# Recommendations for Folder Redirection

To get the best performance from Folder Redirection, it is recommended that you: create the root share on the server and let the system create the users' folders, synchronize files at logoff when you use Folder Redirection with Offline Files, and use the following guidelines for redirecting **My Documents**, and setting options for Offline Files.

## Letting the system create folders for each user

For optimal performance of the Folder Redirection feature, it is strongly recommended that you create *only* the root share on the server, and then let the system create the folders for each user. If you must create the folders for users, ensure that you correctly assign permissions. For more information about assigning permissions see "Security Recommendations for Folder Redirection" later in this chapter.

Important

- If you must create folders for users, make sure that you set the correct permissions. Then, clear the **Grant exclusive rights to** check box on the **Settings** tab of the **Folder Redirection Properties** page. If you do not clear this check box, Folder Redirection first checks preexisting folders to determine if the user is the owner. If the administrator previously created the folder, the check fails, and redirection is cancelled. Folder Redirection logs an event in the Application event log indicating that redirection failed and that the new directories for the redirected folder cannot be created due to not being able to assign a security ID as the owner of the folder (Event ID 101).

## Accepting the default settings for Folder Redirection

If you are storing roaming user profiles on the server where you have enabled Offline Files, Folder Redirection ensures that Offline Files are set to synchronize when the user logs on and logs off.

For Windows 2000 and earlier clients, if you are using Offline Files in conjunction with Folder Redirection and roaming user profiles, it is recommended that you leave the default setting of synchronizing Offline Files at logoff enabled to ensure best performance of these features. This is because if a shared folder is unavailable, Offline Files considers the entire server to be unavailable until the offline cache is manually synchronized. Roaming profiles are *not* synchronized with the server while Offline Files treats the server as being unavailable. For clients that run Windows XP or later, whether the default synchronization setting is selected or not, roaming profiles continue to roam even if Offline Files has marked the server as being offline.

## Using offline files settings

Using offline files settings on a server share where the user data is stored is especially useful for users of portable computers. It is recommended that you use Folder Redirection in conjunction with Offline Files. Table 7.10 lists the recommendations for Offline Files.

**Table 7.10 Recommendations for Configuration of Offline Files**

| Redirected Folder | Recommended Offline Files Settings |
|---|---|
| My Documents | **All files and programs that users open from the share will be automatically available offline** *or* **Only the files and programs that users specify will be available offline** (if you want users to manually designate files and folders to be available offline). |
| My Pictures | **All files and programs that users open from the shared folder will be automatically available offline** *or* **Only the files and programs that users specify will be available offline.** |
| Application Data | **All files and programs that users open from the share will be automatically available offline.** |
| Desktop | **All files and programs that users open from the share will be automatically available offline** if the desktop is read only. |
| Start Menu | **All files and programs that users open from the share will be automatically available offline**. |

## Redirecting My Documents

The following suggestions for redirecting the My Documents folder are appropriate for most deployments and can provide a faster and simpler deployment.

- Redirect My Documents to a network share.
- Allow Folder Redirection to create folders for you. When setting redirection policy for a group, use the path to the share, such as *server**share*. Folder Redirection then appends the user name and the folder name when the policy is applied.
- Allow Folder Redirection to perform all the moving of folders and files when you select a folder for redirection or change the target network share to which you redirect the folder. The Folder Redirection client not only moves files to the appropriate network share, but it also sets proper folder security and renames entries in the Offline Files cache database so that they continue to link to the correct target folders and files. Any files pinned by the user in the Offline File Cache stay pinned.
- Combine Folder Redirection with Offline Files to provide the user access to My Documents, even when the user's workstation is temporarily disconnected from the network. This is particularly useful for people who use portable computers. For more information, see "Make a file or folder available offline" in Help and Support Center for Windows Server 2003.
- Include redirected folders, particularly **My Documents**, in routine server backups. Performing backups of user data that is located on network shares is simpler and more reliable because it requires no action on the part of the user or interaction with the workstation.
- Use Group Policy to set profile quotas and disk quotas to establish limits on the disk space that is used by users' data and settings.
- Redirect user-specific data from the hard disk that holds the operating system files. This data can be redirected to a different hard disk on the user's local computer or to a network share. This simplifies system maintenance by separating system files from user files.
- Centralize storage on large shares to reduce workstation hardware and maintenance costs. Pooling disk space more than offsets the cost of increasing server disk capacity.
- Do not use the **Redirect to home folder** policy setting unless you have already deployed home folders in your organization.
- Leave the **My Pictures** folder located in the **My Documents** folder.

When you redirect the **My Documents**, the Recycle Bin size for **My Documents** defaults to a percentage of the size of the server partition where the redirected **My Documents** resides. You can manually change this size in 1 percent increments. Because a Recycle Bin can grow large, encourage users to empty their Recycle Bins periodically.

Note

- You can grant users exclusive rights to their redirected folders. Select the **Grant the user exclusive rights to My Documents** check box under the **Settings** tab in each folder's **Properties** dialog box to grant full control over the folder to the user and the local system only.

### Redirect folders to home folders

Typically, it is recommended that you do *not* redirect to a home directory unless you have already deployed home directories in your organization. However, if you have home directories and want to transition your users to use **My Documents** while maintaining compatibility with the home directory environment, you can redirect a user's **My Documents** folder to the user's home folder. The **Redirect to home folder** policy setting is intended *only* for organizations in which home folders are already in place. Redirect only the **My Documents** folder to the home folder. For this type of redirection, the client computer must run one of the following operating systems: Windows XP Professional, Microsoft® Windows XP, 64-Bit Edition, or Windows Server 2003. This redirection option does not work for clients that run Windows NT, Windows 2000, or Microsoft® Windows® XP Home Edition.

When a folder is redirected to the home folder, security and ownership are not checked, and permissions are not changed. Folder Redirection behaves as though the administrator has set directory security correctly. This relaxed security is the reason that redirection to the home folder is not recommended if the home folder structure is not already in place, and you have not updated your configuration.

Typically, folder redirection fails if a user is not the owner of the folder to which the **My Documents** folder is redirected. Because redirection to the home folder is intended for an earlier environment, Folder Redirection does not check for proper folder ownership. Instead, ownership check is left to the administrator.

Users must have the home folder property set correctly on their user object in Active Directory. The client computer gets the path for the user's home folder from the user object in Active Directory when the user logs on. User accounts that have redirected folders must have this path set correctly, or Folder Redirection fails.

For more information about creating home folders for profiles, see "Add a home folder to a profile" in Help and Support Center for Windows Server 2003.

### Combining Folder Redirection with Offline Files

The Offline Files technology applies to network shares or mapped drives that contain documents or data that a user might want to use offline. Folder Redirection and Offline Files are functionally independent but complementary in operation.

Folder Redirection provides user access to redirected folders that have been relocated to network shares. Offline Files provides the user with access to any specified folder or file when the network share is unavailable, or offline.

### Redirecting the Start Menu folder

Folder Redirection of the **Start** Menu folder is available in Windows XP, Windows XP 64-Bit Edition, or Windows Server 2003 operating systems. **Start** Menu redirection is treated differently from other redirected folders in that the contents of the user's **Start** Menu are not copied to the redirected location. It is assumed that a redirected **Start** Menu has been previously created by an administrator and that all users share the same **Start** Menu. As a best practice for Windows XP–based computers, do *not* use Folder Redirection to redirect the **Start** Menu folder; instead, use Group Policy to control what appears on the **Start** Menu.

### Redirecting application data and use of Outlook

If a user redirects the **Application Data** folder and runs multiple instances of the Microsoft Outlook messaging and collaboration client on different computers, including an instance of Microsoft® Outlook 2000, mail opening performance is delayed. Outlook 2000 continually keeps the Outcmd.dat file open. (This file stores information about toolbar customizations that users make in Outlook.) When another instance of Outlook tries to access Outcmd.dat, it is unable to access it because Outlook 2000 has locked the file. The second copy of Outlook repeatedly tries to access Outcmd.dat, causing a delay when the user tries to open or reply to messages.

Note

- Outlook *2002*, included in Microsoft® Office XP, does *not* hold the Outcmd.dat file open. This behavior occurs *only* when Outlook 2000 is running on one of the computers.

### Encrypted file system considerations

Folder Redirection has implications for encrypted files that are located in redirected folders.

- Files redirected to a server can be encrypted by Encrypting File System (EFS) *only* if an administrator has designated the remote server as *trusted for delegation*. Administrators can establish a service or computer as trusted for delegation to allow that service or computer to complete delegated authentication, receive a ticket for the user who makes the request, and then access information for that user.
- Encrypted files are decrypted before being transmitted over the network. File encryption only protects the files while they reside on the disk.
- The Offline Files cache cannot be encrypted on Windows 2000 Professional.

For more information about delegating trust and enabling delegated authentication, see "Designing an Authentication Strategy" in *Designing and Deploying Directory and Security Services* of this kit.