

# Chapter 8: GPO Replication

This chapter explains how to use the GPO replication feature of the **FAZAM 2000 Administrator** snap-in. GPO replication is an important tool in Cross-Forest Management.

## Replication Overview

---

When you replicate a GPO, you migrate the GPO's settings, OU links, and security filters to various domains across forest boundaries.

Features of GPO Replication include:

- **Wizard Interface:** To facilitate the process of GPO replication, FAZAM 2000 provides a simple, easy-to-use wizard interface.
- **Offline and Batch Modes of Operation:** Since GPO replication could be a time-consuming and traffic-intensive operation, you can replicate your GPOs as a batch job and execute the job offline. You can also save the replication job details as a file.
- **Replication Job Scheduling:** You can schedule offline batch replication jobs to whatever time is most suitable for you and your organization. The FAZAM 2000 GPO replication feature is integrated with Microsoft's Task Scheduler.
- **Cross-Forest Management:** You can create a single replication job that replicates GPOs from multiple source domains to target domains across forests.
- **Replication Log:** FAZAM 2000 logs every step of the replication process extensively into a replication log file. Administrators can troubleshoot by stepping through the log's Information, Warning, and Error messages.

### Prerequisites

In order to replicate a GPO, the following must be true:

- The domains into which you are replicating the GPO *must* have identical OU and security structures as the domains that contain the original GPO.
- The user account that is performing the replication *must* have Administrator access permissions, including the rights to:
  - create GPOs
  - link OUs
  - create and modify security filters and descriptors

### The Four Replication Categories

Replication is not a simple, “one size fits all” operation. Different replication situations can be summarized into four categories. It is helpful to understand the categories of GPO replication in order to complete the task successfully.

You can replicate GPOs across domains within one forest or across forests. You can run the GPO Replication wizard from the target domain or from a domain other than the target or source domain. When you combine these possibilities, you have the four GPO replication methods:

- Direct replication within the same forest
- Indirect replication within the same forest
- Direct replication across forests
- Indirect replication across forests

**Note**

Never run GPO replication from the source domain. Replication requires that read *from* another domain.

## Direct Intraforest Replication

A direct replication is one in which you run the GPO replication wizard from the target domain—the domain into which you are replicating.

When you directly replicate GPOs across domains within the same forest, you must run the wizard from the target domain with Domain Administrator permissions.

Figure 8-1 illustrates a direct replication within the same forest:

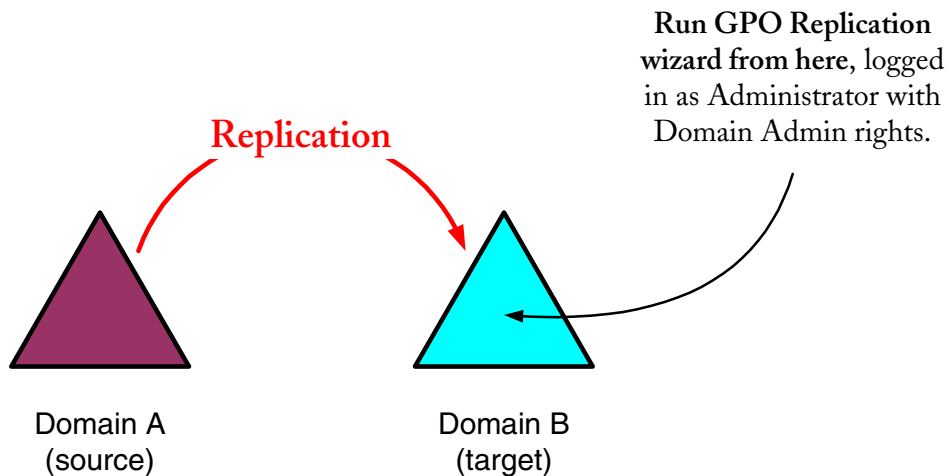


Figure 8-1: Direct Intraforest Replication

### Indirect Intraforest Replication

An indirect replication is one in which you run the GPO replication wizard from a domain that is neither a source nor a destination domain.

When you indirectly replicate GPOs across domains within the same forest, you must run the wizard from the target domain with Enterprise Administrator permissions.

**Note**

For indirect replications, FullArmor highly recommends you log into the root domain of the forest with Enterprise Admin permissions.

Figure 8-2 illustrates an indirect replication within the same forest.

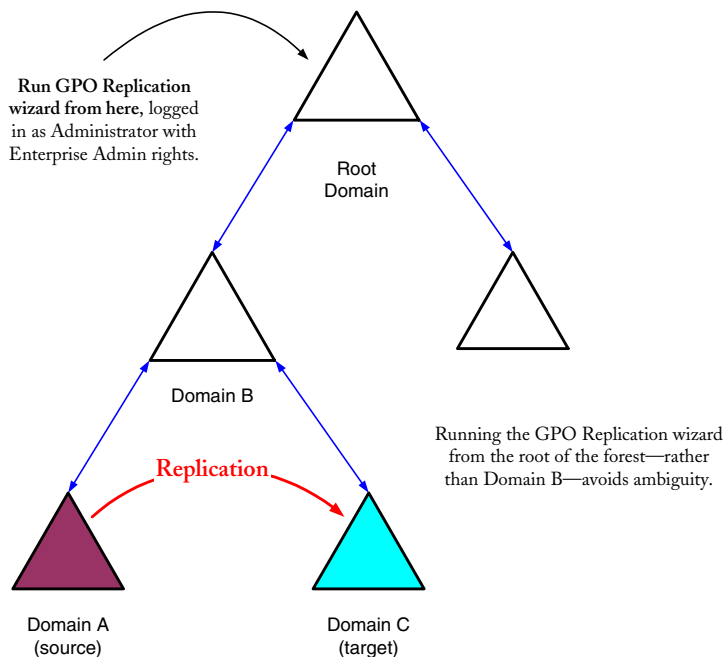


Figure 8-2: Indirect Intraforest Replication

## Direct Interforest Replication

A direct replication is one in which you run the GPO replication wizard from the target domain—the domain into which you are replicating.

When you directly replicate GPOs across forests, you must:

1. Have an existing explicit two-way trust between the source and target domains.
2. Run the wizard from the target domain with Domain Administrator permissions.

Figure 8-3 illustrates a direct replication across two forests.

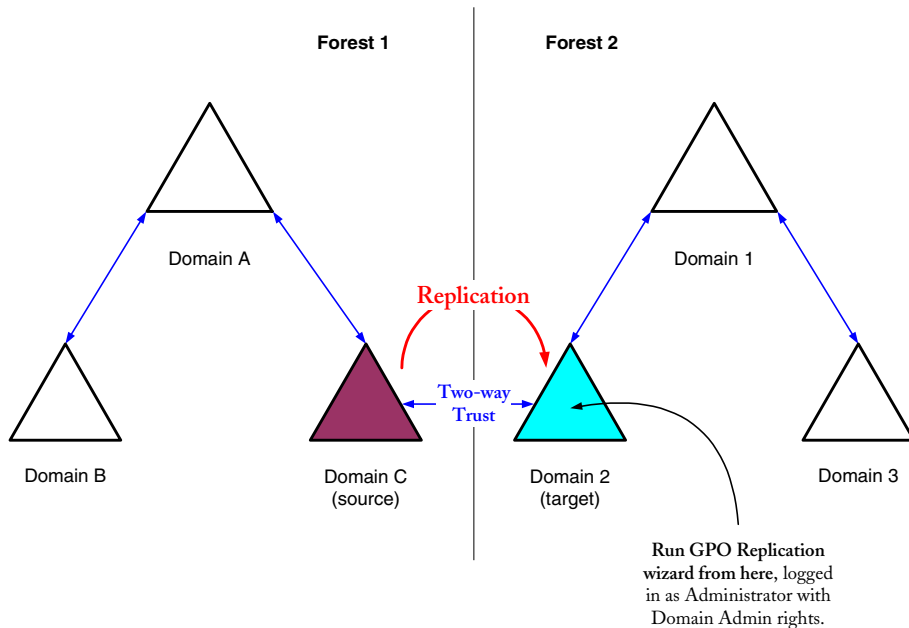


Figure 8-3: Direct Interforest Replication

### Indirect Interforest Replication

An indirect replication is one in which you run the GPO replication wizard from a domain that is neither a source nor a destination domain.

When you indirectly replicate GPOs across forests, you must:

1. Have an existing explicit two-way trust between the root domain of the target forest and *each* source domain in the source forest.
2. Run the wizard from the root domain of the target forest with Enterprise Administrator permissions.

Figure 8-4 illustrates an indirect replication across two forests.

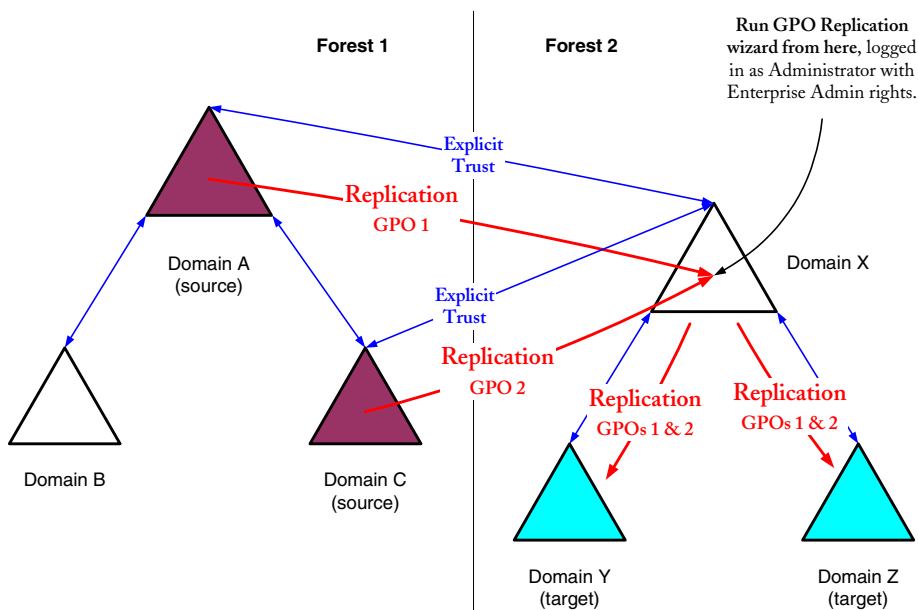


Figure 8-4: Indirect Interforest Replication

Figure 8-4 depicts the capability of the GPO Replication feature to select GPOs from multiple source domains and replicate them to multiple target domains in another forest.

**Note**

Whenever you replicate more than one GPO, whether they originate from one domain or several domains, all the GPOs are replicated into each of the target domains.

## Example scenarios

### *Scenario 1:*

An organization has set up a deployment plan consisting of three forests. The three forests constitute a typical Windows 2000 deployment environment in which an organization can safely create and test new GPOs without affecting normal productivity.

An organization uses the three forests as follows:

1. A “sandbox” forest, which consists of a set of domains that mirrors its production environment

When an administrator changes a GPO, the Windows 2000 server deploys the changes immediately. Everything linked to or associated with that GPO is automatically updated. To prevent a disaster in the production environment due to a simple mistake or oversight, the administrator can “play” with GPOs in the sandbox forest and not worry about the results of the changes or modifications.

2. A test forest, which also mirrors the production environment

After the administrator develops the GPOs, the administrator migrates the GPOs to a Quality Assurance or test environment. In order to create accurate tests and scenarios, the migration must include the GPO settings, along with its OU links and security filters.

3. The production forest, which consists of the set of domains the organization uses on a daily basis to conduct its business

After passing the test phase, the administrator migrates the GPOs to the production environment “as is,” just as they existed in the test environment. If any one setting or link or filter is different than that which was tested, the results could jeopardize normal business.

## GPO Replication

The FAZAM 2000 GPO Replication wizard makes the otherwise tedious and complicated process of migrating GPOs across domains and forests simple.

### Scenario 2:

After the initial deployment of Windows 2000 servers and clients across an organization, its daily administration tasks involve modifications to policy settings based on its business requirements.

The organization recognizes that an effective change and configuration management solution is required for managing changes to the group policies. Using a similar model to the three forests in Solution 1, the organization uses the GPO Replication wizard to publish the modifications to the GPOs to various domains in the enterprise.

## Replicate GPOs

The GPO Replication wizard is available in the **FAZAM 2000 Administrator** snap-in. When you select a domain node in the left pane, the wizard is available:

- As a taskpad icon in the right pane
- As an option when you right click on a domain node

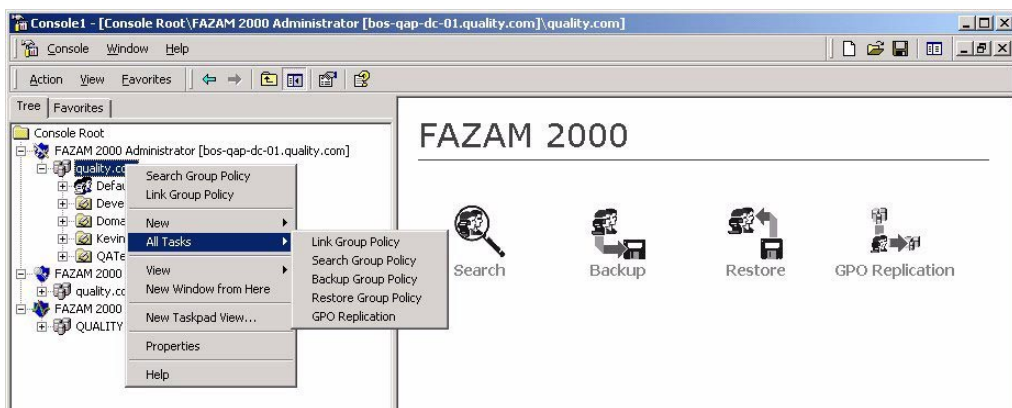


Figure 8-5: Selecting GPO Replication as a menu option or taskpad option