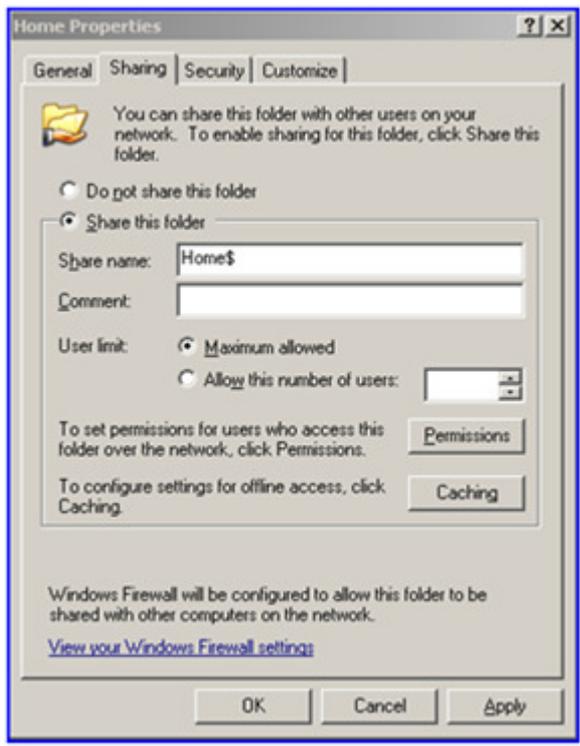**Home directory:**

Home folders are created automatically when the user's account is created and an administrator has enabled the use of home folders. You change the home folders for the user afterwards, but we are all about making the Admin's life easier.

Create the folder and enable sharing

As you can see we create the share name and added a dollar sign ($) to the end.

Next, we'll configure the share permissions. It is important to note that there is a difference in the default permissions for a share between Windows NT/Windows 2000 and Windows Server 2003. By default, Windows 2000 gives the Everyone group Full Control permissions. Windows Server 2003 gives the Everyone group Read permissions. However, we'll change this to:

Administrators: Full Control
System: Full Control
Authenticated Users: Full Control
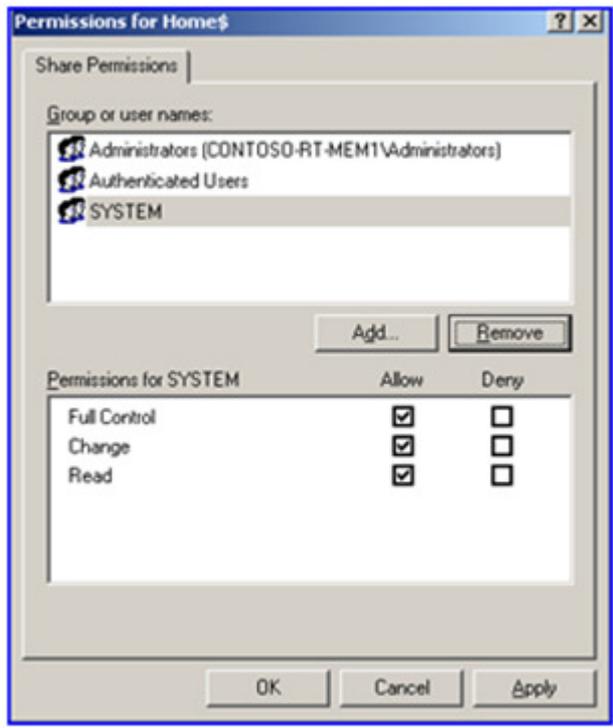
If you expect or want users to be able to select their home directory to be available while they are not connected to the network (also known as **Offline Files**), then you'll want to make sure you turn on Offline file caching of the HOME$ share. You do this by:

1. Click **Offline Settings** on Windows 2000 or **Caching** on Windows Server 2003 or later, which is located on the **Sharing** tab.
2. Click **Only the files and programs that users specify will be available offline**. If you would like more information on the different options and what they mean you can click **here**.
3. Then click **OK**.

NOTE: You should consider configuring Offline Files settings even if you do not want users to work with files while they are not connected to the network—you'll want to disable Offline Files by clicking **Files or programs from the share will not be available offline**.

Configuring NTFS Permissions

Now we need to configure the NTFS permissions, so we need to be on the "Security" tab of the folder we created earlier.

1. Turn off inheritance on the folder and copy the permissions. You do this by:

a. Click the **Advanced** button found on the **Security** tab.
b. Clear **Allow inheritable permissions to propagate to this object** check box in the **Advanced Security Settings** dialog box.
c. Click **Copy** when prompted by the Security dialog box.

2. Click **OK** to return to the **Security** tab. Ensure we have the following permissions set:

Administrators: Full Control
System: Full Control
Creator Owner: Full Control
Authenticated Users: Read & Execute, List Folder Contents, Read

3. Change permissions for Authenticated Users so they cannot access other users' folders. You do this by:

a. Click **Advanced** on the **Security** tab.
b. Click Authenticated Users, and then click **Edit**.
c. On the **Permissions Entry for HOME** dialog box, drop down the Apply **onto** and select **This folder only**.
d. Click **OK** twice.

Here is a screen shot of this step:
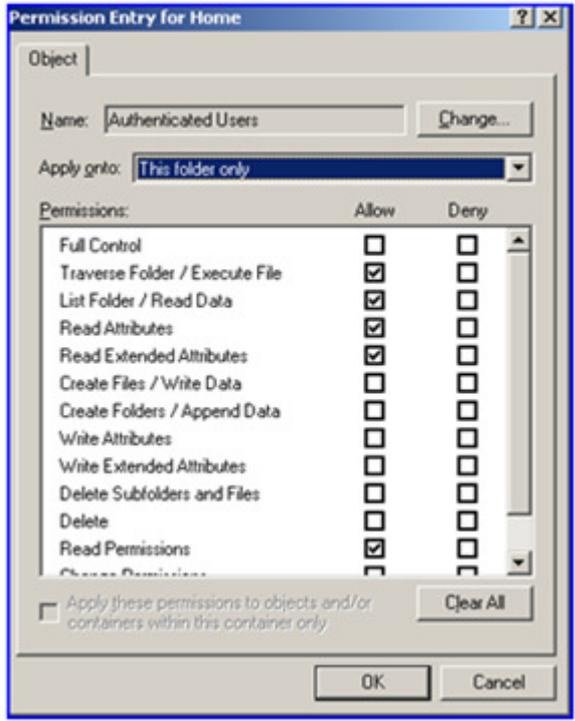
We now have the permissions configured properly. Next, let's create a user and specify the home folder location. This is done by going to the **Profile** tab of the user account in **Active Directory Users and Computers.** In the following screen shot shows an example of a drive mapping.
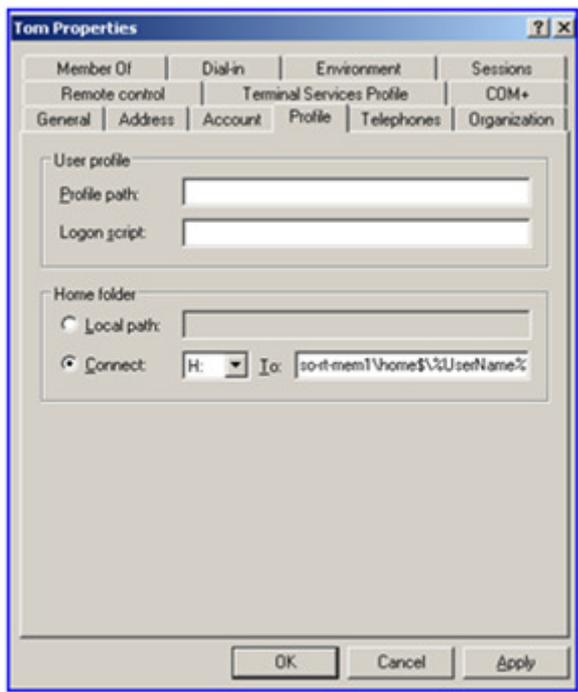
Yep, the **TOM** folder got created without a problem:
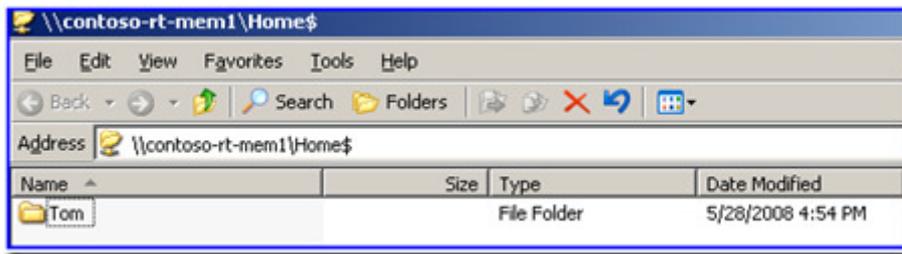
When we look at the permissions of the **TOM** folder we see the following:
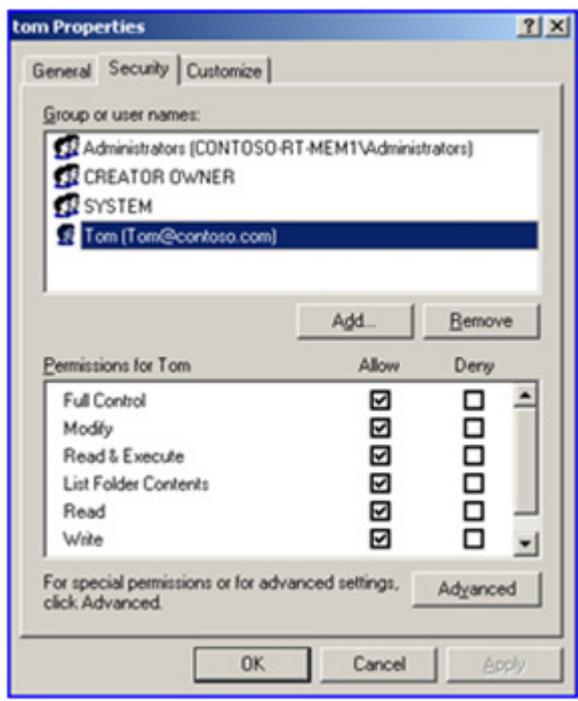
We see that only **Administrators**, **System**, **Tom**, and **Creator Owner** have permissions to the folder. Other users do not.

Roaming Profile:
Configuring roaming profiles uses the same procedure as the home folder share, except for one difference. You should disable Offline Files and you should always hide the profile share using a dollar sign ($).

Since the setup is pretty much exactly the same (except for the share name) so I'm not going to bore you with the same steps as earlier.

The main difference between the roaming profile folder and the home folder is that the roaming profile folder is not created until the user logs on and then logs off. Windows creates the profile directory and copies the profile to the share once the user has completed one successful logon and logoff.

You configure the profile location on the **Profile** or **Terminal Services Profile** tab within Active Directory Users and Computers. Type a UNC path to where Windows should create the user profile. The following screen shot gives you an example a user account configured with a profile path.
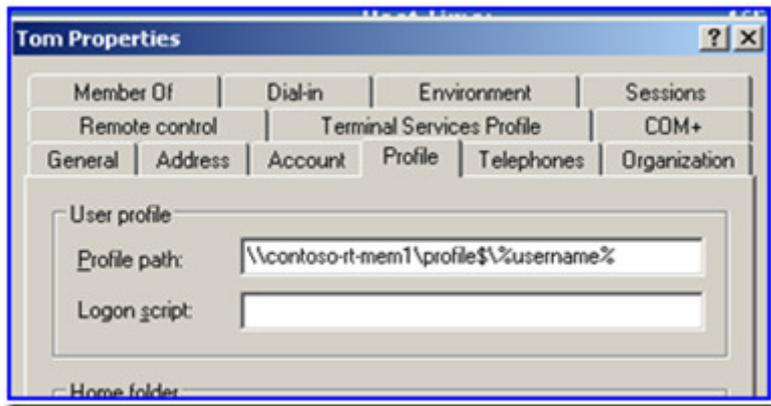
Folder Redirection:

For the most part the share and NTFS permissions are the same as the Home folder configuration except we need to replace Authenticated Users with the Everyone group. This is required for Windows to automatically create the redirected folders. These two KB articles provide more information:

291087 Event ID 101 and Event ID 1000 Messages May Be Displayed When Folder
http://support.microsoft.com/?id=291087
274443 How to dynamically create security-enhanced redirected folders by using
http://support.microsoft.com/?id=274443

Create the folder and enable sharing

So, we need to create a folder on a file server and enable it for sharing, again I would recommend that you hide the share using the dollar sign ($) at the end of the share name.

If you expect or want users to be able to select their home directory to be available while they are not connected to the network (also known as **Offline Files**), then you'll want to make sure you turn on Offline file caching of the HOME$ share. You do this by:

1. Click **Offline Settings** on Windows 2000 or **Caching** on Windows Server 2003 or later, which is located on the **Sharing** tab.
2. Click **Only the files and programs that users specify will be available offline**. If you would like more information on the different options and what they mean you can click **here**.
3. Then click **OK**.

We will also need to set the following permissions for the share:

Administrators: Full Control
System: Full Control
Everyone: Full Control
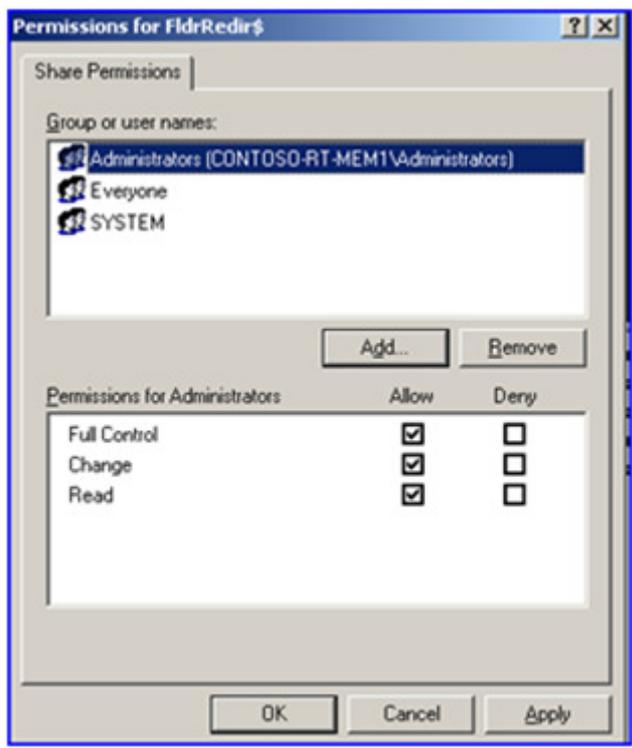
Configuring NTFS Permissions

We need to configure NTFS permissions for the newly created folder. You'll want to remove inheritance from this folder, as we did when configuring home folders.

1. Turn off inheritance on the folder and copy the permissions. You do this by:

a. Click the **Advanced** button found on the **Security** tab.
b. Clear **Allow inheritable permissions to propagate to this object** check box in the **Advanced Security Settings** dialog box.
c. Click **Copy** when prompted by the Security dialog box.

2. Click **OK** to return to the **Security** tab. Ensure we have the following permissions set:

Administrators: Full Control
System: Full Control
Creator Owner: Full Control
Everyone: Read & Execute, List Folder Contents, Read

3. Now we need change the permissions a bit for "Everyone" so that they do not have any permission to other users' folders. This is done by doing the following:

a. Click **Advanced** on the **Security** tab.
b.Click **Everyone**, and then click **Edit**.
c. On the **Permissions Entry for FldrRedir** dialog box, drop down **Apply onto** and select **This folder only**.
d. Click **OK** twice.

Here is a screen shot of this step:
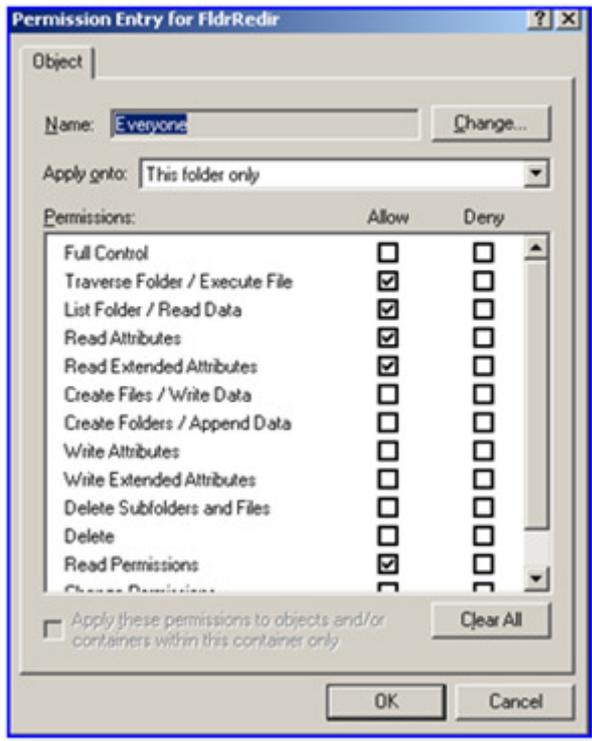
4. Configuring Folder Redirection settings within Group Policy:

a. Use the Group Policy Management Console (GPMC) and edit the GPO containing the Folder Redirection settings you want modified. Configure each from the following list to use the **Basic – Redirect everyone's folder to the same location** Folder Redirection setting. Type the UNC path listed in the table into the Root Path setting for each folder listed in the following table.

Redirected Folder	UNC Path
Application Data	\\contoso-rt-mem1\FldrRedir$
Desktop	\\contoso-rt-mem1\FldrRedir$
My Documents	\\contoso-rt-mem1\FldrRedir$
Start Menu	\\contoso-rt-mem1\FldrRedir$

Here is a screen shot of Application Data being redirected:
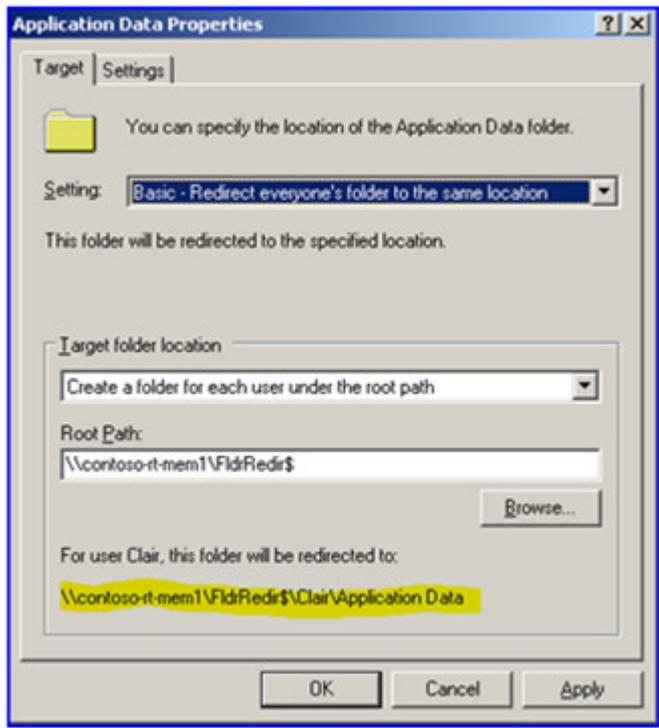
You can see that Windows shows you the entire path used for the Folder Redirection. So although we didn't specify the user's name in the **Root Path,** the redirection example shows the folder path as: \\contoso-rt-mem1\FldrRedir$\Clair\Application Data

b. By default, Administrators do not have permissions to users' redirected folders. If you require the ability to go into the users folders you will want to go to the "Settings" Tab, and uncheck: "Grant the user exclusive rights to" on each folder that is redirected. This allows Administrators to enter the users redirected folder locations without taking ownership of the folder and files.
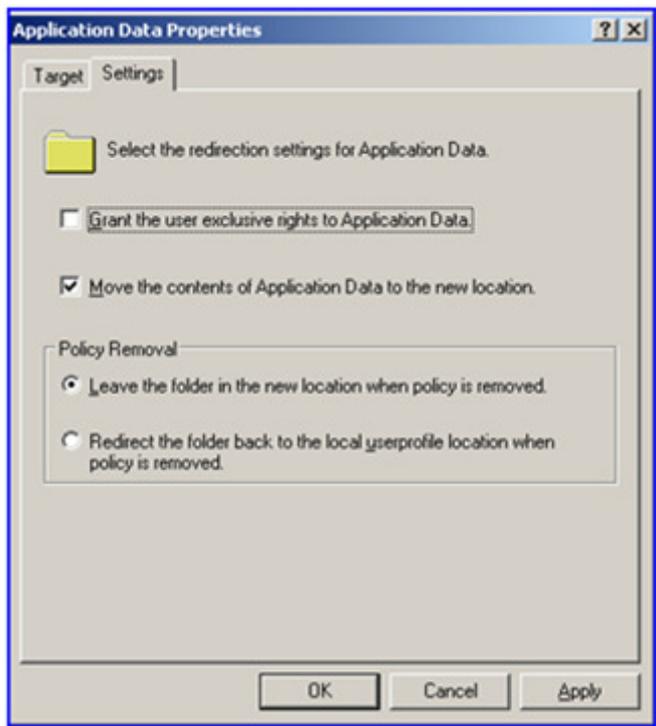
When you're all done, you can kick back and enjoy the easy life of being an administrator. Now when you create the user and define the home path it will create the user's home folder immediately. When Group Policy applies Folder Redirection; folders are created automatically. And, when the user logs off their roaming profile folders will be created after the first logon.

This last part is for the former Novell Admins out there. Yes, you could use **Access Based Enumeration (ABE)** on these new shares; however if there is going to a lot of user folders on any one of these shares you could experience degradation of performance. Enabling ABE on a share does come at a price of performance. If you are still all hyped up to enable this feature please read ABE whitepaper available information so that you make an informed decision.