

Windows Server 2003

## Migrating GPOs Across Domains with GPMC

---

By Mike Treit, Microsoft Corporation

Published: June 2003

### Abstract

One of the key scenarios enabled by Microsoft Group Policy Management Console (GPMC) is the ability to copy Group Policy objects (GPOs) from one domain to another, such as migrating a GPO from a test domain to a production domain. This technical article explains how to move GPOs from one domain to another using GPMC and identifies some of the issues you might encounter. In addition, this article introduces various advanced options in GPMC that make the process easier.

### Introduction

This article discusses how to use the Group Policy Management Console (GPMC) to migrate Group Policy Objects (GPOs) from one domain to another.

Migrating a GPO that works in one domain to another domain requires some planning, but the basic procedure is fairly straightforward. There are, however, two aspects of GPOs that complicate the process:

- The data that comprises a GPO is complex and stored in multiple locations.
- Some data in the GPO can be domain-specific and may be invalid if copied directly to another domain.

The first problem is solved fairly transparently by GPMC—when migrating a GPO from one domain to another, GPMC ensures that all relevant data is properly copied.

To solve the second problem, GPMC uses migration tables that allow an administrator to update domain-specific data in a GPO to new values as part of the migration process. This only needs to be done if the GPO contains certain types of policy settings, details of which are addressed in the section, "Overview of Migrating GPOs."

Before looking at the details, it helps to understand the basic process of migrating one or more GPOs between domains.

### To Migrate GPOs between Domains

1. Identify the GPOs you want to migrate.
2. Note whether there is trust between the source domain and the target domain:
  - a. If there is trust, plan on doing a copy operation.
  - b. If there is no trust, plan on doing an import operation, or consider using the Stored User Names and Passwords utility in Windows XP to gain simultaneous access to both domains. This procedure is documented in detail in "[Administering Group Policy with the GPMC](#)", and will allow you to perform a copy operation even if the source and target domains do not have a trust relationship.
3. If necessary, create a migration table to handle security principals and Universal Naming Convention (UNC) paths in the source GPO that may need to be updated to new values in the target GPO. For further details, see the section, "Understanding Migration Tables."
4. If performing an import operation, do the following:
  - a. Back up the source GPOs to a file system location that will be accessible from the target domain.
  - b. Create new GPOs in the target domain for each backed-up GPO.
5. Perform the actual copy or import operation, specifying the migration table created in Step 3, if applicable.
6. Set any desired security filtering and delegation permissions on the new GPOs.
7. Link the new GPOs to the appropriate site, domain or organizational unit in the Active Directory® directory service. At this point, the new GPOs will be live and functioning in your environment.

The rest of this article focuses on the details necessary to make this process successful.

### Overview of Migrating GPOs

Let's address the basic problem of taking a GPO in a given domain and creating a new GPO that contains the same set of policies in a different domain. In the past, Microsoft did not provide any tools to help with this scenario, and it was not something that could be easily done by a Group Policy administrator.

GPOs are collections of policy settings that are used to create standard configurations for users and computers. You can think of a GPO as a kind of container that holds policy settings of many different types: registry policy settings, software installation policy settings, logon scripts, and so on.

What's so hard about copying a GPO? Although this collection of settings is logically a single entity, the data for a single GPO is stored in multiple locations and in a variety of formats; some data is contained in Active

Directory and other data (of various types) is stored on the SYSVOL share on the domain controllers. This means that copying GPOs is not as simple as taking a folder and copying it from one machine to another—you could not, for example, just write a batch file or even a moderately complex script to accomplish a safe and robust copy of a GPO.

In addition to the complex way in which GPO data is stored, certain policy data may be valid in one domain but be invalid in the domain that the GPO is being copied to. For example, Security Identifiers (SIDs) stored in security policy settings are often domain-specific. In addition, settings that contain UNC paths for folder redirection or software installation policies may not work properly if the data in the GPO is copied without modification to a different domain.

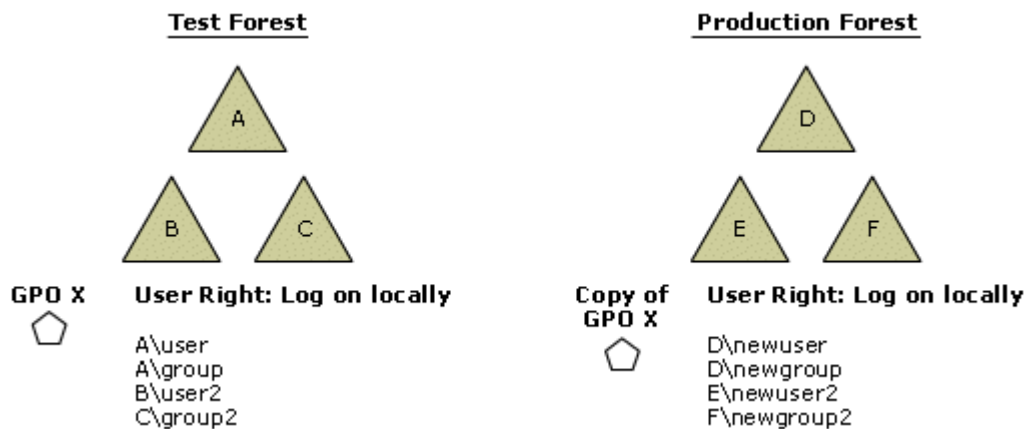
To clarify why certain policy settings can cause problems when copying GPOs from one domain to another, let's look at two common scenarios where a policy administrator would want to migrate some GPOs. These two scenarios are:

- Test-to-production migration.
- Production-to-production migration.

### Scenario: Test-to-Production Migration

In a test to production migration, we usually have two separate Active Directory forests—one for the production environment, and one for the test environment. The test forest is typically configured as a mirror image of the production forest, with no trust between the two.

Figure 1 illustrates migrating a single GPO from a domain in the test forest to a domain in the production forest.



If your browser does not support inline frames, [click here](#) to view on a separate page.

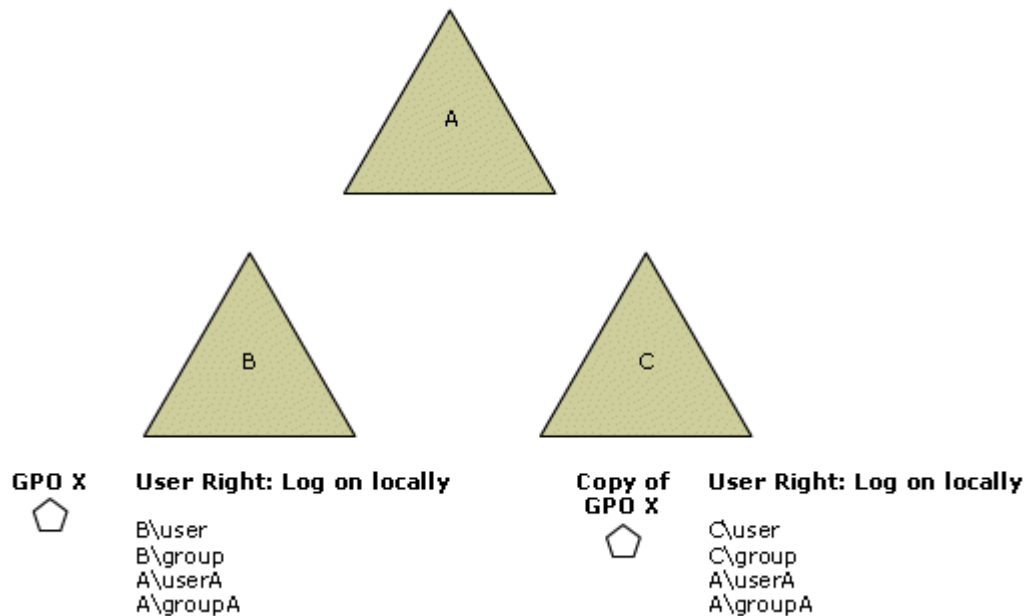
#### Figure 1 Migrating a GPO from test to production

In this case, we want to migrate a GPO called GPO X from Domain B in our test forest to Domain E in our production forest. In the process, we need to translate the settings for the **log on locally** user right configured in the GPO to map to new groups and users in the production forest, rather than the original test groups and users from our test forest.

Why is this necessary? In our test domain, the GPO stores information stating that certain groups, such as A\Group, have some specific rights in the domain. This data is stored as SIDs that are only valid in the test domain. If we copy those SIDs to the production domain when we migrate the GPO, the policy settings will refer to groups that do not exist, and will therefore be incorrect for the domain that the GPO was migrated to.

### Scenario: Production-to-Production Migration

Production to production migration occurs when you want to migrate a GPO from one production domain to another, typically within the same forest. Figure 2 illustrates this process.



If your browser does not support inline frames, [click here](#) to view on a separate page.

### Figure 2 Migrating a GPO between domains in production

In this case, we have copied GPO X from Domain B to Domain C. In the process, it makes sense to map some of the security principals referenced in the **log on locally** user right to new values more appropriate for the target domain. In this case, we would want to change Domain B to Domain C, but leave references to security principals in Domain A unchanged.

### Policy Settings That May Require Mapping

Not all policy settings in a GPO need to have values translated as part of the process of migrating from one domain to another. For example, Administrative Templates policy settings can be copied directly from one domain to another without needing to be modified.

There are two types of settings that often require modification as part of the migration process: security principals and UNC paths. We've already illustrated an example where security principals might need to be changed. UNC paths can also be an issue because servers in the original domain may not be accessible from the domain that the GPO is being migrated to.

The following settings contain security principals and can be updated during import or copy using a migration table, if required.

- Security policy settings of the following types:
  - User rights assignment.
  - Restricted groups.
  - System Services.
  - File system.
  - Registry.
- Advanced folder redirection policy settings.
- The GPO DACL, if you choose to preserve it during a copy operation.
- The DACLs on software installation objects, if any. These DACLs are only preserved if the option to copy the GPO DACL is specified.

The following settings can contain UNC paths, which might also need to be updated to new values as part of the migration process:

- Folder redirection policy settings.
- Software installation policy settings.
- Scripts (such as logon and startup) policy settings that reference UNC paths.

Note that security principals and UNC paths can be referenced in a handful of other settings not listed above,

such as in a few administrative templates settings. These settings cannot be mapped based on the data in the migration table, and will instead be copied as is. There are only a few settings that fall into this category.

## Using GPMC to Migrate GPOs

GPMC hides much of this complexity and provides simple and reliable mechanisms for performing operations such as copy and backup of GPOs.

There are four operations that GPMC provides to allow for archiving and recovery of GPOs, and for migrating GPOs from one environment to another:

- Copy
- Backup
- Import
- Restore

Each of these operations can be performed through the GPMC user interface, or through the GPMC scripting model.

For the purposes of this article, we are most interested in the operations that allow us to move GPOs across domains. This rules out the restore operation, which simply takes a GPO backup and restores it to the same domain that it was backed up from. You cannot restore a GPO from backup into a different domain than the one that the GPO originally came from. This is because restore is designed to put the GPO back exactly as it was, including using the same GUID and other information that is specific to the domain of the GPO.

So, the tools we have at our disposal for doing a cross-domain migration of GPOs consist of the Copy, Backup, and Import operations. Let's look at each of these in turn.

### Copy

A copy operation takes an existing, live GPO and copies it to the desired destination domain. A new GPO is always created as part of this process.

The destination domain can be any accessible domain in which you have the rights to create new GPOs, making it very easy to migrate GPOs among domains. Simply add the desired forests and domains to the GPMC console and use the GPMC user interface to copy and paste (or drag and drop) the desired GPOs from one domain to another. To add a forest to the console in GPMC, you must either have trust to that forest, or you can use the Stored User Names and Passwords utility in Windows. The procedure for using this utility in conjunction with GPMC is documented in detail in the GPMC white paper, and allows you to perform a copy operation even if the source and target domains do not trust one another.

When copying a GPO to another domain, you have the option of specifying a migration table if the GPO contains security principals or UNC paths that may need to be updated to new values in the target domain.

One additional option available when copying GPOs is the choice of whether to copy the Discretionary Access Control List (DACL) on the GPO in addition to the settings within the GPO. This is useful for ensuring that the new GPO that is created as part of the copy operation has the same security filtering and delegation options as the original GPO. If you choose the option to copy the DACL on the GPO, the DACL on any software installation objects in the GPO will also be preserved.

### Backup

The backup operation takes a live GPO and backs it up to the file system. The location of the backup can be any folder to which you have write access. After backing up GPOs, you don't interact with them directly through the file system—you need to use GPMC to display and manipulate the contents of your backup folder, either through the user interface or programmatically through a script. Once backed up, the archived GPOs can be processed by the Import and Restore operations.

Note that you can back up multiple GPOs and even multiple copies of the same GPO to the same location without any problems—GPMC uniquely identifies each backup instance and provides mechanisms to allow you to pick which copy of the archived GPO you want to work with. For example, you can choose to only display the most recent backups when viewing the contents of a backup folder through GPMC.

### Import

An import operation starts with a GPO backup in the file system and transfers the settings stored in that backup to a live GPO in the domain.

As with the copy operation, a migration table can be specified if settings in the GPO need to be updated to new values in the target domain.

Unlike the copy operation, a new GPO is not created as part of the import—you need to target a GPO that already exists. In addition, the DACL on the target GPO, as well as the DACL on any software installation

objects in the GPO, are never modified as part of an import operation.

## Understanding Migration Tables

GPMC supports migration tables that can be used when copying and importing GPOs. A good understanding of how migration tables work is essential to performing a successful cross-domain migration of GPOs.

A migration table is a simple table that specifies a mapping between a source value and a destination value. Conceptually, it looks like Table 1.

**Table 1 Migration Table Concept**

Type	Source Value	Destination Value
Global Group	TestDomain\Test Group	ProductionDomain\Marketing Users
UNC Path	\\TestServer\share	\\ProductionServer\share2

The purpose of these tables is to convert values inside a GPO to new values that will work in the target environment during the copy or import operation.

Consider a GPO that you have created in your test domain that you now want to move to your production domain. Let's say you created a security group in your test domain called Test Group that you used to test application of various security policy settings configured in the GPO. In your production environment, you have a real-world group called Marketing Users that you want to apply those same policy settings to. If you copy the GPO without modification, you will end up with the security policy settings affecting a non-existent group—Test Group—instead of the desired group—Marketing Users.

You might think that you could solve this problem simply by ensuring that you have security principals with the same name in both your test and production domains. However, most policy settings do not store just the name of the group—they store the unique Security Identifier (SID) instead, and the SID value is not going to match that of the security principal you really want to use in your target domain.

A similar problem exists with UNC paths. Let's say you set a folder redirection policy in your test domain that redirects everyone's My Documents folder to \\testserver\share. Let's assume that server is on the private network for your test domain and won't be accessible from your production domain. After you migrate the policy, your users will have their folders redirected to a server in your test domain that they don't have access to.

These are fairly simple examples; if you have configured multiple GPOs many complex settings, this problem can quickly grow much larger and make the migration process difficult.

With migration tables, you can automatically change the values at the time of the import or copy operation. In the example presented in Table 1, the import or copy operation would automatically look for policy settings that specify the global group TestDomain\Test Group and change them to ProductionDomain\Marketing Users, ensuring that the value in the target GPO will be correct for the domain it exists in. Similarly, any occurrence of policy settings with the UNC path \\testserver\share will be updated automatically to \\productionserver\share2.

## Migration Table Details

Migration tables are implemented as XML files and have a .migtable file extension. GPMC includes an editor for creating and modifying migration table files, called the Migration Table Editor, so you don't need to work directly with XML to create migration tables.

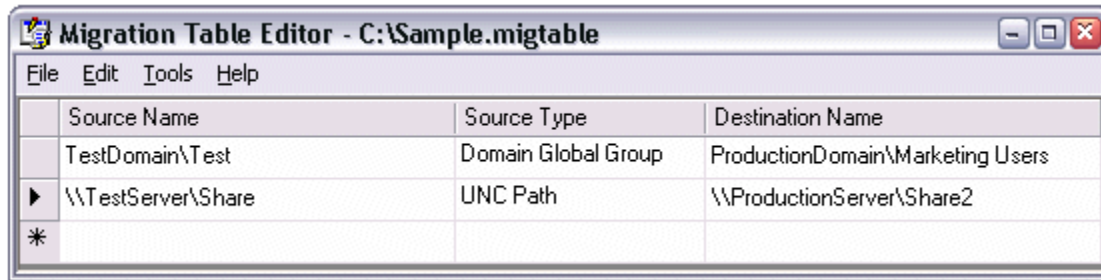
You can launch the editor by running `%programfiles%\gpmc\mtedit.exe`, or by right-clicking the **Domains** node or **Group Policy Objects** node in GPMC and selecting **Open Migration Table Editor** from the context menu.

To get an understanding of how migration tables work, take a look at the following file, installed with GPMC, which illustrates the structure and options available in a migration table:

```
%programfiles%\gpmc\scripts\SampleMigrationTable.migtable
```

You can open this file in the Migration Table Editor, or in a text editor such as Notepad, to view the underlying XML data.

The conceptual migration table that we looked at in Table 1 would look like the following when created in the Migration Table Editor:



Source Name	Source Type	Destination Name
TestDomain\Test	Domain Global Group	ProductionDomain\Marketing Users
▶ \\TestServer\Share	UNC Path	\\ProductionServer\Share2
*		

If your browser does not support inline frames, [click here](#) to view on a separate page.

### Figure 3 A sample migration table

For reference, the XML representation for this migration table is as follows:

```
<?xml version="1.0" encoding="utf-16"?>
<MigrationTable xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
  <Mapping>
    <Type>GlobalGroup</Type>
    <Source>TestDomain\Test Group</Source>
    <Destination>ProductionDomain\Marketing Users</Destination>
  </Mapping>
  <Mapping>
    <Type>UNCPath</Type>
    <Source>\\TestServer\Share</Source>
    <Destination>\\ProductionServer\Share2</Destination>
  </Mapping>
</MigrationTable>
```

In addition to direct mapping from one value to another, migration tables support several special destination options that can be used instead of specifying a new value. The following destination options are available:

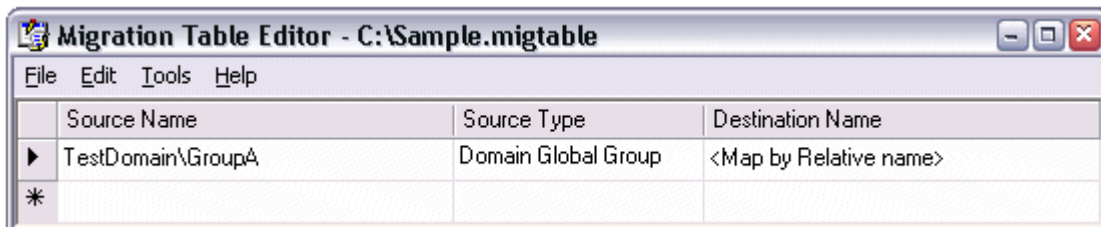
- Same As Source
- No Destination
- Map By Relative Name

The Same As Source option simply copies the value exactly as is. This is equivalent to not specifying this source value in the migration table at all, in which case the values are copied directly, without modification.

The No Destination option will remove the specified security principal from the GPO. This option can be used with security principals, but cannot be used with UNC paths.

The Map By Relative Name option allows you to map security principals by the same relative name. The relative name is the name of the principal without the domain part specified; if your group is called TestDomain\Group1, then Group1 is the relative name. When you specify this mapping option, GPMC will look for a matching security principal in the destination domain with the same relative name, and will replace any policy settings with the matching principal. The benefit of using the Map by Relative Name option is that it allows you to use one migration table to copy GPOs from this source domain to many other destination domains.

As an example, consider the following entry in a migration table:



Source Name	Source Type	Destination Name
▶ TestDomain\GroupA	Domain Global Group	<Map by Relative name>
*		

If your browser does not support inline frames, [click here](#) to view on a separate page.

### Figure 4 Mapping by relative name

If you are copying a GPO that has policy settings containing the SID for TestDomain\GroupA, you can simply create a security group in your destination domain called DestinationDomain\GroupA. Then when you specify a migration table with this entry, it will automatically change TestDomain\GroupA to DestinationDomain\GroupA

as part of the operation. Note that security group DestinationDomain\GroupA is not actually created during the migration operation, and therefore must exist prior to performing the operation.

You can also choose to use the migration table exclusively when performing an import or copy operation. With this option set, the operation will fail if there are any security principals or UNC paths configured in the GPO that are not also included in the migration table you specified. This option is useful if you want to ensure you accounted for every setting in the GPO that may need to be updated as part of the migration.

## Creating Migration Tables

Typically you will use the Migration Table Editor to create migration tables. GPMC supports the ability to auto-populate the relevant entries in your migration table from a set of GPOs or GPO backups. In the Migration Table Editor, simply click **Tools**, and then click **Populate from GPO** or **Tools**, and then click **Populate from Backup** to point to the GPOs or GPO backups you want to use. The security principals and UNC paths referenced in the selected GPOs or backups will be extracted and entered into the migration table. When using either of these auto-populate options, you also have the option to scan the DACL on the GPO for security principals.

Once the initial set of entries is created in the table, you can update the Destination Name field to the appropriate values.

In addition to the Migration Table Editor, a sample script, CreateMigrationTable.wsf, is included in the %programfiles%\gpmc\scripts folder and can be used to create and auto-populate a migration table from the command line.

For more information on using the Migration Table Editor, see the GPMC white paper and GPMC online Help.

## Putting It All Together

Now that you understand the difference between copying and importing GPOs, and the purpose of migration tables, let's look at a basic end-to-end example of how to use GPMC to take a GPO from a test domain and move it to a production domain.

Let's start with a test domain called "TestDomain.gpmcdemo.com" and a production domain called "ProductionDomain.adatum.com."

We have spent some time setting up and testing a new GPO configuration in the test domain. The GPO we created is called Marketing Folder Redirection and contains several advanced folder redirection policy settings which map users' My Documents and Desktop folders to different network shares, based on their security group membership. The GPO is linked to an organizational unit called Marketing.

The following table shows the details of the folder redirection policy settings we have configured in our GPO.

**Table 2 Folder Redirection Policy Settings in Test GPO**

Security Group	Folder	Redirect To
Marketing Users	My Documents	\\TestServer\TestShare\MyDocuments
TestGroup	Desktop	\\TestServer\RedirectedFolders\%UserName%\Desktop

In the production domain, a group already exists called Marketing Users, though it has a different SID than the group of the same name in our test domain. There is no group called TestGroup in the production domain, but there is a new group that has been created called Marketing Developers whose Desktop folder we want to redirect.

The server names are also different—in our production domain we have a server called ProductionServer instead of TestServer.

For the purpose of this scenario, we'll assume there is no connectivity between the test domain and the production domain. As a result, we will need to use an import operation, instead of a copy, to move the GPO from our test domain to production.

### Step 1 – Back up the GPO to a file system location

The first thing we need to do is back up the GPO to a file system location. We'll do that by launching GPMC from a machine in the test domain, navigating to the GPO Marketing Folder Redirection in the GPMC UI, right-clicking it and selecting **Backup**.

When the Backup GPO dialog box appears, we can specify the location where we want to back up the GPO, and can enter a description of the backup. After backing up the GPOs, we'll need to copy them to a server accessible from the production domain.

### Step 2 – Create a New GPO in the production domain

From a machine in our production domain, we'll open GPMC and create a new GPO by right-clicking the Group Policy Objects node and selecting **New**. We'll name the GPO "Marketing Folder Redirection".

### Step 3 – Create a migration table

We need to adjust some of the values in the GPO when we move it to the production domain. Specifically, we need to rename the server (to which we are redirecting folders) to ProductionServer and map TestDomain\TestGroup to ProductionDomain\Marketing Developers. We already have a matching group called Marketing Users in the production domain, so we'll specify the map by relative name option for this group. Alternatively, we could explicitly specify the destination group name in the migration table.

First, we'll create a migration table that we can then modify. To do this, we need to launch the Migration Table Editor by right-clicking on the **Domains** node in GPMC and selecting **Open Migration Table Editor**.

After the editor launches, we'll auto-populate the table based on the settings defined in the backup we created earlier. Here are the steps to auto-populate the migration table:

1. In the Migration Table Editor, click **Tools**, and then click **Populate from Backup**.
2. Enter the backup location used previously in the **Select Backup** dialog box.
3. Select the backup for the Marketing Folder Redirection GPO, and then click **OK**.

Before making any changes, save the migration table as MyTable.migtable on the local computer. Click **File**, click **Save**, and then enter MyTable as the file name.

### Step 4 – Edit the migration table

Now we need to edit the migration table and map all occurrences of \\TestServer to \\ProductionServer. To do that, we need to copy the text from the Source Name column and paste it in the Destination Name column for each UNC path entry, then edit the Destination Name column and replace TestServer with ProductionServer.

After that, we need to map TestGroup to the Marketing Developers group, and set the Marketing Users entry to map by relative name, since a group with the same name exists in our production domain.

Our final migration table should look like this:

Source Name	Source Type	Destination Name
TestGroup@TestDomain.gpmcdemo.com	Domain Global Group	Marketing_Developers@ProductionDomain.gpmc.demo.com
Marketing_Users@TestDomain.gpmcdemo.com	Domain Global Group	<Map by Relative name>
\\TestServer\TestShare\MyDocuments	UNC Path	\\ProductionServer\Share\MyDocuments
\\TestServer\RedirectedFolders\%UserName%\Desktop	UNC Path	\\ProductionServer\RedirectedFolders\%UserName%\Desktop
*		

If your browser does not support inline frames, [click here](#) to view on a separate page.

**Figure 5 Final migration table**

### Step 5 – Perform the import operation

At this point we should be set to perform the actual import operation, which will populate the new GPO we created with all of the policy settings from the GPO backup.

To do this, right-click on the GPO named Marketing Folder Redirection in GPMC and choose the **Import** option. This will launch the GPO import wizard, where we will specify the GPO backup and the MyTable.migtable migration table that we want to use.

After completing the wizard, the import operation will run. When it completes, we will have a fully populated GPO in our production domain—with the appropriate settings mapped to their new values based on our migration table. Table 3 shows the details of the folder redirection policy settings in the destination GPO, as a result of applying the migration table.

**Table 3 Folder Redirection Policy Settings in Production GPO**

Security Group	Folder	Redirect To
Marketing Users	My Documents	\\ProductionServer\Share\MyDocuments



Marketing Developers	Desktop	\\ProductionServer\RedirectedFolders\%UserName%\Desktop
----------------------	---------	---

## Step 6 – Configure any security filtering and delegation settings on the GPO

Once the import completes we need to evaluate if we want to filter the scope of the GPO using security group filtering or modify the list of who has rights to edit the GPO. For this scenario, we'll leave the GPO with the default set of permissions.

## Step 7 – Link the GPO to the relevant containers in Active Directory

The GPO has been created and populated with the folder redirection settings we originally configured in our test domain, but it isn't linked anywhere yet. We need to link it to the Marketing organizational unit in our Active Directory tree. To do this, we'll right-click on the Marketing organizational unit and select **Link an Existing GPO**. After finding the Marketing Folder Redirection GPO in the list and clicking **OK**, the GPO will be linked.

We have now successfully migrated our GPO from test to production. Of course, this GPO only had a few policy settings—but this procedure will work equally well with GPOs containing hundreds of settings, saving hours worth of time and energy manually re-creating and configuring GPOs.

## Summary

In this example we used the import operation because our test and production domains were isolated and did not have network connectivity. If we had connectivity between the two domains, we could have added both domains to GPMC and, after creating and editing our migration table, simply performed a drag and drop operation to copy the GPO.

Finally, it is worth noting that in many cases you will not have to use migration tables—if your GPO contains only registry policy settings, for example, there are no SIDs or UNC paths you will need to map and therefore a migration table does not need to be specified.

In addition, when creating copies of GPOs in the same domain, you generally can just make a copy in a single step—the only choice you have to make is whether to copy the DACL on the GPO.

## Larger-Scale Migrations

While copying or importing individual GPOs can work quite well for small-scale deployments or incremental updates, moving larger numbers of GPOs from test to production can be considerably more work.

Thanks to the scripting functionality in GPMC, you can write custom scripts to automate larger-scale migrations. GPMC includes several sample scripts that you can use to get started, all of which can be found at %programfiles%\gpmc\scripts on any computer where you have installed GPMC. Below are three sample scripts that are particularly useful for migrating GPOs across domains:

- **ImportAllGPOs.wsf.** This script will take all of the GPOs in a backup location and automatically re-create them in the target domain. You can specify a migration table when importing a single GPO, and the script takes care of re-creating the GPOs for you.
- **CreateEnvironmentFromXML.wsf.** This script will take an XML file representing a complete policy environment and re-create that environment from scratch. This includes creating the organizational unit tree, creating GPOs, importing settings into the GPOs from backups, linking GPOs to the correct organizational units, setting security filtering and delegation on the GPOs, configuring group membership, and so on. An /undo switch can be passed to the script to do the inverse, and delete the data specified in the XML file instead of creating it. This script can be a very useful and powerful tool for setting up and tearing down test environments.
- **CreateXMLFromEnvironment.wsf.** This script creates an XML file that is compatible with the CreateEnvironmentFromXML.wsf script. You can run this in your production domain to create an XML file and set of backups that represents that domain, then pass it to the CreateEnvironmentFromXML.wsf script in your test domain to completely re-create your production domain's policy infrastructure.

These scripts can be modified to suit your individual needs. See the GPMC SDK for details on scripting the GPMC object model. The GPMC SDK is located at %programfiles%\gpmc\scripts\gpmc.chm on any computer where you have installed GPMC.

## Related Links

For more information, see the following resources:

- [Administering Group Policy with the GPMC white paper](#)
- [Microsoft GPMC Web site](#)
- [TechNet Group Policy Center](#)

- [Windows Server 2003 Management Services](#)
- [Windows Server 2003 Web site](#)

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003. Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Version 1.1

---

[Send feedback to Microsoft](#)

[© Microsoft Corporation. All rights reserved.](#)