best possible use of bandwidth during the protection.

 Be sure to communicate with users before the migration to have them clean up their profile data as much as possible. There is no need for your project to transport outdated data and favorites across the network. Integrate this into your communication strategy and provide this as one of the actions users are responsible for before your project reaches them.

Most profile protection tools will support this analysis through some form of pre-migration inventory. For example, Microsoft's command-line User State Migration Tool (USMT) supports this type of pre-analysis, but since its findings are not stored in a database, you will need to record them in some manner to get a global picture of the status of your network. It does provide results in Extended Markup Language (XML) so it may not be too complicated to program some form of automated collection tool, but why burden your migration project with this additional task if you don't need to?

 For more information on the USMT, read **Migrating to Windows Vista Through the User State Migration Tool** at <http://technet.microsoft.com/en-us/windowsvista/aa905115.aspx>.

 Commercial tools provide graphical interfaces for profile management. See Ghost Solution Suite at http://www.symantec.com/enterprise/products/overview.jsp?pcid=1025&pvid=865_1 or Altiris Deployment Solution at <http://www.altiris.com/Products/DeploymentSolution.aspx>.

In addition, the personality protection team must work closely with the application preparation team to determine which applications will be transferred over to the new OS. You don't want to capture settings for applications which will not be carried over during the migration. The application preparation team will also be performing an application rationalization to reduce the level of effort required to prepare applications for the migration and help streamline operations once the migration is complete.

Part of this effort will involve the removal of multiple versions of the same application when possible. Therefore, your migration tool must support the migration of application customizations from one version to another. For example, an organization with multiple versions of Microsoft Office should standardize on one single version. This means that the personality protection tool should be able to capture settings from older versions of Office and convert them to the version you have elected to standardize on (see Figure 8.7).

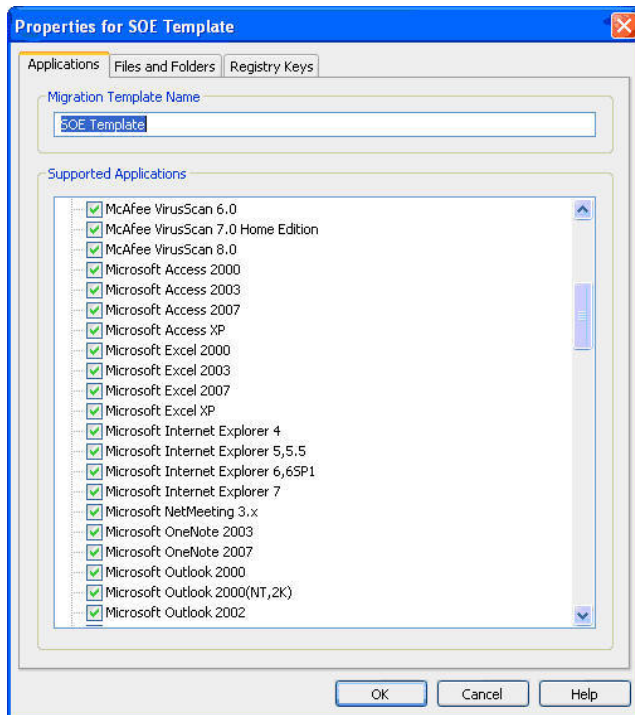


Figure 8.7. Symantec Ghost Solution Suite can capture setting from multiple versions of Microsoft Office

If your organization is like most, you will rely on at least one in-house or custom developed application. Make sure your migration tool can support the capture of data and settings for any proprietary programs and not just standard programs like Microsoft Office.

You should also be able to create personality capture templates that can be optimized for different departments or groups. Users in marketing appreciate having settings for Microsoft Office transferred to their new machines while developers will want to keep their Visual Studio .NET configuration. Advanced tools support the ability to create a template to capture the unique settings of each user type (see Figure 8.8).

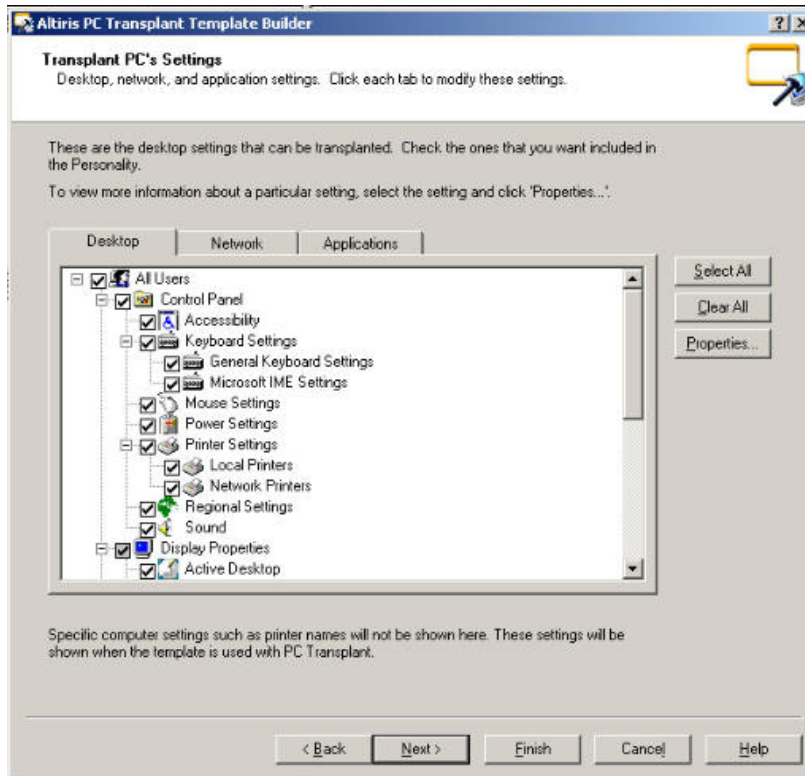


Figure 8.8. Altiris Deployment Solution support the creation of personality protection templates on a per group basis

The personality protection tool must seamlessly integrate into the overall OS migration process. Command-line tools such as USMT let you script the process and integrate the script into both the pre-migration and post-migration stages. More sophisticated tools let you remotely and silently capture personalities from end user machines through a central administrator console.

In sensitive environments, you might also want to protect profile contents through the assignment of a password to the profile package. In addition, since the ability to capture a profile requires high-level administrative rights on the machine, you will need to make sure the profile capture and restoration occurs in the proper security context (see Figure 8.9). Using a tool that lets you integrate both levels of security through a central console will certainly facilitate the overall process.

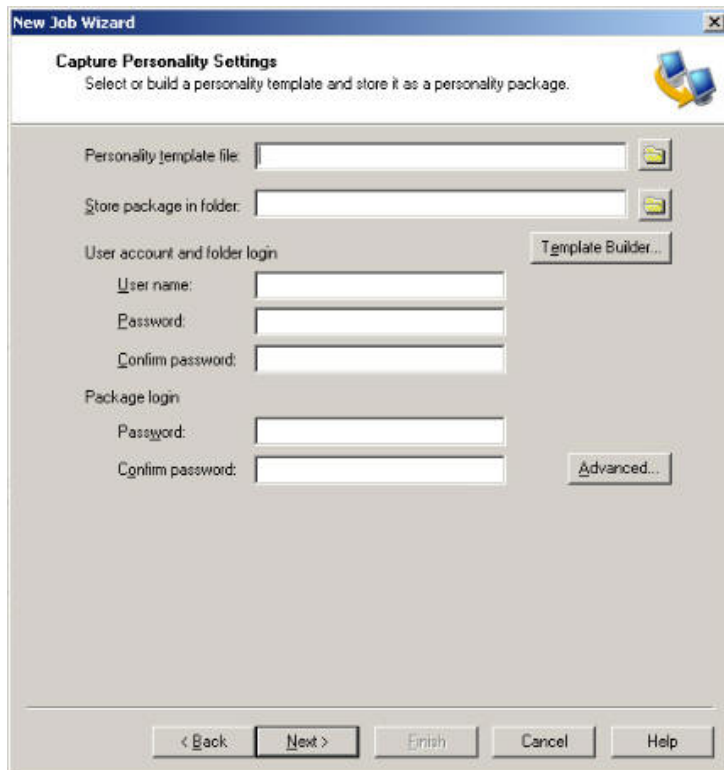



Figure 8.9. Altiris Deployment Solution support the protection of profile contents as well as the assignment of a security context for profile capture and restoration

Some users may require more personal interaction in which a project member sits down with the user and walks them through a wizard-based, highly customized personality capture. An easy-to-understand, wizard-based personality capture is also helpful with remote users who may need to do the job on their own.

Any user whose settings have been saved and properly restored will remember the project team with fondness and will not fear future migrations. Keep this in mind at all times when you are working on this aspect of the project.

You should also consider how the personality data is stored and then reapplied. Ideally, all personality settings should be rolled into a single compressed executable package. This helps with remote users who may have to restore their own settings. Just double-clicking the executable on the new machine is all that it takes to re-apply the personality data.

Finally, your protection strategy should include the ability to store personality data across different removable media—such as a CD, DVD or USB flash drive—which will also be useful for remote users who have to both capture and restore personalities on their own. An undo option to remove the personality in case it is applied to the wrong machine is also a very helpful feature.

 If you decide that your personality capture efforts will be limited to only official data types, be sure to communicate it to end users. Give them plenty of time to archive anything that won't be migrated by IT so they can access it later if need be. Many organizations tend to capture a complete image of the legacy machines before performing a migration. This provides a failsafe method of retrieving user data not included as part of a migration for the users that did not have time to backup their own data or simply did not know how. This also provides a great solution for rolling back to a previous state if an in-place hardware refresh was not completed successfully.

Determine your Backup Policy

Personality protection is, as mentioned earlier, the most important aspect of the migration for end users. This is why most organizations opt to take the time to transfer profiles over the network and create a centralized backup of each personality they protect. It is true that moving profiles over the network will take time and will slow down the overall migration process, but the good will it will buy you from users will make it worthwhile. You should aim to back up all profiles if you can. Some organizations even choose to back up the entire PC image just in case the profile protection misses something.

This begs a discussion of the actual migration process itself. There are several approaches:

- The in-place migration
- PC rotations
- Hardware attrition

Each involves its own benefits and potential issues.

If you decide to perform in-place migrations, then you will be leaving PCs where they are and perform the system replacement—whether it is an actual upgrade or a complete OS replacement including a system disk wipe. To do so, you will need high-speed network connections and your technicians will either have to work at night or during weekends to minimize the disruption to the business. High-speed links and proper network storage should not be a problem in large central offices but they may be an issue in remote offices. Many organizations use portable servers for this purpose. These servers are designed to support many processes such as OS system image deployment, protection for personality captures, software deployment and so on.



Performing upgrades—replacing the OS without wiping the system disk—is often the very easiest migration process to choose. Upgrades are non-destructive so no profile migration is required. Of course, few organizations choose to use upgrades because it does not give them an opportunity to ‘clean up’ their systems as they perform the OS migration.

PC rotations use a different process. When organizations perform OS migrations, they often have to replace a significant portion of their PC systems. This new batch of computers are often much higher-powered than the other systems in the network, especially if you choose systems that will support all of Vista’s features. With this new pool of computers, the organization can set up a rotation system that removes existing systems from the network and replaces them with systems from the replacement pool. This often involves a cascade where each user will receive a PC that is better than the one they were using before, once again using the systems from the original purchase to begin the cascade. Since many users will be receiving used systems, the migration team also implements a cleaning process to make sure that each user has the impression of getting a nice new and clean computer.

The point of this discussion is that when rotations are performed, each computer is taken away from the network and moved to a staging area for the OS replacement. This means that the mechanisms you need to protect personalities need only be in the staging area, reducing the cost of performing the migration and reducing the impact on production networks. You may still need to have a solution for remote sites, but this can often be nothing more than a mobile staging center.



Do not confuse the staging area with the staging test level. While some organizations merge the two roles together, many choose to maintain the staging area—the area where new computers are prepared—within the production domain and the staging test level—the last level of testing before moving into the production network—uses its own, independent domain.

If you choose to rely on hardware attrition for the migration, then you should use a staging area for system preparation. Of course, you may choose to perform the personality capture from user systems while they are still in the network. Ideally, you will try to perform all migration activities in a staging center because this approach has the least impact on productivity.

Whichever method you use to protect profiles in central and remote offices, once the profile is on the network, you'll want to back it up to permanent storage. Many organizations choose to protect the personality, moving it to a network drive, back it up to permanent storage and then, leave it on the network share for a period of about two weeks. This lets you define your backup policy:

- Profiles are stored on network shares for a period of two weeks.
- Profiles are backed up to permanent storage.
- Any missing contents from the restored system can be retrieved from the profile stored on the network share during the first two week period.
- After two weeks, the profile contents are removed from the network share.
- Missing contents that are discovered after the two week period must be restored from permanent backups.

This strategy provides a compromise between a personality protection guarantee to end users and the amount of storage space required for this aspect of the migration process during the actual migration. Make sure you communicate this strategy to your end users *before* you begin the migration.

Prepare your Protection Mechanisms



This is part of the **Organize** phase of the QUOTE System.

Now that you have determined your overall protection policy, you can move on to the preparation of all of the engineering mechanisms required to support it. Here, the PC team will have to work with their server counterparts to complete these engineering activities.

Perhaps the first place to start is to describe to the server team how you intend to proceed and indicate to them the protection flowchart you intend to use. They can then provide the best assistance based on your protection choices. Basically, this is what you should detail to them (see Figure 8.10):

1. You'll begin with a profile analysis to help determine storage sizing and determine network bandwidth requirements.
2. If you are using roaming profiles in Windows XP and you don't want to implement joint folder redirection and roaming profiles, then you'll need to turn them off prior to the migration of each system.
3. Then, you'll create templates to meet specific protection goals. Work with the application preparation team to identify the applications you need to protect.
4. You'll use the templates to protect each system's core profile (see Figure 8.2).
5. If you've decided to back up the entire system, then this will be done after the personality has been protected.
6. You'll store the system backup offline, backup the profile and keep it available for 2 weeks.
7. Profiles will be available from offline backup after 2 weeks.
8. Profiles will be restored after the OS migration has been completed. This should occur after applications have been reloaded on the system.
9. Your profile protection guarantee will include the following:
 - a. Profile implementations can be rolled back in the case of problems.
 - b. Machine OS upgrades can be rolled back if serious issues arise after the migration.
 - c. If generic profiles were in use, they will be migrated to individual profiles. In this case, the same generic profile is migrated to multiple individual profiles. Users will rely on Fast User Switching to provide continuous operations.
10. A 20 working day support guarantee will be provided to each user after the migration.

Storage resources will be liberated once the migration has been successful. The personality protection team members will be responsible for automating both the capture and restoration of the profiles. If you have the right tools, this should involve nothing more than providing the appropriate answers and settings to wizard-based interfaces.



If you decide to work with application virtualization and stream them to each desktop, you will need to integrate the streaming process with the personality restoration. More on this topic will be covered in chapter 9 as we discuss how you bring every element of the migration together.

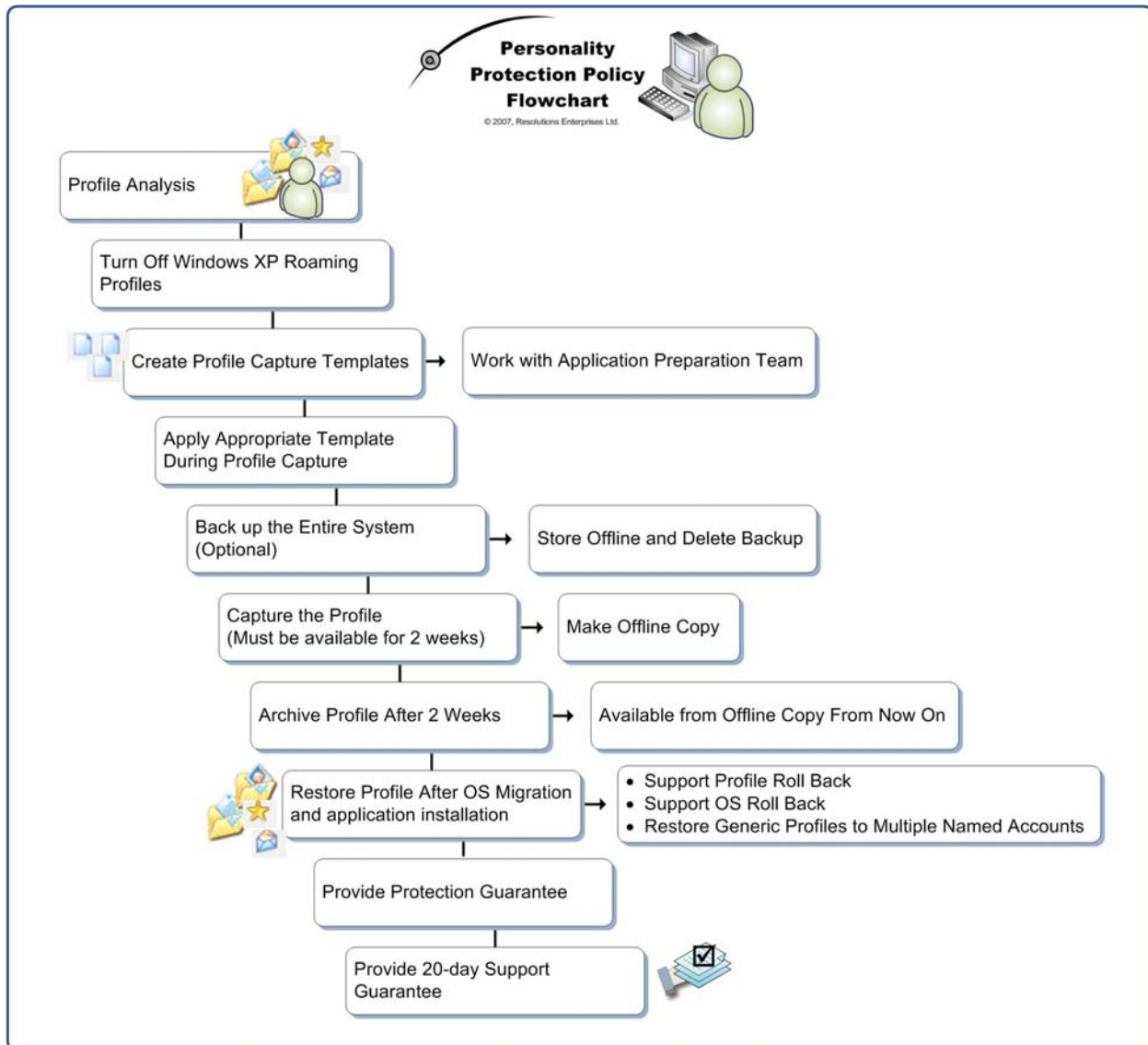



Figure 8.10. The Personality Protection Policy Flowchart

Be sure to perform end-to-end testing of each phase of the personality protection process and be sure to have end users sign off on acceptance testing for the solution you propose. This will avoid any nasty surprises during the project. Then, once all testing is done, you can sign off on your personality protection strategy.

Long-term Personality Protection Mechanisms

As you can see, preparing a personality protection strategy involves a lot of different steps. And, you might think the personality protection team's efforts stop when this is achieved, but what do you do once the OS migration is complete and the new OS is in production? Microsoft has put in a lot of effort to make personality protection an everyday process. That's right; the entire User folder structure has been revamped in order to provide support for one thing: folder redirection and general profile protection.

Folder redirection is an aspect of Group Policy that will automatically redirect user folders to central locations. When coupled with offline folder caching, folder redirection can provide the best of all worlds for users whether they are roaming or not: folders are located on network shares where they can be backed up and made available at all times. Their contents are cached locally so even mobile users have access to their data even when disconnected. If any changes are made locally, they are automatically synchronized the next time the network connection is available. This means that both connected and disconnected users have constant access to their data.

 You can combine folder redirection with roaming user profiles to gain the best of both worlds. Volatile items such as the NTUser.DAT file are not contained in folder redirection. This means that relying on folder redirection alone may provide a less than complete experience for users. In addition, relying on roaming profiles alone limits the experience because data is not available in real time as it is with folder redirection. Combine both to have folder redirection manage the data within the profile and roaming profiles manage the rest. The result is a profile that loads really fast because its contents are small and users that have access to data at all times through folder redirection. An additional advantage is that combining the two lets you support roaming users in both Windows XP and Vista. This is great for the duration of the migration when you will be managing a mix of operating systems.

But, for many, this means rethinking how they provide protection for user data. Many organizations have relied on the user home directory and/or roaming profiles to provide this type of protection. The home directory was originally designed to provide a simple way to map user shares on a network. In Windows NT, 2000 and Windows Server 2003, using the %username% variable in a template account automatically generates the home directory folder and applies the appropriate security settings giving the user complete ownership over the folder when you create a new account. When the user logs on, this folder is automatically mapped to the H: drive or any other letter you assign. But today, you shouldn't be relying on mapped drives anymore. You should be relying on the Distributed File System (DFS), especially DFS namespaces.

DFS namespaces use universal naming convention (UNC) shares to map resources for users. But, instead of using the [\\servername\sharename](#) approach, DFS namespaces use [\\domainname\sharename](#) and each namespace is mapped to an appropriate target in each site of your organization's network. DFS replication keeps the content of these target shares synchronized over the WAN.

 Find more information on DFS at <http://www.microsoft.com/windowsserver2003/technologies/storage/dfs/default.aspx>.

Since Windows 2000, Microsoft has focused on the use of the “My Documents” folder as the home of all user documents. This folder is part of the security strategy for all Windows editions beyond Windows 2000 even though it has been renamed to “Documents” in Windows Vista. This folder is stored within a user’s profile and is automatically protected from all other users (except, of course, administrators).

In Windows XP, folder redirection could manage four critical folders and assign network shares for each. These included:

- Application Data which stores all application-specific settings.
- Desktop which includes everything users store on the desktop.
- My Documents which is the user’s data storage folder. Storing the My Pictures sub-folder on the network is optional.
- Start Menu which includes all of a user’s personal shortcuts.

When redirection is activated through Group Policy, the system creates a special folder based on the user’s name (just like in the older home directory process) and applies the appropriate security settings. Each of the above folders is created within the user’s parent folder. Data in these folders is redirected from the desktop PC to the appropriate network folders. But, the user profile includes much more than these four main folders. In fact, highly volatile information such as Local Data and Favorites were not protected. Because of this, you can’t rely on Windows XP’s folder redirection to properly protect a system’s personality.



For users that roam to remote offices, you can combine folder redirection with DFS namespaces and replicate the contents of their folders to DFS target shares in remote offices. Make sure you are running Windows Server 2003 R2 to take advantage of the new delta compression replication engine in DFS replication.

Relying on Vista’s Folder Redirection

All of this changes with Windows Vista because it finally provides a mechanism for true folder redirection and personality protection. This is evidenced in the settings available for folder redirection in the Vista GPO (see Figure 8.11). As you can see, it includes redirection for much more than XP ever did.

This makes folder redirection an excellent choice for long term personality protection. It is completely transparent to the user. While they think they are using the Documents folder located on their PC, they are actually using a folder that is located on the network. This way you can ensure that all user data is protected at all times.



Microsoft provides a guide for Vista roaming user management at <http://technet2.microsoft.com/WindowsVista/en/library/fb3681b2-da39-4944-93ad-dd3b6e8ca4dc1033.msp?mfr=true>. Rely on the online version because the downloadable document does not contain as much information.

Using a folder redirection strategy rather than using a home directory simplifies the user data management process and lets you take advantage of the advanced features of the Vista network. For example, even though data is stored on the network, it will be cached locally through offline files. Redirected folders are automatically cached through client-side caching when they are activated through a GPO. Data in these folders can also be encrypted through the Encrypted File System (EFS). In fact, all offline files can be encrypted.

Vista lets you redirect ten different folders. When you combine the redirection of these folders with roaming profiles, you offer the best roaming experience to users with a lower impact on network traffic than with roaming profiles alone (see Table 8.2).

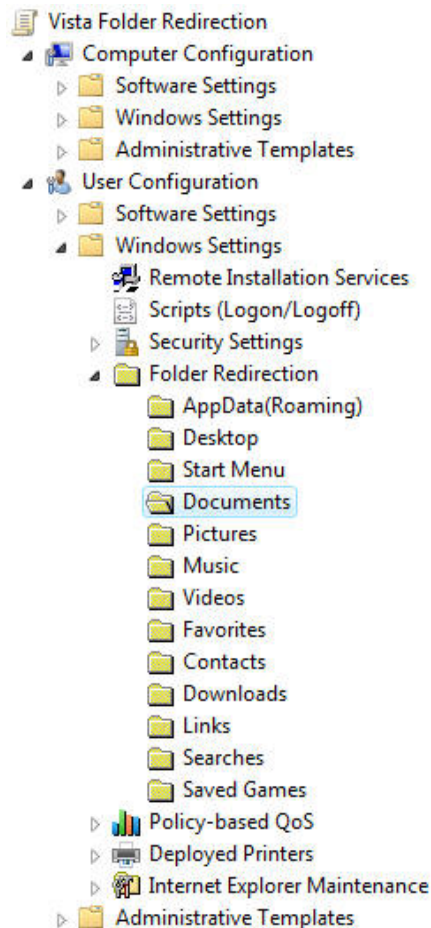


Figure 8.11. Vista's Folder Redirection GPO

Vista folder redirection policies include more settings. For example, you can automatically delete older or unused user profiles from your PCs (see Figure 8.12).

In addition, the settings you can use for personality protection are much more granular than ever before. Music, pictures and video can all be set to automatically follow the policy you set for the Documents folder. In addition, you can use the same policy to manage folder redirection for both Windows XP and Windows Vista (see Figure 8.13). This provides powerful system management capabilities.

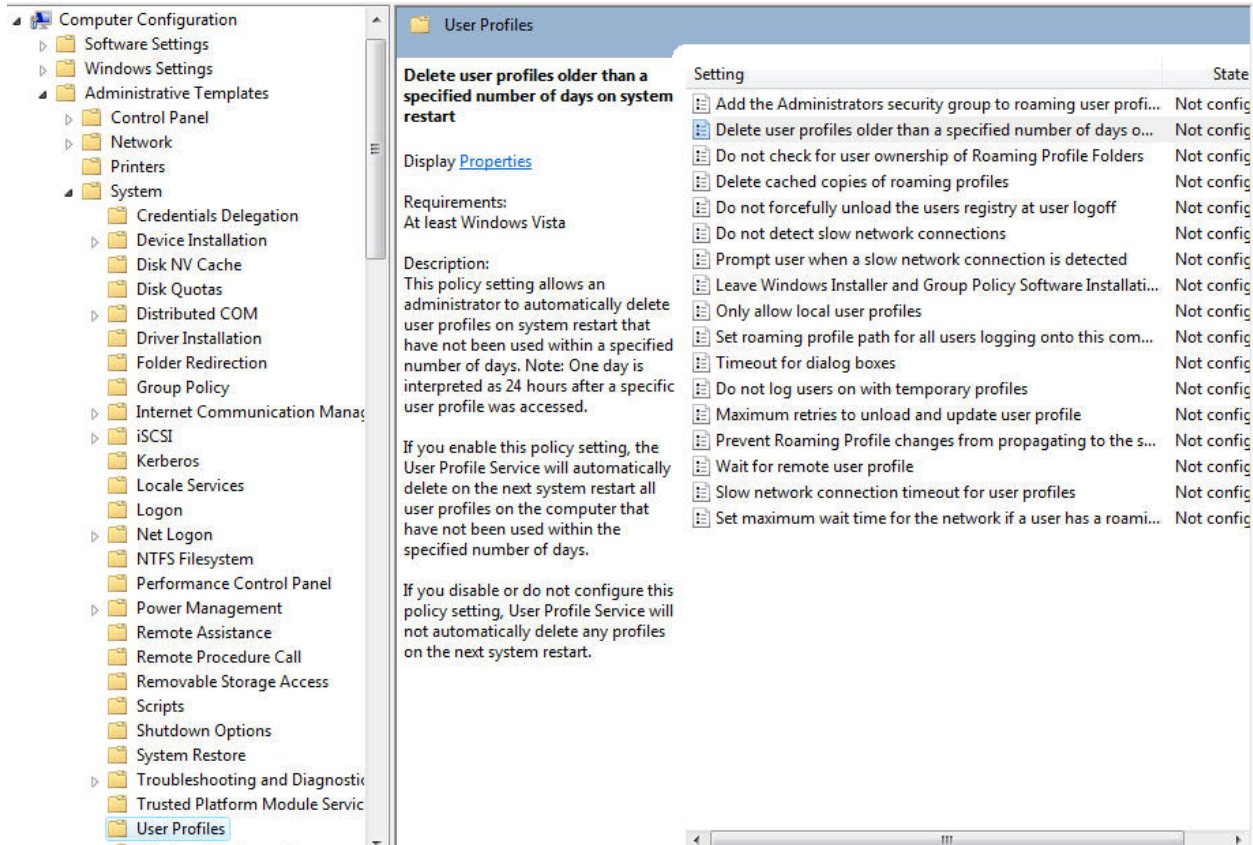


Figure 8.12. Windows Vista lets you control the behavior of User Profiles on each PC

Profile Type	Comments
AppData (Roaming)	This folder contains all roaming application data. Redirecting this folder will also support Windows XP clients with limitations.
Desktop	Users should not store data or any other items on their desktops; they should rely on the Quick Launch Menu instead. This reduces the size of the folder to redirect. Include this in your communications to them. Redirecting this folder will also support Windows XP clients.
Start Menu	The contents of the Start Menu are redirected. If you use application virtualization, then users will always have access to their applications on any PC even if they are not installed. Redirecting this folder will also support Windows XP clients.
Documents	This contains all user data. Make sure your storage policy and quotas support today's large file sizes and give users enough room to breathe. Redirecting this folder will also support Windows XP clients. Applying this policy to pre-Vista OSes will automatically configure Pictures, Music and Videos to follow Documents even if they are not configured.
Pictures	Determine if your organization wants to protect this folder. If you do, use the Follow the Documents folder option or rely on the setting in Documents. Redirecting this folder will also support Windows XP clients.

Profile Type	Comments
Music	Determine if your organization wants to protect this folder. If you do, use the Follow the Documents folder option or rely on the setting in Documents. Using this option will also support Windows XP clients.
Videos	Determine if your organization wants to protect this folder. If you do, use the Follow the Documents folder option or rely on the setting in Documents. Using this option will also support Windows XP clients.
Favorites	Only applies to Vista.
Contacts	Only applies to Vista. If you are using Outlook, then this Contacts folder is not necessary.
Downloads	Only applies to Vista. You will need to determine if your organization wants to protect downloads users obtain from the Internet.
Links	Only applies to Vista.
Searches	Only applies to Vista.
Saved Games	Only applies to Vista. The contents of this folder are very small and apply mostly to the games included in Vista. Your organization will need to determine if you want to spend network bandwidth and storage space on this content.

Table 8.2 Recommended Settings for combining Vista Folder Redirection with Roaming Profiles.

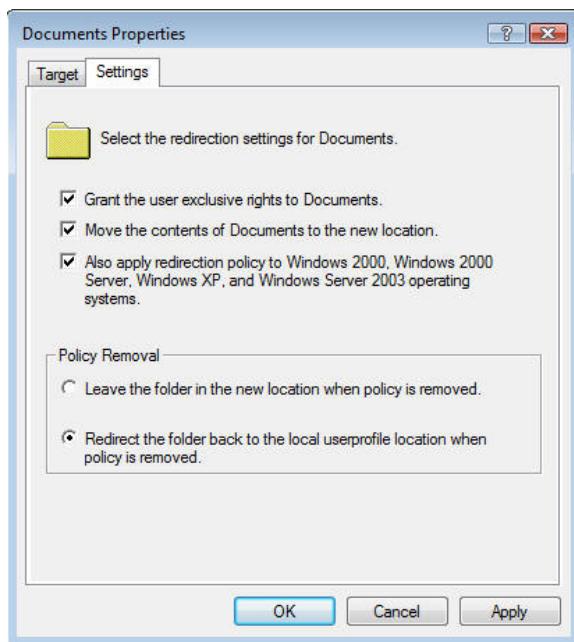




Figure 8.13. Folder Redirection in Vista offers several more choices than in Windows XP


 If you choose to use folder redirection to provide a bridge between XP and Vista during the migration, you will need to supplement this approach with some form of local content capture because many key profile folders are *not* protected by Windows XP folder redirection. You don't want to find out after the fact that users are missing their favorites or even worse, their Outlook data files.


Enabling Folder Redirection with Roaming Profiles

There are special considerations when enabling folder redirection. First, you need to ensure that each user is redirected to the appropriate server. It wouldn't do to have a user in New York redirected to a server in Los Angeles. To do this, you must create special administrative groups that can be used to regroup users and ensure that each user is assigned to the appropriate server; you most likely already have security groups you can use for this. You must also ensure that offline settings are appropriately configured to guarantee that users are working with the latest version of their offline files.

 Make sure you assign appropriate amounts of storage to each user for folder redirection. There is no point in making this effort if you limit their disk space access to something that is unacceptable.

Redirecting folders through user groupings is in fact very similar to creating regional or rather geographically-based user groups. Since each server is in fact a physical location, you will need to create a user group for each server. Begin by enumerating the location of each file server that will host user folders, and then name each global group accordingly. Once the groups are created, you can begin the redirection process. Using groups allows you to limit the number of GPOs required for the folder redirection implementation.

 In chapter 7, we discussed how to create the default user profile. With Windows, you can store this profile under a folder named **Default User** in the **Netlogon** share of your domain controllers—use [\\domaincontrollername\netlogon](#) to access the share; Active Directory replication will automatically make this folder available on every domain controller in your domain. Placing the default profile in this location will let each PC load the default profile from the network instead of from the local machine. Since profiles are not compatible between Vista and XP, you need to name the Vista network profile folder to **Default User.v2** (the v2 identifies Vista); this will separate the Vista profile from its XP counterpart. Be sure to fully test this strategy with both Vista and XP systems to make sure nothing untoward occurs when default profiles are created.

 Vista also supports mandatory profiles, but since it relies on version 2 profiles, you must name the network folder containing this mandatory profile with the .v2 extension as with any other profile-related folders in Vista.

Use the following procedure to prepare your folder redirection with roaming profiles strategy. Make sure you are running Windows Server 2003 Service Pack 1 or R2 as your server OS. Make sure all GPO settings are prepared and modified from a Vista PC.

1. Begin by creating the shares that will support redirection and roaming. You will need a minimum of two shares: one for the user profiles (for example, User_Profiles) and one for folder redirection (for example, Folder_Redir). If you are already using XP roaming profiles, then use this share for the profiles.
2. Next, create a folder for each user in your organization under the profiles section. Name each folder with the user's account name followed by a .v2 extension. Vista will rely on this folder to enable the Vista roaming profile. Assign full control to each folder for the user and for the System accounts. You can generate a script to do this by exporting your user list from AD and adding the appropriate command line settings in a program like Microsoft Excel. Vista will populate these folders when users first log on to the system.

3. Because Vista does not display much user information during log on and log off, you might want to change this default behavior. Apply a GPO to all Vista PCs and set the **Administrative Templates | System | Verbose vs normal status messages** option under Computer Configuration. This will let users know what is happening during logon and it might also be useful for debugging issues.
4. Verify that roaming profiles have been set up in user account properties in AD. Each user will have two profiles during the migration—version 1 for XP and version 2 for Vista.
5. To reduce the content of the roaming user profile and therefore limit network traffic and logon times, exclude key folders from the roaming profile contents. Use the **Administrative Templates | System | User Profiles | Exclude directories in roaming profile** option under User Configuration. List each of the ten folders supported by Vista's folder redirection (see Table 8.2). Type the name as it appears in Windows Explorer and separate each name with a semi-colon (;).
6. Rely on the suggestions in Table 8.2 to set your folder redirection policy. Use **Windows Settings | Folder Redirection** options under User Configuration to do this. Change the property of each folder. Redirect them to your folder redirection share. There are a couple of caveats:
 - a. When you set the folder properties for folders that are supported by both Windows XP and Vista, use the **Also allow redirection policy...** option under the Settings tab (see Figure 8.13).
 - b. When redirecting AppData (Roaming), you will get a compatibility warning message (see Figure 8.14). This is because older Windows OSes do not support the full functionality of Vista in terms of folder redirection.
 - c. When redirecting the Documents folder, you will also get a warning message. In this case, it tells you that by selecting to support older OSes, you automatically change the behavior of the Pictures, Music and Video folders; they will be protected by default and set to **Follow the Documents folder**. If you do not want to protect them, then set the policy explicitly for each folder.
7. When Windows XP systems are no longer in use, archive all XP profiles (the ones without the .v2 extension) and remove them from your servers.

Test the strategy in the lab before deploying it to production. Once again, have users sign off on it through acceptance testing to make sure they are also happy with its operation. You will need to warn users that their first logon will take time as Vista downloads the contents of their profiles.

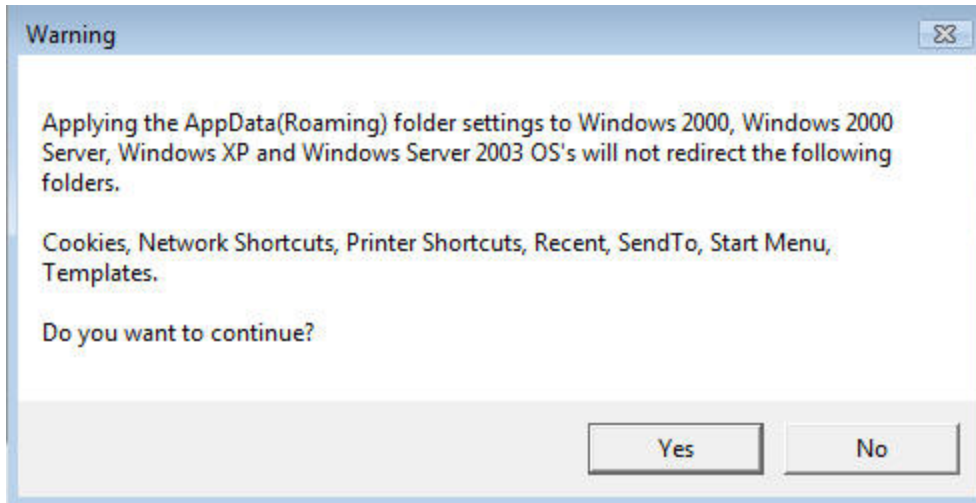


Figure 8.14. Vista's compatibility warning message for the AppData folder.

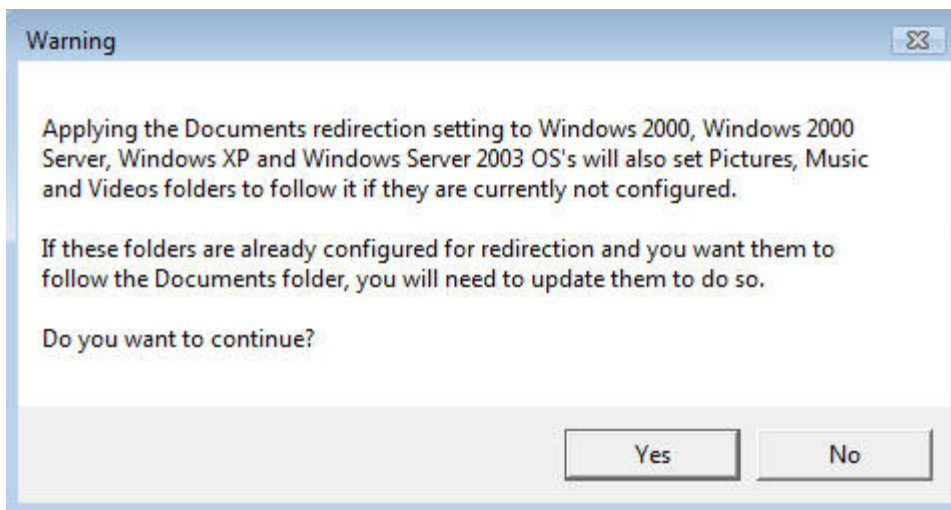


Figure 8.15. Vista's warning message for the Documents folder.

Finalizing the Personality Protection Strategy

Take the time to preserve what makes your users feel successful and comfortable in doing their jobs and it will pay dividends. When mapped drives are restored, printers appear just as they did previously, and data, shortcuts, and favorites are exactly as the user left them, the focus of the user shifts toward learning the benefits of their new hardware and operating system. You can spend less time training users on how all the old features in Windows XP are still in Vista and focus instead on more advanced topics such as new multi-tasking features, advanced searching and using new peripherals.

In addition, if you take the time to prepare a proper long term protection policy through folder redirection, you'll also be ready for the next migration when it comes along. Make this a smart profile protection policy!

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.