**Folder Redirection Setup Guide**

2011-07-22

Michael Spence

**Audience:**

Field Support and Systems Administrators

**Preamble:**

This document describes the methods used to setup a Folder Redirection setup for My Documents and Desktop.

The acronyms, DLR or dlr, within this document are aliases for the desired dealership code as defined in the "Standard Naming Conventions" document.

**Steps to be followed:**

1. Active Directory Security Group

a. Parent Group

b. Dealership Group

2. Server Share Group

a. Share Creation

b. Share Securities

3. Group Policy Setup

4. Changing Users

a. Assigning to Security Group

b. Potential Features

**Steps in Detail:**

**1. Active Directory Security Group**

For the APEagers environment, the Folder Redirection setup is controlled by Security Groups.

**1.a. Parent Group**

The security group "Folder Redirection Parent Group" is the group which causes the Folder Redirection group policy to be activated for a user. All dealership Folder Redirection groups are members of this group. Users assigned to this group will not get Folder Redirection as this is not the method used for configuring Folder Redirection under this setup; users must be assigned to the dealership Folder Redirection group.

**1.b. Dealership Group**

Each dealership has its own unique security group for the purpose of Folder Redirection. The standard naming convention for a dealership Folder Redirection group is:

\_DLR Folder Redirection

As recommended in other documentation, this group should be placed in the Control OU for that dealership:

\_DLR Control

**2. Server Share**

The configuration of the Group Policy to enforce Folder Redirection for a dealership requires the creation of a share, which may or may not be in the local network for the dealership. Specific securities must be assigned to this share for Folder Redirection to work correctly.

**2.a. Share Creation**

Each dealership using a particular server must have its own share created for use with Folder Redirection. Using recommended specifications for the server being dealt with, create a folder for Folder Redirection in the appropriate location.

Now share this folder, using a share name which follows the following formula:

dlr.users

Edit the permissions for this share and allow "Everyone" to have Full Control permissions to this share. Securities will take care of access to the share as detailed below.

**2.b. Share Securities**

As previously mentioned, specific securities must now be applied to the newly created share. The following table details the required groups to have access to the share and their required permissions:

**Group Name Permission**

\_DLR Folder Redirection Full Control

Domain Admins Full Control

Folder Redirection Parent Group ALL but Full Control

Assign these security options to the newly created share.

These steps have now created a share ready to be assigned to the group policy with the aid of the above created security group.

**3. Group Policy Setup**

In the existing APEagers domain there exists a Group Policy "My Documents Folder Redirection GP" (possibly this should be called "Folder Redirection GP"). This Group Policy controls all Folder Redirection for all users who are members of their respective dealership Folder Redirection security group.

Using the Group Policy Management tool, select the Group Policy. Now add the dealership Folder Redirection group to the list of groups which are Security Filtering this group to users.

To apply the destinations for the Folder Redirection, right click the GP and choose "Edit...". The Group Policy Object Editor tool will appear, from which the Folder Redirection options can be edited. Find the Folder Redirection settings under "User Configuration" -> "Folder Redirection".

When either "Desktop" or "My Documents" is selected, nothing is displayed. This is normal. To alter the configuration, right click on "Desktop" or "My Documents" and select "Properties". The displayed window will contain a list of the security groups applied to this GP.

Add the new security group and destination share to this list by pressing "Add...". Now type the security group name and UNC path into the options window supplied.

Be sure to repeat this step for the other type, either "Desktop" or "My Documents" and press "OK" to save all changes made. There is no "save" option such as exists in a word processor.

This has finalised the setup of the Folder Redirection system for the dealership. Testing should be performed prior to adding real users to this setup.

**4. Changing Users**

The following process applies to test users and real users of the dealership Folder Redirection share.

**4.a. Assigning to Security Group**

Users, who are to be configured for this Folder Redirection setup, are simply to be added to the security group created for this purpose. Users should not be members of more than one Folder Redirection group as this has been known to cause issues and temporary misplacement of data.

**4.b. Potential Features**

Windows is a clever system, or so the general populace is led to believe. In reality, it is just a program with interesting features with even more intriguing quirks. Some of these are evident in the issues surrounding Folder Redirection.

Active Directory user accounts ARE simply numbers. Each user is assigned a unique number according to some *random* process and all security references to that person throughout the network are referenced by that number.

Folders on the other hand ARE NOT referenced by numbers. Folders are assigned *tags*, which are literally *text* strings and all reference to them is done in plain and obvious text.

Folder Redirection is controlled by Windows on the user's computer, ONLY; it is simply configured by the Group Policy. When the Folder Redirection system creates a folder for a user, it creates a named folder with the same string as the user's login name. Windows then stores in the user's Registry entries an entry for the location of this folder.

Folder redirection changes this Registry entry when there is a change to the Group Policy controlling the user.

Knowing these facts, consider what happens under the following circumstances:

**4.b.i. User Name Change**

When a user's login name is changed in Active Directory, Windows on the user's computer still acts as if it is the same user; the security ID number HAS NOT changed. Due to this, the Registry entry which points to the user's Folder Redirection folders remains the same as the Group Policy has not changed with respect to the user. So similarly, the destination folder name DOES NOT change and the user continues to use a folder which NO LONGER MATCHES his login name.

**4.b.ii. Destination Deleted/Changed**

What if the user's destination Folder Redirection folder changes names, changes security or is deleted? In this case Folder Redirection, at login attempts to locate the folder and deems that the destination is MISSING. At this point, Folder Redirection creates a NEW folder where data is redirected to. This new folder has the current login name for the user.

NOTE: For this case, if the original folder is renamed to match the new login name the new destination will be *user*.APEAGERS

**4.b.iii. Folder Redirection Group Changes**

This feature is actually one of Folder Redirection's strengths, but it must be understood. At login, when the Folder Redirection setup for a user changes, Windows prepares a new location for the folder redirection as if it was newly configured. However, before it performs this, it notes that it already has a destination for Folder Redirection. Windows then verifies that this original location exists and is in the same state as it was previously. If this verification is positive, all information is then moved from the original destination to the new location. This move is VIA the user's computer, and if the user's documents are large, then this can take some time to complete.

NOTE: if this move IS NOT completed and the user reset the computer, the new location will be used from the next logon and old data will be ORPHANED.

**4.b.iv. User Deletion**

When a user is deleted from Active Directory, that user obviously can no longer log into the network. Hence, Windows will never again act upon the redirected folders. These folders are then considered to be ORPHANED. By examining the ex-user's parent folder (i.e. the one with the user name), the securities of this folder will display the security ID for the folder and NOT the user's display name as this display name is no longer resolved to the security ID number. This is the primary method used to determine if an unknown folder is still in use or not.

**4.b.v. User Removed from Group**

If a user is removed from a Folder Redirection group, the user no longer has use of the destination folders. Windows will notice the Group Policy change and then ensure that its local copy of the user's Desktop and My Documents locations is up to date and then remove the data from the original location. The user's registry is altered to reflect this change.