



Troubleshooting Group Policy in Microsoft® Windows® Server

Microsoft Corporation

Published: July 2003

Updated: November 2004

Abstract

This white paper helps you troubleshoot the most common problems affecting the deployment of Group Policy in a Windows Server 2003 or Windows Server 2000 environment.

To troubleshoot Group Policy, you need to understand the interactions between Group Policy and its supporting technologies (such as Microsoft® Active Directory® directory service and the File Replication Service), and the ways that the Group Policy objects themselves are managed, deployed, and applied. With that understanding, you can use specific tools to find answers to specific question to identify and resolve problems.

This white paper discusses the likely sources for problems with Group Policy application and administration, and suggests ways to identify the source of problems you might encounter. It also summarizes many of the tools (such as Group Policy Management Console and GPupdate.exe), log files, and other resources that you can use to troubleshoot problems with Group Policy. This white paper does not provide detailed information about Group Policy or its supporting technologies, but does refer you to sources for that information.

Microsoft® Windows® Server White Paper

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.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows 2000 Server, Windows Server 2003, and Windows XP Professional 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.

Contents

Group Policy Overview	1
Feedback on this Paper	1
Infrastructure Requirements	2
Windows 2000 or Windows Server Domain with Active Directory.....	2
Organizational Unit Membership and GPO Links	2
Network Connectivity and Configuration.....	2
Domain Name System	3
SYSVOL Share	3
Active Directory and File System Replication	3
Default Domain Policy GPO and Default Domain Controllers Policy GPO	3
Client Operating System	4
Understanding Group Policy Processing	5
Troubleshooting Group Policy Core Functionality	6
Flowchart for Troubleshooting Group Policy Core Functionality	6
Navigating the Troubleshooting Flowchart	7
GPO Applied, Policy Setting Listed	8
GPO Inheritance (Setting Listed)	9
Replication (Setting Listed)	9
Group Policy Refresh (Setting Listed).....	9
Asynchronous Application of Group Policy (Setting Listed).....	10
Client-Side Extension Issue (Setting Listed).....	10
Loopback Processing (Setting Listed)	10
GPO Applied, Policy Setting Not Listed.....	11
Replication (Setting Not Listed)	11
Group Policy Refresh (Setting Not Listed)	12
Lack of Operating System Support (Setting Not Listed).....	12
GPO Not Applied, Listed as Denied	12
Security Filtering (GPO Denied)	13
Disabled Link (GPO Denied).....	13
Inaccessible GPO (GPO Denied)	13

Empty GPO (GPO Denied)	13
WMI Filter (GPO Denied)	13
GPO Neither Applied nor Denied	13
Scope of Management (GPO Not at Client).....	14
Replication (GPO Not at Client)	14
Group Policy Refresh (GPO Not at Client).....	15
Network Connectivity (GPO Not at Client)	15
Details for Troubleshooting Core Group Policy Application Functionality	15
Network Connectivity	15
Troubleshooting.....	15
Slow links	16
Troubleshooting.....	16
DNS.....	16
Troubleshooting.....	16
Multi-homed computers.....	17
Missing or Corrupted Files.....	17
Troubleshooting.....	17
Replication Convergence.....	17
Troubleshooting.....	18
Group Policy Refresh.....	19
Troubleshooting.....	19
Trust Relationships	20
Troubleshooting.....	20
OU Memberships and GPO Linking	20
Troubleshooting.....	20
Adding a User or Computer to an OU	21
User Settings vs. Computer Settings	21
Troubleshooting.....	21
Security Filtering	22
Troubleshooting.....	22
Cached credentials	22
Troubleshooting.....	23

WMI Filtering.....	23
Group Policy Inheritance Rules	23
Troubleshooting.....	24
Migrating GPOs Between Forests.....	25
Troubleshooting.....	25
Loopback Processing	25
Troubleshooting.....	26
Details for Troubleshooting Client-Side Extensions	27
Operating System Support.....	27
Troubleshooting	27
Asynchronous Processing and Logon Optimization in Windows XP.....	27
Registry CSE.....	28
Scripts CSE.....	29
Software Installation CSE	29
Troubleshooting.....	30
Folder Redirection CSE	31
Troubleshooting.....	31
NTFS Permissions for Folder Redirection Root Folder.....	32
Share-Level (SMB) Permissions for Folder Redirection Share.....	32
NTFS Permissions for Each User's Redirected Folder	32
Troubleshooting Group Policy Administration	33
Domain Controller Selection in the Group Policy Object Editor and GPMC.....	33
Troubleshooting.....	33
Security	33
Troubleshooting.....	33
Exposing Preferences in Administrative Templates	33
Troubleshooting Tools.....	34
GPMC as a Troubleshooting Tool.....	34
Group Policy Results.....	34
To generate a Group Policy Results report:.....	34
Summary Tab.....	35
Table 2 Summary Tab of Group Policy Results Reports	35

Settings Tab	35
Policy Events Tab	35
Table 3 Policy Events Tab of Group Policy Results Reports	36
Group Policy Modeling	37
To generate a Group Policy Modeling report:	37
Viewing Active Directory Objects and GPOs	37
Scripting Built-in to GPMC.....	37
Other Group Policy Tools.....	38
GPRresult.exe	38
GPMonitor.exe	38
GPOTool.exe.....	38
Software Installation Diagnostics Tool (adddiag.exe)	39
Tools for Troubleshooting External Issues	39
Sonar.exe	39
Active Directory Support Tools.....	40
Other Windows Server 2003 Command-Line Tools.....	40
Appendix: Group Policy Log Files.....	41
Client Log Files	41
Table 4 Client Log Files for Troubleshooting Group Policy -	42
Server Log Files.....	43
Table 5 Server Log Files for Troubleshooting Group Policy	43
Appendix: Migrating from Windows NT 4.0.....	44
Table 6 Migrating from Windows NT 4.0: Group Policy Application	45
Appendix: Group Policy and Roaming User Profiles	46
Troubleshooting.....	46
Appendix: Resources.....	47
Feedback on this Paper	47
Newsgroups About Group Policy	47

Group Policy Overview

You can use Group Policy to manage the configurations on computers throughout networks with domains based on Microsoft® Windows® Server 2003 or Microsoft® Windows® 2000. You can also use Group Policy to meet service-level agreements. For example, you can make software available to users based on their security group memberships and other criteria and to enforce the organization's policies regarding computer usage.

Group Policy depends on several technologies in Windows Server 2003 and Windows 2000. These include Active Directory, Directory Name System (DNS), and File Replication Service (FRS). Group Policy is delivered to clients based on the placement of both the computer and the user account in the Active Directory hierarchy. In addition, Group Policy uses the security groups defined through Active Directory to determine whether policies are applied, as well as to control who can manage Group Policy in the organization. The interactions between Group Policy and its supporting technologies make Group Policy flexible. It is important to understand these interactions when troubleshooting Group Policy.

Before you work with Group Policy, you need a firm understanding of the interactions between Group Policy and its supporting technologies and the ways Group Policy objects themselves are managed, deployed, and applied. This white paper highlights some key points to keep in mind as you troubleshoot Group Policy problems. For detailed information about Group Policy and the various supporting technologies, see [Designing a Managed Environment](http://go.microsoft.com/fwlink/?LinkId=4755) (http://go.microsoft.com/fwlink/?LinkId=4755) in the *Microsoft® Windows® Server 2003 Deployment Kit*.

The Group Policy Management Console (GPMC) is the recommended tool for managing Group Policy. GPMC is also an excellent troubleshooting tool. If you have a licensed copy of Windows Server 2003, GPMC is available to you as a free download from the Microsoft.com Group Policy Home Page. It can be installed on any computer running either Microsoft® Windows Server 2003 or Windows XP Professional. The computer that runs Windows XP Professional must have Service Pack 1 or later and .NET Framework installed. You can use GPMC to manage Group Policy in domains based on Windows Server 2003 or Windows 2000. For more information, see [Introduction to Group Policy for Windows Server 2003](http://go.microsoft.com/fwlink/?LinkId=14958). (http://go.microsoft.com/fwlink/?LinkId=14958).

Feedback on this Paper

If you have any comments about this paper, contact <mailto:gpdocs@microsoft.com>.

Infrastructure Requirements

Problems with the application of Group Policy often involve the technologies on which Group Policy depends, or with easy-to-correct oversights in the implementation of Group Policy itself. This section provides a quick review of these dependencies and summarizes how they relate to troubleshooting Group Policy.

Windows 2000 or Windows Server Domain with Active Directory

Group Policy is not supported in earlier operating systems such as Microsoft® Windows NT® 4.0.

Windows NT 4.0 policies cannot be applied using Group Policy. If you are migrating from Windows NT 4.0 to Windows 2000 or Windows Server 2003, see [Migrating from Windows NT 4.0](#).

Your Active Directory structure should be designed with an understanding of Group Policy inheritance rules so that it can support your objectives for using Group Policy. For more information about how your Active Directory structure affects your Group Policy implementation, see [Designing a Managed Environment](#) (<http://go.microsoft.com/fwlink/?LinkId=4755>) in the *Windows Server 2003 Deployment Kit* and the white paper, “[Windows Server 2003 Group Policy Infrastructure](#)” (<http://go.microsoft.com/fwlink/?LinkId=14950>)

To use the loopback features of Group Policy, the computer must be in a Windows 2000 or Windows Server 2003 domain, as must the user. You cannot deploy Group Policy to users in a Windows NT 4.0 domain by applying loopback to a computer in a Windows 2000 or Windows Server 2003 domain.

Organizational Unit Membership and GPO Links

To receive the Group Policy objects that are created and stored at the domain level, the user or computer must be a member of a site, domain, or organizational unit (OU) that links to a GPO. Group membership is not the basis for Group Policy application, but is used to further restrict the application of the GPO – this is called *security filtering*. For more information about how your Active Directory structure supports your Group Policy implementation, see [Designing a Managed Environment](#) (<http://go.microsoft.com/fwlink/?LinkId=4755>) in the *Windows Server 2003 Deployment Kit*.

Network Connectivity and Configuration

For Group Policy to be received at the client, there must be network connectivity between the client and the domain controller. Several issues can affect network connectivity:

- TCP/IP is used as the transport for Group Policy, so TCP/IP must be implemented in your network. For more information about TCP/IP, see [Designing a TCP/IP Network](#) (<http://go.microsoft.com/fwlink/?LinkId=4707>) in the *Windows Server 2003 Deployment Kit*.
- If you use a firewall, be sure that Internet Control Message Protocol (ICMP) is enabled on the network. For more information, see “Internet Control Message Protocol (ICMP)” in Help and Support Center for Microsoft® Windows® Server 2003.
- A user who can log on with cached credentials might not be aware of a connectivity issue. For more information, see [Cached credentials](#) later in this paper.

- If a computer's clock is not synchronized with other clocks on the network, that computer can encounter a variety of problems, including authentication problems. Authentication problems can be masked if a user is able to log on to the computer with cached credentials. In this case, the user appears to have logged on to the network successfully but is unable to access system resources including Group Policy. To check for time synchronization issues, compare the time and date on the client with the time and date on other system resources. To avoid the problem, use the Windows Server 2003 Time Service to keep the computers on your network synchronized. For more information about clock synchronization and the Time Service, see "Windows Time Service" in Help and Support Center for Windows Server 2003.

Domain Name System

The client uses the fully qualified domain name to access the domain controller (including the SYSVOL share) when reading the GPO. In order for the client to obtain the fully qualified domain name, the Domain Name System (DNS) must be functioning.

If Group Policy settings that apply to that client require access to other network resources, the client-side extensions (CSE) to Group Policy might use DNS to locate those resources.

For best results, do not use host files with DNS. It is more efficient, more scalable, and less error-prone to configure DNS to work dynamically.

For more information, on DNS, see [Deploying DNS](http://go.microsoft.com/fwlink/?LinkId=4709) (<http://go.microsoft.com/fwlink/?LinkId=4709>) in the Microsoft® *Windows Server® 2003 Deployment Kit*.

SYSVOL Share

GPO information is stored in two locations. The Group Policy container (GPC) portion of the GPO is stored in Active Directory. The Group Policy template portion is stored in a file-based location under the SYSVOL folder on domain controllers. Clients must be able to access the SYSVOL folder and retrieve information from the Group Policy template in order to apply Group Policy settings.

For this reason, the SYSVOL share must be accessible to the client. If you suspect SYSVOL problems, first check replication issues, as described in "[Replication Convergence](#)" later in this paper.

Active Directory and File System Replication

Two types of replication are required: Active Directory replication and file system replication. Both must be functioning before you can deploy Group Policy. If Active Directory replication is working properly, but file system replication is not, you might have success when editing or managing Group Policy with Active Directory Sites and Services and with Active Directory Users and Computers, but the application of Group Policy to clients will fail. For more information, see "[Replication Convergence](#)" later in this paper.

Default Domain Policy GPO and Default Domain Controllers Policy GPO

Two default GPOs are installed when a domain is created – the Default Domain Policy and the Default Domain Controllers Policy. In general, editing the Default GPO's is neither necessary nor recommended, with the exception of some security settings that must be edited. If the settings in these default GPOs are incorrectly configured you might have problems with client authentication, directory replication, FRS, and other components. For example, if the default policies are damaged by deleting

the Group Policy template files or by modifying the settings in them so that they no longer function as designed, you need to restore them.

In Windows Server 2003 domains, you can do this by using Dcgpofix.exe, which is included with Windows Server 2003 operating systems. This tool restores these GPOs to their original settings. Any settings that have been added, including those added by applications such as Systems Management Server or Exchange that have been installed on the domain controller, will be lost. For more information, see “Dcgpofix” in Help and Support Center for Windows Server 2003. There is no tool for repairing the default policies in Windows 2000 domains, but you can repair them manually. For information on how to do so, contact Microsoft Product Support Services.

Client Operating System

Group Policy relies on client functionality that is built in to Windows 2000, Microsoft® Windows® XP Professional, and Windows Server 2003. If the client is running an earlier operating system, it cannot process GPOs and apply Group Policy settings. In addition, some settings are supported only on certain operating systems.

Windows XP and Windows Server 2003 provide Supported On information for each administrative template policy setting. This information is exposed when you use GPMC to view a report of GPO settings.

Understanding Group Policy Processing

Before discussing Group Policy troubleshooting, you need a general understanding of how Group Policy is processed at the client. Group Policy processing has two distinct phases: core Group Policy processing and CSE processing.

When a client begins to process Group Policy, it must determine whether it can reach a domain controller, whether any GPOs have changed, and what policy settings (based on client side extension) must be processed. The core Group Policy engine performs the processing this in this initial phase.

Policy settings are grouped into different categories, such as administrative templates, security, folder redirection, wireless, IPsec, EFS, and Software Installation. The settings in each category require a specific CSE to process them, and each CSE has its own rules for processing settings. The core Group Policy engine calls the CSEs that are required to process the settings that apply to the client.

This document focuses first on troubleshooting core Group Policy processing, and then on troubleshooting CSE processing.

Troubleshooting Group Policy Core Functionality

This section provides a structured approach to troubleshooting Group Policy core functionality. In Windows XP and Windows Server 2003, a mechanism called Resultant Set of Policy (RSoP) allows you to track the final set of processed policy settings. RSoP can also be used to track problems with the core Group Policy processing. GPMC provides an easy view into the RSoP data through its Group Policy Results tool. This section is based on the use of Group Policy Results reports to view and analyze RSoP data.

There are three main parts of this section:

- [Flowchart for Troubleshooting Group Policy Core Functionality](#) helps you quickly eliminate many of the possible causes of the problem, based on three questions that are easily answered from the Group Policy Results report.
- [Navigating the Group Policy Troubleshooting Flowchart](#) tells you where to look in the Group Policy Results report for the information referred to in the flowchart, and ties observed results to possible root causes.
- [Details for Troubleshooting Group Policy Core Functionality](#)- for more detailed information, including troubleshooting tips, for the root causes you have identified as most likely in the previous step.

The following information is not covered in this section, but is provided later in this paper:

- [Details for Troubleshooting Client-Side Extensions](#) addresses problems with the CSEs that process specific types of settings, such as security settings or Software Installation settings.
- [Troubleshooting Group Policy Administration](#) is devoted to problems with Group Policy administration.

Flowchart for Troubleshooting Group Policy Core Functionality

Use the flowchart (see Figure 1) in this section to quickly identify the likely root causes for unexpected Group Policy behavior, based on three questions that are easily answered from the Group Policy Results report.

Here is an example of how you can use the flowchart:

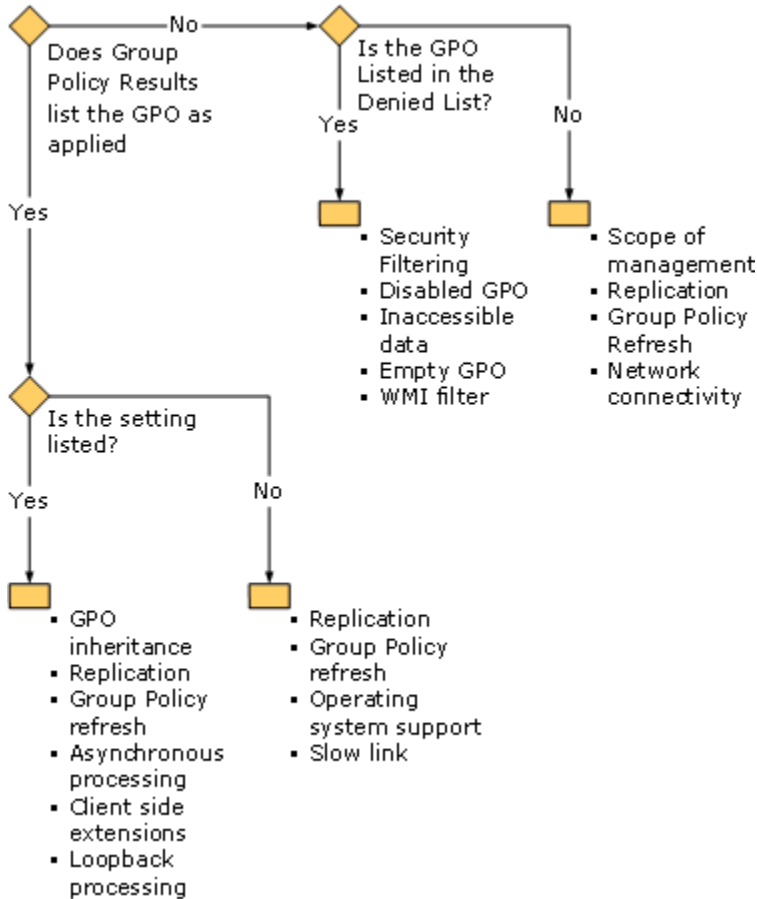
You have created a new setting in a GPO, but the setting is not being applied to a specific computer / user combination where you expect it to be applied. You generate a Group Policy Results report for that computer and user. The report shows that the GPO has been applied, but the setting is not listed in the report. Following the decision points in the flowchart you find replication, Group Policy refresh, operating system support, and slow link processing as potential causes. You determine that replication and Group Policy refresh seem the most likely reasons for the problem.

For a brief explanation of how each of these two factors might apply in this case, you look in the “Navigating the Group Policy Troubleshooting Flowchart” section. Based on the information presented there, you decide that for the case you are investigating Group Policy refresh seems the more likely cause, with replication as a possible but less likely culprit.

For a more detailed explanation and specific troubleshooting tips on these two issues, you look in “Details for Troubleshooting Group Policy Core Functionality.” Looking at the troubleshooting tips for Group Policy refresh, you conclude that this is the probable cause and one that you can easily test by

running GPupdate. After you run GPupdate, you see the desired behavior on the client. When you refresh the Group Policy Results report for that computer with that user logged on, you see that the setting as been applied and that the GPO you modified was the winning GPO.

Figure 1 Group Policy Troubleshooting Flowchart



Navigating the Troubleshooting Flowchart

The troubleshooting flowchart focuses on core Group Policy processing. Its primary purpose is to help you validate that the underlying infrastructure is in place to support delivery of GPOs to the client, that the user and computer are appropriately targeted to receive the intended GPOs, and that Group Policy processing puts the correct GPOs into effect.

A Group Policy Results report is the primary resource for troubleshooting Group Policy using this flowchart. Specifically, when investigating a problem, the administrator — where possible — should generate a Group Policy Results report for the user and computer combination encountering the problem. The sections of the report contain the information you use to navigate through the flowchart. For instructions on generating a Group Policy Results report, see “Determine Resultant Set of Policy with Group Policy Results” in GPMC Help.

An example of a Group Policy Results report is shown in Figure 2.

Figure 2 Example of a Group Policy Results Report

Group Policy Results

MYDOMAINjhaas on MYDOMAINCLIENT14
Data collected on: 4/21/2003 11:48:15 AM

Summary [show all](#) [hide](#)

Computer Configuration Summary [hide](#)

General [show](#)

Group Policy Objects [hide](#)

Applied GPOs [hide](#)

Name	Link Location	Revision
Default Domain Policy	mydomain.adatum.com	AD (3), Sysvol (3)

Denied GPOs [hide](#)

Name	Link Location	Reason Denied
Local Group Policy	Local	Empty
AssignedApps	mydomain.adatum.com	Disabled GPO

Security Group Membership when Group Policy was applied [show](#)

WMI Filters [show](#)

Component Status [show](#)

User Configuration Summary [hide](#)

General [show](#)

Group Policy Objects [hide](#)

Applied GPOs [hide](#)

Name	Link Location	Revision
Default Domain Policy	mydomain.adatum.com	AD (1), Sysvol (1)
AssignedApps	mydomain.adatum.com	AD (12), Sysvol (12)

Denied GPOs [hide](#)

Name	Link Location	Reason Denied
Local Group Policy	Local	Empty

This example shows the **Summary** tab of the report with the **Group Policy Objects** sections under **Computer Configuration Summary** and **User Configuration Summary** expanded.

By examining the GPMC Results report, you can find answers to the following three basic questions associated with the flowchart:

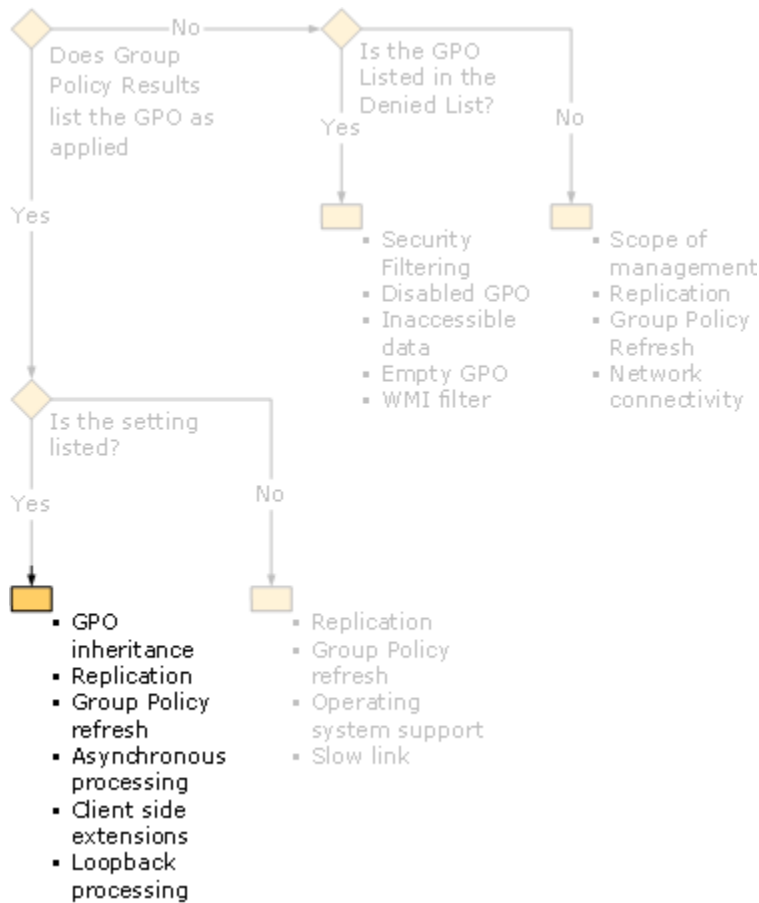
- Was the GPO applied to the client? The **Summary** tab shows this information.
- Is the policy setting listed in GPMC Results? The **Settings** tab shows this information.
- Is the GPO listed as Denied in GPO Results? The **Summary** tab shows this information.

Each question is answered under the following headings that correspond to the flowchart in Figure 3.

GPO Applied, Policy Setting Listed

In this scenario the client has successfully received the GPO and the specific policy setting is in effect at the client. This means that the only problem is that the actual value of the policy setting is incorrect. See the **Settings** tab of the Group Policy Results report for information about the individual settings that have been applied.

Figure 3 GPO Applied, Policy Setting Listed



The following factors can contribute to this scenario:

GPO Inheritance (Setting Listed)

Although GPOs have been applied, and the correct policy setting is listed, Group Policy inheritance might result in an unexpected GPO “winning” and providing a different value from the one expected. The settings are nested by source and type; click **Show** on the nested rows to expose the settings. Then look at the **Winning GPO** column to discover which GPO defines the value for the policy setting. For more information, see [Group Policy Inheritance Rules](#) in the section *Details for Troubleshooting Core Group Policy Application Functionality*.

Replication (Setting Listed)

After a change is made to either the GPO or the user or computer, that change must be replicated throughout the network. If you expected the winning GPO to supply a value for the setting other than the value that was actually applied, it might be that the GPO was changed recently, but the change has not yet been replicated to the domain controller that supplied the GPO to the client. For more information, see “[Replication Convergence](#)” later in this paper.

Group Policy Refresh (Setting Listed)

If Group Policy Refresh has not occurred since the winning GPO was modified and replicated, the old value for the setting is applied. After the changes to a GPO have been replicated to the client’s domain

controller, they need to be transmitted to the client. This occurs when the client refreshes Group Policy. Until this has occurred the change will not be reflected at the client. You can either wait for a background refresh or force the refresh. For more information, see [Group Policy Refresh](#).

Asynchronous Application of Group Policy (Setting Listed)

Group Policy can be applied after the computer has started and the user has logged on. This is called asynchronous application of Group Policy, in contrast to synchronous processing that occurs as part of startup or logon.

If the problem is with a setting that can only be applied during startup or logon, it might have been detected during asynchronous Group Policy processing – for example as part of a Group Policy refresh or during the asynchronous processing used for logon optimization in Windows XP. For more information, see [Asynchronous Processing and Logon Optimization in Windows XP](#).

Client-Side Extension Issue (Setting Listed)

After the core Group Policy engine has completed initial processing of the GPOs, it passes specific settings to CSEs to process. If the setting is listed but the value is wrong or the behavior on the client does not reflect the setting value, the failure might have occurred after this setting was passed to a CSE to process. For example, even if a Folder Redirection setting has been successfully passed to the Folder Redirection CSE, the CSE might not be able to complete processing for the setting. For more information, see [Details for Troubleshooting Client-Side Extensions](#).

Loopback Processing (Setting Listed)

Loopback processing is a way to enforce a set of user settings at a computer regardless of who logs on at that computer. Typically, user settings are applied based on the site and OU membership of the user. If loopback processing is set for a computer, the user settings for anyone logged on to that computer are dependent (partially or fully) on the site and OU membership of the computer. The behavior depends on the mode of loopback processing. In Replace mode, only the user settings defined in GPOs applied to the computer are used. In Merge mode, user settings from GPOs that would normally apply to the user are used provided they do not conflict with user settings in GPOs that apply to the computer.

Loopback processing only works if the computer and user are both in Windows 2000 or Windows Server 2003 domains. They can be in different domains, and one can be in a Windows 2000 domain while the other is in a Windows Server 2003 domain. You cannot deploy Group Policy to users in a Windows NT 4.0 domain by applying loopback to a computer in a Windows 2000 or Windows Server 2003 domain.

Security filters can affect the way loopback processing is applied. Even when the GPOs associated with the computer are used to define user settings, the user's credentials – not the computer's credentials – are validated against the GPO's security filter. Therefore the user's credentials determine whether the GPO should be applied.

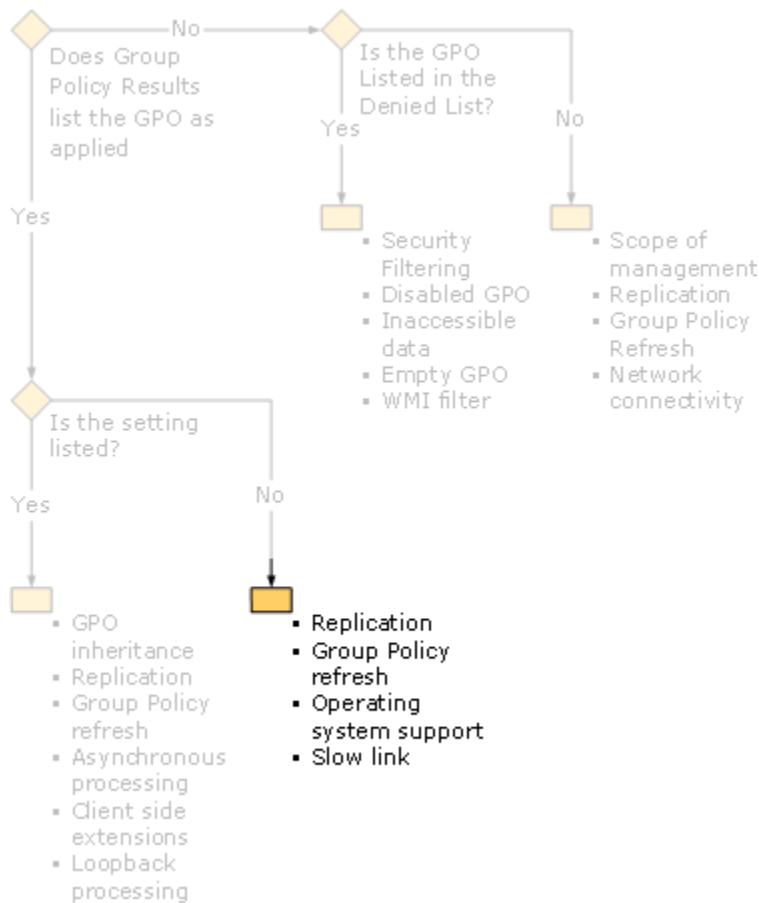
For example, you could create a GPO with a security filter that restricts the GPO to system administrators, and then associate that GPO with a computer that is configured for loopback processing. The settings in that GPO would only be applied when a system administrator is logged on.

To determine whether loopback processing is in effect, look for the **User Group Policy loopback processing mode** setting on the **Settings** tab of the report, under **Computer Configuration \Administrative Templates \System/Group Policy**. For more information, see [Loopback Processing](#).

GPO Applied, Policy Setting Not Listed

In the Group Policy Results report, the structure of the **Settings** tab is similar to the structure used in the Group Policy Object Editor. Expand the sections on the **Settings** tab by clicking **Show**. If the expected policy setting does not appear at all, either no updated GPO containing the expected setting reached the client, or the setting might not be processed at the client.

Figure 4 GPO Applied, Policy Setting Not Listed



Replication (Setting Not Listed)

After a setting is added to either a GPO, that change must be replicated throughout the network. If the setting is specified in the GPO but is not listed in the Group Policy Results report on the client, it might be that the setting was recently added to the GPO, but the change has not yet been replicated to the domain controller that supplied the GPO to the client.. For more information, see "[Replication Convergence](#)" later in this paper.

Group Policy Refresh (Setting Not Listed)

If Group Policy Refresh has not occurred since the winning GPO was modified and replicated, a newly added setting will not be applied. After the changes to the GPO have been replicated to the client's domain controller, they need to be transmitted to the client. This occurs during Group Policy refresh. You can either wait for a background refresh or force the refresh by running gpupdate, by logging off/on (for user configuration), or by restarting the computer (for computer configuration). For more information, see [Group Policy Refresh](#).

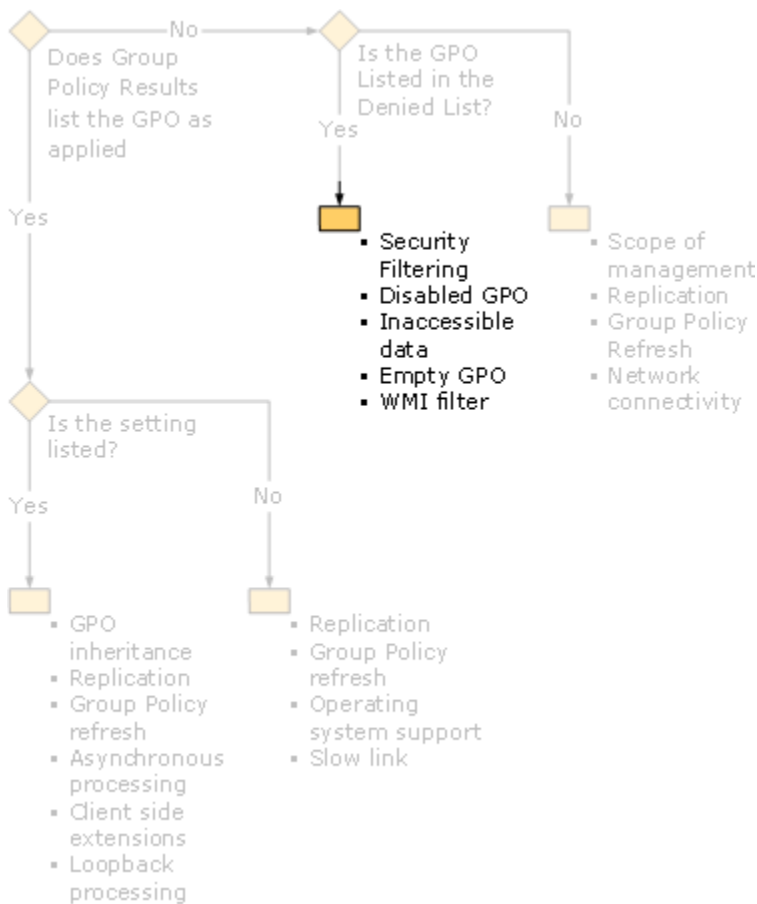
Lack of Operating System Support (Setting Not Listed)

Some policy settings are supported on only certain operating systems or require a minimum service pack to be applied. When a GPO delivers a policy setting to a client computer that does not support that setting, the operating system ignores the setting. For more information, see [Operating System Support](#).

GPO Not Applied, Listed as Denied

If the GPO successfully reaches the client, it appears either in the list of Denied GPOs or in the list of Applied GPOs. A GPO can be explicitly denied for any of a number of reasons.

Figure 5 GPO Not Applied, Listed as Denied



To determine whether a GPO is denied, look on the **Summary** tab or the Group Policy Results report. Under **Computer Configuration Summary** and again under **User Configuration Summary**, click

Show to expand **Group Policy Objects**, and then show **Denied GPOs**. The reason for the denial is given for each denied GPO.

Security Filtering (GPO Denied)

The user or computer does not have the user rights assigned for the GPO. The required privileges are Read and Apply Group Policy. Alternatively, a GPO might be associated with a Deny ACE, which overrides any other privileges granted to the user or computer. For more information, see [Access Control and Security Filtering](#).

Disabled Link (GPO Denied)

There is a link to the GPO from a site, domain, or OU in the hierarchy of the user or computer, but that link has been explicitly disabled. You can quickly scan the navigation pane of GPMC for disabled links, as described in Viewing Active Directory objects and GPOs in the “Troubleshooting Tools” section of this paper.

Inaccessible GPO (GPO Denied)

There is a link to the GPO, but the GPO cannot be accessed. There are several possible reasons for this:

- The permissions on the GPO or on folders in the path to the Group Policy template are insufficient for it to be accessed and read. If this situation occurs the **Component Status** section of the Group Policy Results report will indicate **Failure** for the component **Group Policy Infrastructure**.
- The GPO might have been deleted, but the link to it remains for some reason (such as replication lag).
- Network connectivity problems might prevent access to the GPO.
- The client is unable to contact any domain controller.

For more information, see the sections [Missing or Corrupted Files](#), [Replication](#), and [Access Control and Security Filtering](#).

Empty GPO (GPO Denied)

A GPO will be denied if it has no settings. This occurs when an administrator has configured a GPO and linked to it, but has not set any policy settings within the GPO. Either remove the link to the GPO or add policy settings to the GPO. If there are no remaining links to the GPO, you might want to delete it.

WMI Filter (GPO Denied)

A WMI filter applied to a GPO is essentially a Boolean (true/false) decision as to whether the entire GPO should be applied to the client computer. The filter is evaluated at the client when GPO is applied. Based on the embedded WQL query, the GPO will either be enabled or disabled. See [WMI Filtering](#) for further details.

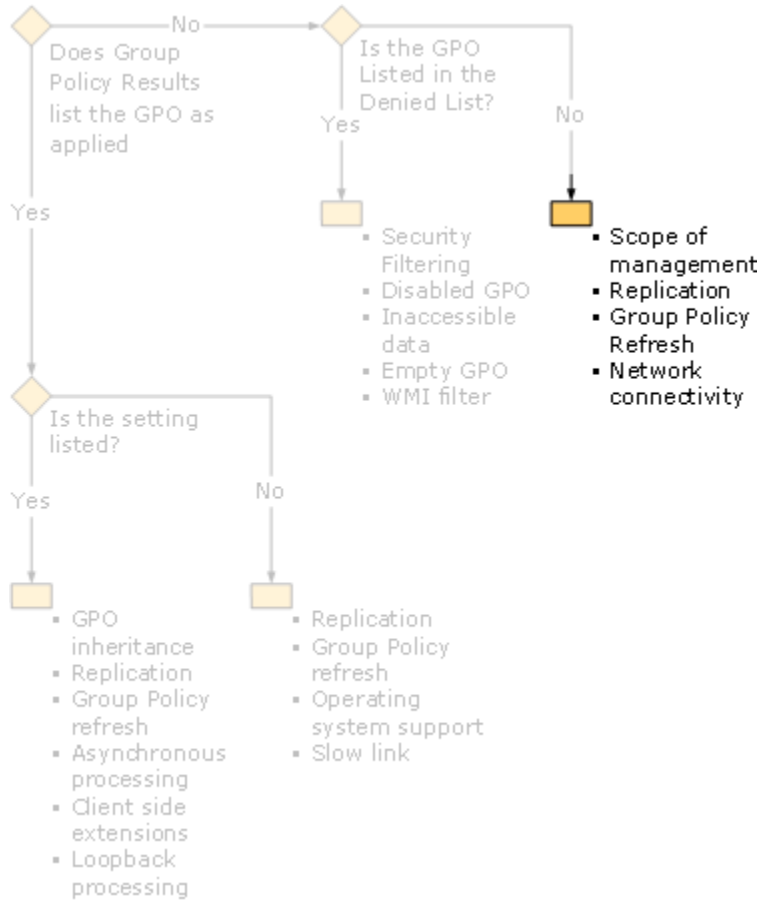
GPO Neither Applied nor Denied

All the GPOs that reach the client appear on the **Summary** tab in either the **Group Policy Objects Applied** section or the **Group Policy Objects Denied** section. There are four lists altogether: two lists (Applied GPOs and Denied GPOs) under **Computer Configuration Summary** for settings that are delivered from the computer’s Active Directory hierarchy, and another two under **User Configuration**

Summary for settings that are delivered from the user’s Active Directory hierarchy. If the GPO is not listed as either Applied or Denied under either Configuration Summary, it did not reach the client.

Also note whether the GPO is listed in the expected Configuration Summary (Computers or Users). That can affect which settings are actually applied, particularly if loopback processing is in effect.

Figure 6 GPO Neither Applied Nor Denied



Scope of Management (GPO Not at Client)

One of the most common causes of a GPO not being applied to a user or computer is that the GPO is not linked to a site, domain, or OU of which the computer or user is a member. GPOs are delivered to clients based on the site and OU memberships of the computer and the logged-on user; group memberships are only used to further restrict application of the GPO. See [Organizational Unit \(OU\) Membership and GPO Links](#) for further details.

Replication (GPO Not at Client)

After an administrator has linked a GPO to a site, domain, or OU in the hierarchy of the user or computer, the change must be replicated to the domain controller from which the client retrieved its GPOs. Also, if the user or computer has recently been added to an OU, the GPOs that apply to that OU might not be applied to the client until the change in OU membership has been replicated to the domain controller from which the client retrieves GPOs. For more information, see [“Replication Convergence”](#) later in this paper.

Group Policy Refresh (GPO Not at Client)

After an administrator has linked a GPO to a site, domain, or OU in the hierarchy of the user or computer, and the change has been replicated to the client's domain controller, the GPO still needs to reach the client. This occurs during Group Policy refresh. You can either wait for a background refresh or force the refresh. For more information, see [Group Policy Refresh](#).

Network Connectivity (GPO Not at Client)

Group Policy requires a reliable networking infrastructure to ensure appropriate communication between the client computer and a domain controller. This includes TCP/IP, DNS and other dependent technologies, See [Network Connectivity](#) for further details.

Details for Troubleshooting Core Group Policy Application Functionality

You can get a wealth of information about Group Policy application on a client by going to the Group Policy Results node in GPMC and generating a report for that client. The Group Policy Troubleshooting Flowchart and the text that accompanies it tell you what to look for in that report and which factors might be responsible for the results you see.

This section discusses the factors that affect core Group Policy functionality: the delivery of GPOs to the clients by way of the domain controllers and the evaluation of the ordered set of GPOs to be applied to the client. Each time Group Policy is applied the full set of GPO's is reevaluated and reapplied if there is a change. In addition to this core functionality, there are special cases for software distribution, Folder Redirection, scripts processing, administrative templates, security, etc. These functions are handled by Group Policy CSEs and are discussed under *Factors Affecting Group Policy Client-Side Extensions*.

Network Connectivity

Obviously, Group Policy cannot be delivered to clients who are not connected to the network. In this case the user can log on with cached credentials, and the last set of policies that the computer received will be applied. This is relevant to a user who logs onto a corporate network through a VPN connection. In this scenario, the usual application of Group Policy does not occur because the user is already logged on to the computer before the VPN connection is established. One way to ensure that the normal Group Policy processing occurs at logon is by using the option to connect to a remote network through the initial logon prompt (Ctrl-Alt-Del).

Other issues that are related to network connectivity with regard to Group Policy application include slow links, DNS problems, and multi-homed clients. These are discussed in this section. A client might also be unable to access network resources due to time sync problems, as discussed in the Infrastructure Requirements at the beginning of this document under Networking.

Network connectivity can also be the root cause of replication problems.

Troubleshooting

- To test for network connectivity problems, check system event logs on the client computer (look for failed access attempts). You can also use the **ping** or **netdiag** commands to test network connectivity. For more information, see "Using Network Diagnostics" and "Active Directory support tools" in Help and Support Center for Windows Server 2003.

- TCP/IP must be enabled on the network and on the client. ICMP is used to detect a slow link when the client initially connects to a domain controller, and therefore is required for Group Policy. ICMP must also be enabled if a firewall is in use. By default, the packet size used for slow link detection is 2048 bytes. Routers and firewalls must also support this packet size to ensure that slow link detection can succeed. For more information, see [TCP/IP and ICMP](#) under [Infrastructure Requirements](#) earlier in this document.

Slow Links

By default, Group Policy defines a slow link as 500 kilobits per second or less. You can change this setting in the computer configuration, the user configuration, or both. The setting is in the **Administrative Templates**; look under **System** and then under **Group Policy**.

Troubleshooting

- When the computer is connected to the network over a slow link, Security settings and Administrative Template settings are always applied.
- By default, Software Installation, scripts, and Folder Redirection settings are not applied over a slow link.
- Group Policy is not processed if the user connects to the network over a slow link with cached credentials. To ensure that Group Policy is applied over a slow link, the user must select the **Logon using dialup connection** check box while using the **Logon** dialog box.
- Even if Group Policy settings are configured to run scripts over slow links, the scripts might be executed so slowly that they exceed the configured time-out period. In this case the script will fail to complete and a UserInit event will be posted.

DNS

Group Policy application requires clients to access specified servers, including domain controllers and other servers such as share points and install points. Group Policy management also requires access to domain controllers. DNS is used to locate and identify these servers. In Windows Server 2003, Active Directory requires DNS support.

If the network is functioning, but clients or GPMC consoles are unable to locate the servers, there might be a problem with your network's DNS system.

Troubleshooting

- First, Ping the computer using the NetBIOS name. Then Ping the computer again using the fully qualified domain name of the target computer. If the first Ping works but the second does not then there is probably a DNS problem. Use Netdiag.exe to research the problem further.
- Use **Dcdiag.exe** to troubleshoot domain controllers, and use **Netdiag.exe** to troubleshoot client computers. These tools can help determine both server and client DNS misconfigurations. For more information, see article Q265706, "DCDiag/NetDiag Facilitate Join and DC Creation" in the [Microsoft Knowledge Base](#) (<http://go.microsoft.com/fwlink/?LinkId=4441>).

Multi-Homed Computers

If a client has multiple network adapters connected to multiple networks, assign the highest priority to the network adapter that connects to the network that is providing Group Policy to that client. For more information, see [Microsoft Knowledge Base Article 258296](http://go.microsoft.com/fwlink/?LinkId=17909) (<http://go.microsoft.com/fwlink/?LinkId=17909>).

Missing or Corrupted Files

Group Policy information is contained in files on both the domain controllers and the clients. If any of these files are missing or corrupted, only some or none of the policies can be applied. For a brief discussion of this issue, see "[SYSVOL Share](#)" earlier in this document.

Troubleshooting

- Use GPOtool.exe to check for the presence and integrity of the following files in the SYSVOL share and its subfolders on the domain controller.
 - Files in the Group Policy template.
 - Registry.pol (Search %windir%\debug\usermode\UserEnv.log for references to this file). This file is used for processing administrative templates through the registry CSE.
- When a process is unable to access a file, it generates an event. Whether this event is recorded depends on the event severity and whether verbose logging is enabled for that process. Check the **Policy Events** tab in the Group Policy Results report for events that point to problems accessing files. You can also use Event Viewer on the client to view the Application logs, and you can enable and view verbose logging for UserEnv and for specific CSEs to Group Policy. For more information, see "[Appendix: Group Policy Log Files](#)."
- On the client, check for the presence and integrity of the following files in the %windir%\system32 folder. Replace suspect or files missing from the CD for the client's operating system. The System File Checker (Sfc.exe) can be used to scan all protected files to verify their versions.
 - UserEnv.dll
 - Dskquota.dll
 - Fdeploy.dll
 - Gptext.dll
 - Appmgmts.dll
 - Gptext.dll
 - Scecli.dll

Replication Convergence

Most networks use more than one domain controller for fault tolerance and performance reasons. Any of these domain controllers can respond to system requests from computers in the domain — authentication requests or Group Policy refresh requests, for example. For consistent behavior throughout the network, all the domain controllers need to be providing the same information to clients. This is accomplished by replicating the data among the domain controllers in a single domain.

Two forms of replication are employed:

- Active Directory replication copies the changes to directory information to the data stores on other domain controllers. The replicated information includes the Group Policy container for each GPO, as well as information about the relationships between Active Directory containers that Group Policy client-side extensions use to determine what Group Policy settings apply to them. Active Directory replication occurs at a set interval and can be forced.
- File Replication service (FRS) copies changes to files to other domain controllers, so that the files are mirrored from one domain controller to another. This includes the SYSVOL share, which contains Group Policy template for each GPO. FRS replication occurs at set intervals according to its replication schedule and cannot be forced.

There can be a lag time after a change has been made on one domain controller before the change is replicated to all other domain controllers. The propagation and resolution of these changes throughout the network is an ongoing process called *replication convergence*.

Troubleshooting

- Until changes to a GPO have been replicated to the domain controller a client is accessing, that client will receive the earlier version of the GPO during Group Policy refresh. If you suspect both replication and Group Policy refresh issues, address the replication issue first. Then refresh Group Policy at the client.
- Changes to the OU memberships of computers and users also need to be replicated before they can be reflected in Group Policy application at the client. For more information see "[Organizational Unit Membership and GPO Links](#)."
- In general, it is best to use the same domain controller for all GPO editing or to agree a process – such as delegated administration of GPO's – to minimize the likelihood of the same GPO being edited on different domain controller. If changes are made to the same GPO at two different domain controllers, the last change wins. Also, if you delegate control of a specific GPO to a user group, members of that group might be unable to perform the delegated tasks until the permissions have been replicated to their domain controller. For more information see "[Domain Controller Selection in the Group Policy Object Editor and GPMC](#)" later in this paper.

There are several options for troubleshooting replication issues:

- The Group Policy container and Group Policy template are each assigned version numbers, which are incremented when the GPO is modified. Use GPOTool to verify that the versions are synchronized.
- Use Event Viewer to examine the directory service for event log on the domain controller. Active Directory replication errors will appear with source=KCC.
- Use Event Viewer to examine the File Replication service event log on the domain controller. FRS errors will appear with source=NTFRS.
- Verify that the SYSVOL share exists on the domain controller. You should be able to find `\\domain_controller_name\SYSVOL`, where *domain_controller_name* is the fully qualified domain name (not the NetBIOS name) of the domain controller.

- To troubleshoot Active Directory replication issues, use replmon.exe and the other Active Directory support tools that ship with Windows Server 2003. These are listed in “Active Directory support tools” in Help and Support Center for Windows Server 2003.
- You can use GPOtool.exe to identify problems related to domain controller health, including Active Directory replication and FRS issues.
- To troubleshoot file replication issues, check the status of the Directory File Service links and targets as described in “To check status of a DFS root, DFS link, or target” in Help and Support Center for Windows Server 2003. Group Policy requires Directory File Service.
- You can use the Sonar.exe tool to check the health of the SYSVOL share.

Group Policy Refresh

Group Policy refresh refers to the retrieval of GPOs by a client. During Group Policy refresh, the client contacts an available domain controller. If *any* GPOs have changed, the domain controller provides a list of *all* the appropriate GPOs, regardless of whether their version numbers have actually changed.

Replication and Group Policy refresh are both instances of lag-time issues: the system is working properly, but changes have not yet appeared at the client.

Troubleshooting

- By default, GPOs are processed by CSEs at the computer only if the version number of at least one GPO has changed on the domain controller that the computer is accessing. You can use policy settings to change this behavior.
- Some CSEs process unchanged GPOs if the user’s group membership has changed.
- At startup, Group Policy is refreshed, and computer settings are applied.
- Group Policy is refreshed and computer and user settings are applied in the following instances:
 - When a user logs on.
 - When gpupdate is run at the client computer.
 - At the refresh interval, if one is configured at that computer. By default, domain controllers are refreshed every five minutes, and all other computers are refreshed every 90 minutes, with a random factor of up plus or minus 30 minutes.
- To see the last time the GPOs from the computer’s OU were processed, look on the **Summary** tab of the Group Policy Results report under **Computer Configuration Summary**, and then under **General**.
- To see the last time the GPOs from the user’s OU were processed, look on the **Summary** tab of the Group Policy Results report under **User Configuration Summary**, and then under **General**.
- To collect Group Policy refresh information from clients and store them at a central location, use gpmonitor.exe. This tool is included in the *Windows Server 2003 Deployment Kit*.

Note

Some types of settings can only be applied during logon. These include Folder Redirection, Roaming Profiles, and Software Installation settings. If these settings are received when Group Policy is refreshed, the settings are evaluated, but they are not applied until the next time the user logs on.

If the computer is running Windows XP and these settings first reach the computer during logon, they might not be applied until the next time the user logs on. For some extensions, it might take two or three logons for the settings to be applied. For more information see [“Asynchronous Processing and Logon Optimization in Windows XP”](#) later in this paper.

A simple way to troubleshoot a suspected Group Policy refresh issue is to force the refresh by running gpupdate and either restarting the computer, or by logging off and logging on again. If Folder Redirection, roaming profiles, or Software Installation is involved and the computer is running Windows XP, run gpupdate and then log off and log back on. You might need to log off and log back on more than once. For more information, see [“Asynchronous Processing and Logon Optimization in Windows XP”](#) later in this paper.

Trust Relationships

You can link GPOs across domains, provided there is a trust relationship between them. If the trust relationship is broken, clients will be unable to access the GPO and related files. You might also encounter performance issues with links across domains.

GPMC supports management of other forests from within the console when there is a trust relationship between those forests and the forest in which your user account resides. However, you cannot link a GPO in one forest to a site, domain, or OU in a different forest.

Troubleshooting

- If the GPO cannot be applied due to lack of trust, it will appear in the list of Denied GPOs and the reason given will be **Inaccessible**.
- Use Active Directory Domains and Trusts or nltest.exe to verify the trust relationship, and to if repair it if necessary.
- If you are not concerned about the identical GPO being applied in both domains, copy the GPO to the domain with the Active Directory containers you want to link to it.

For more information see “Forests in Group Policy Management Console” in GPMC Help and “Forest trusts” in Help and Support Center for Windows Server 2003.

OU Memberships and GPO Linking

GPOs are applied to a client only if they are linked to a site, domain, or OU to which the computer or the user at that computer belongs.

For troubleshooting purposes, you need a solid understanding of your organization’s Active Directory structure and the Group Policy inheritance and filtering rules. With this information and the Resultant Set of Policy (RSOP) functionality in Windows Server 2003 and Windows XP, you can manipulate your Active Directory structure and your Group Policy links and filters to deliver targeted settings to the users and computers in your organization. The same information is needed to troubleshoot situations where these manipulations produce an unexpected result.

Troubleshooting

- Check Active Directory Users and Computers to see what site, domain, and OU the user and the computer are in.

- In GPMC, expand the Active Directory containers that contain the affected client. In the navigation pane, scan the list of GPOs for each container for disabled links.
- GPOs are filtered according to the Active Directory groups that the users and computers belong to. The Active Directory objects in which you place your Active Directory groups and the ways you group users or computers affect how GPOs can be distributed and applied.
- Active Directory and FRS replication lag can affect either part of the GPO.
- If you have an OU that contains other OUs and you remove Read permissions to the parent OU, then no policy will be processed by computers or users in that OU hierarchy.

If there are conflicting settings in the GPOs that apply to the client, they are resolved according to the Group Policy inheritance rules, which are discussed elsewhere in this section.

Adding a User or Computer to an OU

When a user or computer is added to an OU, two things need to happen before the GPOs that the new OU links to are applied to the client:

- The new OU assignment must be replicated to the client's domain controller. For more information, see ["Replication Convergence"](#) earlier in this paper.
- After the replication is complete, you must either log off and log back on again if the user account moved to the new OU, or restart the computer if the computer moved to the new OU.

Some settings can only be applied at system startup or logon. For more information see ["Asynchronous Processing and Logon Optimization in Windows XP"](#) later in this paper.

User Settings vs. Computer Settings

In most cases, the computer settings are taken from GPOs that are linked to nodes in the hierarchy that the computer belongs to, and user settings are taken from GPOs that are linked to nodes in the hierarchy that the user belongs to. The exceptions are loopback processing, which is discussed in General Issues for CSE Processing, and explicit denials, which are discussed in the white paper, [Windows Server 2003 Group Policy Infrastructure](http://go.microsoft.com/fwlink/?LinkId=14950) (<http://go.microsoft.com/fwlink/?LinkId=14950>).

There are two main issues involving user settings and computer settings. The first is when settings are applied – at system startup, at logon, or through background refresh while the computer is in use. The second is how conflicts are resolved after inheritance rules have been applied to determine the GPOs that apply to the client.

Troubleshooting

- Loopback processing can determine which GPOs provide user settings. For more information, see [Loopback Processing](#).
- If a setting is not supported by the operating system running on the computer where the user logs on, the setting is ignored. For more information, see [Operating System](#).
- Computer settings are not applied until Group Policy is refreshed on that computer, or the computer is restarted.
- User settings are not applied until Group Policy is refreshed on that computer, or the user logs on.

Some user settings, notably those involving Software Installation or Folder Redirection, cannot be applied until the user logs on. If the computer is running Windows XP and logon optimization is in effect, the user might need to log on more than once. For more information see "[Asynchronous Processing and Logon Optimization in Windows XP](#)" later in this paper.

The computer configuration settings and user configuration settings for a client are listed in the Group Policy Results or Group Policy Modeling report for that client, on the **Settings** tab.

The computer configuration settings and user configuration settings for a GPO are listed in the GPO, on the **Settings** tab.

Security Filtering

Group policy can be used to provide or deny access to programs and data in your network, and to enforce policies regarding computer configuration based on assigned privileges and security group memberships. This is accomplished by using the access control functionality built in to Windows 2000 Server and Windows Server 2003 domains and is known as security filtering.

You can restrict application of all the settings in a GPO on the basis of security group memberships by setting a security filter on that GPO. If the computer account or user account does not meet the security filtering criteria, the entire GPO will be denied at that client. For example, you can assign special settings to all the administrators in a portion of the hierarchy by setting the security filter to apply the GPO to all administrators, and then linking the GPO to the highest node in the portion of the hierarchy where you want the settings to apply. All users in that portion of the hierarchy will receive the GPO, but only members of the administrators group will be affected by it.

Troubleshooting

- To see the security groups that were in effect when Group Policy was applied to a specific computer, look in the Group Policy Results report for that computer. Under both Computer Configuration Summary and User Configuration Summary, expand Security Group Membership when Group Policy was applied.
- To see the access control lists that affect where a GPO can be applied, open the GPO in GPMC and look at Security Filtering on the Scope tab. This is also where you would change those settings.
- If a GPO is incorrectly denied or applied due to security filtering because the user or computer had different security group memberships than expected, use Active Directory Users and Computers to check and if necessary change the security group memberships.
- When restricting the application of a GPO, be sure to remove **Authenticated Users**. Otherwise all users will always be affected by the GPO.
- Computers are members of the Authenticated Users group. If you remove **Authenticated Users** from the list on the **Scope** tab and you want the GPO to apply to a computer, you must specifically ensure that the computer belongs to a group that is included in the **Security Filtering** section on the **Scope** tab.

Cached Credentials

When a user successfully logs on to the network, the credentials for that user can be cached on the local computer. If network connectivity problems prevent the user from being authenticated the next

time the user logs on to the same computer, these cached credentials can be used to give the user access to resources on that computer. If the computer successfully connects to the network later, the cached credentials can be used to provide access to network resources, including GPOs that are received at the next Group Policy refresh.

Troubleshooting

- If a domain controller is not available when the user logs on Group Policy cannot be refreshed at logon. In this case, new Group Policy settings will not be applied until a Group Policy refresh occurs while a domain controller is available.
- Some user settings can only be applied during logon. These include roaming user profile path, Folder Redirection path, and Software Installation settings. If the user is already logged on when these settings are detected, they will not be applied until the next time the user is logged on. For more information, see "[Asynchronous Processing and Logon Optimization in Windows XP](#)" in this paper.
- When a user logs on to a computer locally and then accesses the network by using a dialup or VPN connection, cached credentials are always used.

WMI Filtering

If the GPO is linked to a WMI filter, the queries in the WMI filter are evaluated against the data provided by WMI on the client. Such data can include hardware and software inventory, settings, and configuration information.

If all of the criteria are true, the GPO is applied.

If any of the criteria is false, the GPO is denied.

If a WMI filter is deleted, the links to the WMI filter are not automatically deleted. If there is a link to a non-existent WMI filter the GPO with that link will not be processed until the link is removed or the filter is restored.

Note

Only Windows XP, Windows Server 2003, and later operating systems support WMI filtering. If the computer is running an earlier operating system (such as Windows 2000), the WMI filter is ignored and the GPO is applied. Troubleshooting:

-
- If the filter is not producing the expected results, troubleshoot and edit the filter. WMI filters are stored on a per-domain basis separately from the GPOs that link to them. They can be accessed in GPMC on the **WMI Filters** node under the domain. For more information see GPMC online Help.
 - You can also use the WBEMtest and WMIC utilities to troubleshoot WMI issues. For more information, see "Windows Management Instrumentation Command-line" and "Windows Management Instrumentation Tester" in Help and Support Center for Windows Server 2003.

Group Policy Inheritance Rules

Before you apply or troubleshoot Group Policy, you should be familiar with Group Policy inheritance rules. These are described in GPMC Help and in "[Designing a Group Policy Infrastructure](#)" (<http://go.microsoft.com/fwlink/?LinkId=4757>) in the Windows Server 2003 Deployment Guide. GPOs can be linked to sites, domains, and OUs.

The following inheritance rules apply to GPOs:

- Certain settings can only be set at the domain level. One example is domain password policies. If an OU lower in the hierarchy links to a GPO with password policy settings, those settings only apply to the local accounts.
- OUs inherit the GPOs linked to their parents. Exceptions are due to the use of **Block Inheritance** and **Enforce** settings. (**Enforce** was previously called **No Override**.) In contrast to OUs, domains do not inherit Group Policy from parent domains.
- The order in which GPOs are applied is critical because where there are conflicts in settings between these GPOs, the last GPO applied wins. Exceptions are due to **Enforce** and **Loopback Processing** settings.
- GPOs from the most distant container are applied first, and GPOs from the nearest container are applied last.
- GPOs from any one Active Directory container are applied according to their precedence, as defined by the link order.

When you view a site, domain, or OU in GPMC, you can view the GPOs linked directly to that container and its parents, including the link order. You can also see where inherited GPOs are linked and whether they are enforced.

Troubleshooting

- Conflict resolution applies to individual settings, not to entire GPOs. It could easily happen that one setting in a GPO encounters a conflict but all other settings in that GPO are applied.
- The GPO with the lowest link number prevails over other GPOs that the same site, domain or OU is linked to. You can use GPMC to change the order of links for a specific site, domain, or OU. (The links are a property of the site, domain, or OU; they are not a property of the GPO.)
- **Enforce** and **Block Inheritance** settings can complicate troubleshooting because they counteract the usual inheritance rules.
- The **Enforce** setting is a property of the link between an Active Directory container and a GPO. It is used to force that GPO to all Active Directory objects within a container, no matter how deeply they are nested. The settings within a GPO that is enforced override other settings that would prevail because they are applied later. If there are conflicting settings in GPOs that are enforced at two levels of the hierarchy, the setting enforced *furthest* from the client prevails. This is a reversal of the usual rule, in which the setting from the nearest-linked GPO would prevail.

The actual effect of **Enforce** is to change the order of processing. The settings in an Enforced GPO are processed after all other GPOs settings are processed.

- The **Block Inheritance** setting applies to an entire Active Directory container. It blocks the inheritance of all GPOs except for those for which the link from the parent Active Directory object to the GPO has the **Enforce** setting enabled.
- Administrators who have set **Block Inheritance** on their domain or OU can still make explicit links to GPOs elsewhere in the domain, including GPOs that might otherwise be inherited. (Domains do not

inherit GPOs from parent domains.) Note that when Block Inheritance is applied at a domain level it blocks GPO's linked to sites.

Migrating GPOs Between Forests

Migration in this context refers to transferring a GPO from one forest to another — from a test environment to a production environment, for example. Migrating from a Windows NT 4.0 domain to a Windows 2000 or Windows Server 2003 domain is a different issue and is covered in Migrating from Windows NT 4.0.

Simply backing up and importing the GPO often does not produce the results you want because GPOs include domain-specific information such as security principals and UNC paths. GPMC includes migration support, including a migration table editor, to address these issues. If a GPO that worked in one forest is not working as expected in the new forest, you might need a migration table. You also might need to back up and import the GPO instead of copying it.

Troubleshooting

- Check for a trust relationship between the source domain and the target domain. If there is trust, copy the GPO; if not, import it.
- If the GPO has references to security principles or UNC paths, use a migration table.
- The migration table editor that is included with GPMC provides error checking. However there is still a possibility of mistyped UNC paths.

For more information see [Migrating GPOs Across Domains with GPMC](http://go.microsoft.com/fwlink/?LinkId=14321) (<http://go.microsoft.com/fwlink/?LinkId=14321>).

Loopback Processing

Some GPOs are delivered to the client through the Active Directory hierarchy the computers belong to, and other GPOs are delivered through the user's Active Directory hierarchy. GPOs from either source can have both computer settings and user settings.

Typically, the user settings in GPOs linked to a site, domain, or OU in the user's hierarchy prevail over user settings in GPOs directed to the computer. User settings in GPOs applied to the computer are ignored. If the computer is configured for loopback processing, the user settings from GPOs directed to the computer will affect the processing of the user's Group Policy settings. The exact effect depends on which mode of loopback processing is configured.

Note

The user's account is used to check against security filtering for user settings, even if loopback processing is implemented.

There are two modes for loopback processing. In **Loopback with Replace**, the GPO list for the user is replaced in its entirety by the GPO list assigned based on the computer's inheritance hierarchy. This is evaluated each time Group Policy is applied. In **Loopback with Merge**, the user-assigned settings are applied after the computer-assigned user settings – in effect the two sets of user policy settings are merged.

Loopback processing can only be applied to computers in Windows 2000 or Windows Server 2003 domains.

To find out whether loopback processing was applied when Group Policy was evaluated on the client, look in the Group Policy Results report on the **Settings** tab in the following location:

- Computer Configuration
 - Administrative templates
 - System/Group Policy

Troubleshooting

- If the loopback processing is appropriate for this client you might need to educate the users so they know what to expect.
- If loopback is desired and it appears that it is not being applied, first verify the loopback policy setting (which is a computer configuration policy) has been applied to the computer through an appropriate GPO.

Details for Troubleshooting Client-Side Extensions

After the core Group Policy processing is completed at the client, the GPOs are handed to the appropriate CSEs. The CSEs are DLLs that process the GPOs. A CSE might process only certain types of settings. For example, the Scripts CSE deals only with settings involving startup, shutdown, logon, and logoff scripts, while the Folder Redirection CSE deals only with settings involving Folder Redirection.

Several CSEs ship with Windows 2000, Windows XP Professional, and Windows Server 2003. Other software manufacturers might create additional CSEs to leverage Group Policy functionality and make their products more manageable.

Because CSEs cannot begin to work until core Group Policy processing is completed, the issues described in the previous sections apply regardless of which CSE processes the setting. For example, they can all be affected by network connectivity problems that prevent the GPO from reaching the client, or by inheritance rules.

Operating System Support

Many Group Policy settings were introduced for Windows XP and Windows Server 2003 that are not supported by earlier operating systems. If a setting is not supported, Group Policy will set the registry key to the specified value, but it is effectively ignored because no application or component will read that registry key. Computers earlier than Windows 2000 do not support Group Policy at all.

WMI Filtering is only supported by Windows XP, Windows Server 2003, and later operating systems. Other operating systems ignore the WMI filter and apply the GPO.

Troubleshooting

- Verify that the setting is supported by the client's operating system. The Group Policy Object Editor displays the operating systems where each policy setting is supported.

Asynchronous Processing and Logon Optimization in Windows XP

Group Policy can be applied during startup and logon (synchronous processing) or as a background task after startup or logon has completed (asynchronous processing). Changes received during periodic Group Policy refresh or in response to the gpupdate command are processed asynchronously. On computers running Windows XP, Group policies received during logon are also processed asynchronously by default, so that the logon is completed more quickly.

Software Installation and scripts processing must be applied during startup or logon. Folder Redirection assigned to the user must be applied during logon. By default, Windows XP logs a user on in asynchronous mode. Group Policy is then applied in the background after the user is logged on. This results in faster logons. However, when a new GPO setting for Software Installation, Scripts, or Folder Redirection arrives at a computer running Windows XP, the user has already logged on by the time Group Policy has been evaluated. It is too late to apply the Software Installation setting. In this case a flag is set so that the next time computer is rebooted or the user logs on Group Policy will be evaluated and applied before the startup or logon is completed.

In situations where you need for users to receive software, implement folder redirection, or run new scripts in a single logon, apply a GPO with the setting **Always wait for the network at computer startup and logon** to the computer. This setting is located under Computer Configuration\Administrative Templates\System\Logon in the Group Policy Object Editor. For this setting to take effect Group Policy must be refreshed or the computer restarted.

Table 1 Timing of Synchronous and Asynchronous Processing

By default, how is policy processed on the client?	@ Startup	@ Logon	@ Policy Refresh
Windows 2000	Synchronously	Synchronously	Asynchronously
Windows XP Pro	Asynchronously	Asynchronously	Asynchronously
Windows Server 2003	Synchronously	Synchronously	Asynchronously

Note

Servers do not perform asynchronous processing.

Registry CSE

Administrative Template settings take the form of **true policies** or **preferences**. Preferences can be deployed using Group Policy, but they cannot be enforced to the same degree as true policies. For this reason they are hidden by default in the Group Policy Object Editor.

- Users can change preferences, but they cannot change true policies.
- True policies are more secure because they are stored in secured registry hives.
- Changes to true policies override but do not overwrite user preferences. If the policy is later removed, the user setting will again prevail.
- If the GPO ceases to apply to the user or computer, policies no longer apply but preferences remain. This occurs if the user or computer moves out of the site, domain, or OU that the GPO is linked to, or if the GPO is deleted.

If the setting you are using is a preference rather than a true policy be aware that because preferences can be overwritten but are not removed, the end user might see their behavior as unpredictable. As a result, there might be perceived problems even when preferences are behaving as intended.

Troubleshooting preferences requires knowledge about changes to both the GPO and the preferences set by the user.

The registry CSE writes the value for the setting to the registry. Some settings take effect as soon as they are written to the registry, but others take effect only at startup or logon. If you are not seeing the expected results and the Group Policy Results report shows that the policy has been applied, restart the computer or log off and log back on.

Scripts CSE

Startup, logon, logoff, and shutdown scripts can be applied using Group Policy settings. The Scripts CSE processes these script settings.

The Scripts CSE updates the registry with the location of one or more script files so that the UserInit process can find those values in the course of its normal processing. When a CSE reports success, it might only mean that the value has been placed in the registry. Even though the setting is in the registry, there could be problems preventing the setting from being applied to the client. For example, if a script specified in a Script setting has an error that prevents it from completing, that Script CSE does not detect error.

Scripts processing contains two steps:

1. Group Policy processes a GPO and stores the script information in the registry:
 - HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts (User Scripts)
 - HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts (Machine Scripts)

Note

Script is run by means of a UserInit process. (By default, scripts that cannot be completed time out after 10 minutes.)

Only Windows XP, Windows Server 2003, and later operating systems support WMI filtering. If the computer is running an earlier operating system, the WMI filter is ignored and the GPO is applied.

Note

The time-out is the time allotment for all scripts to run. This can be modified using the Computer policy setting: "Maximum wait time for Group Policy Scripts."

Common script errors include:

- Bad script path.
- Script time-out.
- Access to script is restricted by means of ACLs (typically for startup/shutdown scripts that run as computer, not user).

If a logon script fails, it typically does not affect the other scripts. However, startup scripts are often run synchronously, and a failure of one of these scripts can affect scripts intended to run later.

To investigate, check the Application Event Log for entries with UserInit as the source.

Software Installation CSE

A number of special issues affect Group Policy software installation. For example, network connectivity issues can disrupt access to the software installation packages. Software installation processing is never performed while the user is logged on because doing so could disrupt work and result in data loss. This has implications when Group Policy is configured to run asynchronously. These and other issues are addressed in the troubleshooting issues list in this section.

Software Installation is managed by the Software Installation CSE, which appears as the source **Application Manager** on the **Policy Events** tab in Group Policy Results reports. If you need additional logging information, enable verbose logging for the Software Installation CSE and Microsoft® Windows® Installer, as described under Appendix: Group Policy Log Files.

The Software Installation Diagnostics tool (addiag.exe) provides detailed information about the applications visible in Active Directory and installed for the current user, as well as general diagnostic information and related Event Log entries. It is available in the *Windows 2000 Server Resource Kit*.

Troubleshooting

- Startup and logon requirements
 - Software Installation processing occurs only during computer startup or when the user logs on. This is because processing periodically could cause undesirable results. For example, if an application is no longer assigned, it is removed. If a user were using the application while Group Policy tries to uninstall it or if an assigned application upgrade takes place while someone is using the application, errors would occur.
 - If the software installation settings are applied through computer configuration, they are applied at startup. If software installation settings are applied through user configuration, they are applied at logon.
 - If the computer is running Windows XP with logon optimization enabled, the user will need to log on after Group Policy refresh. This can entail logging on two or three times. For more information see [“Asynchronous Processing and Logon Optimization in Windows XP”](#) earlier in this paper.
- Access to share points
 - Test for mistyped elements in the path specification by manually following the path.
 - Verify that the user account or system account has the necessary privileges to traverse the path and access those resources. The account whose OU supplied the GPO is the one that needs to traverse the path.
- Computer versus User settings, and OU memberships
 - If the user has a roaming user profile and the user uninstalled the application on another computer using Add or Remove Programs, the application will be unavailable to that user on every computer (with the possible exception of computers where loopback processing rules apply). For more information about roaming user profiles, see “Using roaming user profiles” in Help and Support Center for Windows Server 2003.
 - If the application was deployed with the **Uninstall this application when it falls out of the scope of management** option, verify that the computer and user are still in the necessary security groups and that the GPO is still linked to a site, domain, or OU that the user or computer is in.
- Installation package
 - Windows Installer packages are the preferred packaging for software installation using Group Policy. ZAP files can be used but they do not support elevated installation privileges (the user must be an administrator or power user in order to install the software). Software installed with ZAP files cannot be repaired or removed by Group Policy after they are installed.

- If problems occur when a Windows Installer package is used, the problem could be with the package itself. For example, the package might be corrupted. For more information, see “Windows Installer” in Help and Support Center for Windows Server 2003. See also the Windows Installer topic “Managing options for computers through Group Policy” in Help and Support Center for Windows Server 2003.
- Add or Remove Programs
 - For the software to appear in the **Add New Programs** section of **Add or Remove Programs**, it must be **Published** (not **Assigned**) in Group Policy.
 - The Windows Installer package must be written such that the software can appear in Add or Remove Programs.
- Install on demand
 - Check the order of file name extensions specified for the GPO and ensure that the file name extension is associated with the application, as follows:
Edit the GPO. Find the **Software Settings** node; there is one under **Computer Configuration** and another under **User Configuration**. Right-click **Software Settings** and select **Properties**. Then click the **File Extensions** tab.
 - Check the client computer for applications that have been installed locally. If there is a conflict, the locally installed application is used instead of the deployed application.
- Terminal Services
 - User configuration settings for Software Installation cannot be applied to a terminal server. Use Terminal Services Manager to determine whether the computer is a terminal server.
 - If the application should be available on the terminal server, you must install it as an administrator at that computer. The administrator can install the application from Add or Remove Programs if has been Published using a Computer Configuration setting.

Folder Redirection CSE

Folder Redirection is used to maintain user data in a centralized location. This permits regular backups of the information, and also provides the user with access to the data from any computer in the network.

The following folders can be redirected:

- My Documents
- Application Data
- Desktop
- Start Menu

The Folder Redirection CSE manages folder Redirection. When events from this CSE are listed on the **Policy Events** tab in Group Policy Results reports, the source is listed as **Folder Redirection**.

Troubleshooting

- In order to use the folder, the file system and share permissions must be set such that the user can navigate the path to the folder, and if the folder exists the user must have ownership privileges on it.

(The user is given ownership of the folder by default if you allow the folder to be created automatically.) This is a common cause of confusion with folder redirection. When using Folder Redirection Policies, it is best to allow the system to create and set permissions on the folder. This reduces the likelihood of error due to incorrect security settings. For more information, see [User Data and Settings Management](http://go.microsoft.com/fwlink/?LinkId=15288) (<http://go.microsoft.com/fwlink/?LinkId=15288>).

- If you need to set permissions manually, ensure that the user has the appropriate minimum file system and share permissions. The permissions needed are shown in the tables below:

NTFS Permissions for Folder Redirection Root Folder

User Account	Minimum permissions required
Creator/Owner	Full Control, Subfolders And Files Only
Administrator	None
Security group of users needing to put data on share.	List Folder/Read Data, Create Folders/Append Data - This Folder Only
Everyone	No Permissions
Local System	Full Control, This Folder, Subfolders And Files

Share-Level (SMB) Permissions for Folder Redirection Share

User Account	Default Permissions	Minimum permissions required
Everyone	Full Control	No Permissions
Security group of users needing to put data on share.	N/A	Full Control,

NTFS Permissions for Each User's Redirected Folder

User Account	Default Permissions	Minimum permissions required
%Username%	Full Control, Owner Of Folder	Full Control, Owner Of Folder
Local System	Full Control	Full Control
Administrators	No Permissions	No Permissions
Everyone	No Permissions	No Permissions

- Folder Redirection, like Software Installation settings, can only be applied during computer startup or user logon. On computers running Windows XP with logon optimization enabled, this can mean that the user needs to log on more than once before the setting takes effect. For more information see [“Asynchronous Processing and Logon Optimization in Windows XP”](#) in this paper.
- If the path to the folder does not exist (for example if the path specification is mistyped in the policy setting, if folders in the path have been renamed or removed, or if the server is unavailable), Folder Redirection will fail.
- Ensure that the correct Fdeploy.ini file is available on the domain controller that the client is accessing.

Troubleshooting Group Policy Administration

The primary focus of this white paper is on problems with the application of Group Policy at the client. However there are a few issues of which you should be aware when performing or delegating Group Policy administration.

Domain Controller Selection in the Group Policy Object Editor and GPMC

Each domain controller has a copy of every GPO in the domain. The default and best practice is to edit GPOs on the primary domain controller (the PDC Emulator), and allow the changes to replicate to other domain controllers.

If that is not practical due to bandwidth or other issues, administrators can change the domain controller focus for the instances of GPMC that they are using.

Troubleshooting

- If administrators in your organization edit GPOs on different domain controllers, set up processes to avoid this sort of conflict. For example, you might delegate editing permissions on individual GPOs to specific users, or to a group that focuses on the same domain controller.

Security

In order to administer Group Policy, you must have the necessary privileges to use GPMC and the Group Policy Object Editor. You also need privileges to create GPOs or to manage links from a specific site, domain, or OU to GPOs. Control of existing GPOs can be delegated to specific users or groups, so it is possible for an administrator to be able to use GPMC to view GPOs, but not be able to modify, delete, or link them.

Troubleshooting

- Use Active Directory Users and Computers to verify that the account you are using is a member of a group that has these privileges. (Check the group memberships for the user account, and also verify that the privileges for the group have not been changed.)
- Avoid adding the privileges to an individual user account. If necessary create a new group with a name that clearly indicates its purpose.
- Changes to security groups' memberships or privileges, or to the permissions on Group Policy objects or actions, need to be replicated to domain controllers throughout the system. Until this replication is completed the changes might be applied unevenly. In rare cases you might want to force replication.
- To see or change the access control lists that affect management of a GPO, open the GPO in GPMC and look at the **Delegation** tab. The GPO can only be applied by members of groups that have **Read** permissions. To change the security filters, click **Advanced**.

Exposing Preferences in Administrative Templates

Administrative Templates can contain both true policies and preferences, but by default the Group Policy Object Editor exposes only true policies. To expose preferences, highlight the Administrative Templates node for which you want to see preferences. On the **View** menu, click **Filtering**, and then clear the **Only show policy settings that can be fully managed** check box.

Troubleshooting Tools

GPMC is the preferred tool for administering Group Policy and is also an excellent tool for troubleshooting Group Policy. Several other tools are available from the Windows Server 2003 CD, from the *Windows 2000 Server Resource Kit*, or as free downloads from www.microsoft.com.

GPMC as a Troubleshooting Tool

You can get a lot of well-organized information about how Group Policy has been applied on a specific client by generating a Group Policy Results report for the client, as discussed in the following section. You can also test proposed changes to Group Policy by generating a Group Policy Modeling report.

GPMC includes several other features that will help you troubleshoot Group Policy:

- The GPMC user interface clarifies the relationship between GPOs, the Active Directory objects that link to them, and the sites and domains where they reside.
- You can easily see which links are enabled.
- You can automate many tasks using scripting, including tasks such as reporting that support troubleshooting.
- You can view GPO properties by clicking on the GPO or on any link to the GPO and looking at the information on the various tabs.

In addition, two types of reports can be generated for clients running Windows XP or Windows Server 2003:

- Group Policy Modeling reports are used to predict the policies that will be applied at a specific client. A Windows Server 2003 domain controller is required to generate Group Policy Modeling reports.
- Group Policy Results reports gather information directly from the client to show the policies in effect, and include key policy events that have been logged at that client.

Both of these reports include valuable troubleshooting information. For example, you can see a list of the GPOs applied, and also the denied GPOs with the reason for denial. You can see which settings are or would be applied, and the winning GPO that supplied the value for the setting.

Group Policy Results

GPMC leverages the RSoP functionality in Windows Server 2003 and Windows XP to provide reports on the way Group Policy is applied at individual clients. Because these reports rely on functionality that is new with Windows XP and Windows Server 2003, the clients for which you generate the reports must be running one of these operating systems.

To generate a Group Policy Results report:

Right-click **Group Policy Results**, at the bottom of the navigation pane, and select **Group Policy Results Wizard**. In the wizard, specify the computer or computer/user combination you want to investigate. The report that appears in the details pane provides information about Group Policy application on the client.

Summary Tab

On the **Summary** tab, the following sections appear under both Computer Configuration and User Configuration headings as shown in Table 2.

Table 2 Summary Tab of Group Policy Results Reports

Section on the Tab	Information
General	Computer name The domain and site of which the computer is a member The last time Group Policy from the computer's Active Directory hierarchy was applied User name (if any) The domain and site of which the user is a member The last time Group Policy from the user's Active Directory hierarchy was applied
Group Policy Objects Applied	List of GPOs that were applied.
Group Policy Objects Denied	List of GPOs that were denied, with the reason for the failure.
Security Group Membership when Group Policy was applied	Security group memberships in effect when group policies were evaluated.
WMI Filters	WMI filters that were applied, whether they evaluated as True or False, and what GPO called them.
Component Status	Success or failure, including errors, of core client Group Policy functionality and CSEs.

Settings Tab

On the **Settings** tab you will find a list of the actual settings applied. These are sorted by the source of the setting, for example Computer Configuration/Windows Settings or User Configuration/Administrative Templates. The report includes the winning GPO for each setting.

With this information you can easily locate the GPO in the navigation pane. The information exposed when you click the GPO depends on the privileges granted to your user account. If you have sufficient privileges, you can review or edit the settings and also get a list of the sites, domains, and OUs that link to that GPO.

Policy Events Tab

When you use GPMC to generate a report of the resulting set of policy on a client, events that were logged at that client and pertain to Group Policy are listed on the **Policy Events** tab. Sources for these

events include the core Group Policy engine on the client (the UserEnv process) and the CSEs for Group Policy.

The display on the **Policy Events** tab is similar to the Event Viewer display. In fact, the events are what you would see if you looked at Event Viewer on the client and filtered for the sources that influence Group Policy. The sources are defined in Table 3.

Note

To view the Group Policy events on computers running Windows XP SP1 or Windows Server 2003 you must be a local administrator that computer. If you have the necessary privileges to generate a Group Policy Results report but you do not have the privileges to view Group Policy events on the client, the **Policy** tab will display the message “Unable to open event log: Access is Denied” instead of the list of events.

Table 3 Policy Events Tab of Group Policy Results Reports

Source Name in Policy Events Log	Full name of source	Functionality
UserEnv	User Environment (Group Policy core engine)	Locates and applies GPOs at startup, logon, or the configured Policy Refresh Interval.
SceCli	Security CSE	Reads all GPOs that reach the client and determines which policy settings are applied.
Application Management	Software Installation CSE	Processes Software Installation settings, including installation, upgrades, and removal.
Folder Redirection	Folder Redirection CSE	Processes Folder Redirection.
UserInit	Scripts CSE	Implements logon, logoff, startup, and shutdown scripts

To avoid flooding the client log file, some logging is blocked in certain situations. For example, if a computer is not connected to the network and a user logs on with cached credentials, the **Component Status** entries on the **Summary** tab of the Group Policy Results report show the failure to access and apply Group Policies. However, the list of associated failure events do not appear in the Application event log on the client or on the **Policy Events** tab.

Note

By default, UserEnv logging is not verbose – only errors and warnings are reported, and these are all that appear on the **Policy Events** tab. For more information, see [Appendix: Group Policy Log Files](#).

Group Policy Modeling

Before you implement a GPO, use Group Policy Modeling to validate the effect it will have. The Group Policy Modeling report has the information on the **Summary** and **Settings** tabs similar to what you would see for a Group Policy Results report. Group Policy Modeling reports do not collect policy events from the client. Instead of the **Policy Events** tab, there is a **Query** tab that lists the conditions that were applied when creating the model.

To generate a Group Policy Modeling report:

Right-click **Group Policy Modeling**, near the bottom of the navigation pane, and select **Group Policy Modeling Wizard**. In the wizard, specify the computer or computer/user combination you want to investigate. The report that appears in the details pane provides information about the anticipated Group Policy application on that client.

Viewing Active Directory Objects and GPOs

There are a few quick checks you can make in GPMC. For example, by looking at the icons in the navigation pane you can quickly see which links are disabled, which GPOs have some settings disabled, which GPOs have all settings disabled, and where in the hierarchy inheritance is blocked. For more information, see the guide to icons in GPMC Help.

Scripting Built-in to GPMC

You can use GPMC sample scripts to quickly perform a number of different troubleshooting tasks. If you can't find a sample script that fits your needs, you can easily modify a sample script, or create your own script. The following sample scripts will help you troubleshoot various issues:

- List All GPOs in a Domain: ListAllGPOs.wsf
- List Disabled GPOs: FindDisabledGPOs.wsf
- List GPO Information: DumpGPOInfo.wsf
- List GPOs at a Backup Location: QueryBackupLocation.wsf
- List GPOs by Policy Extension: FindGPOsByPolicyExtension.wsf
- List GPOs by Security Group: FindGPOsBySecurityGroup.wsf
- List GPOs Orphaned in SYSVOL: FindOrphanGPOsInSYSVOL.wsf
- List GPOs With Duplicate Names: FindDuplicateNamedGPOs.wsf
- List GPOs Without Security Filtering: FindGPOsWithNoSecurityFiltering.wsf
- List SOM Information: DumpSOMInfo.wsf
- List SOMs With Links to GPOs in External Domains: FindSOMsWithExternalGPOLinks.wsf
- List Unlinked GPOs in a Domain: FindUnlinkedGPOs.wsf
- Print the SOM Policy Tree: ListSOMPolicyTree.wsf

For a complete list of available sample scripts, script documentation and a list of scripting interfaces exposed by GPMC, please see the Group Policy Management Console SDK located at **%programfiles%\gpmc\scripts\gpmc.chm** on any computer where GPMC has been installed. (The Group Policy Management Console SDK is only available in English.).

Other Group Policy Tools

In addition to the Group Policy-specific command-line tools listed here, a number Active Directory support tools are listed in “Active Directory support tools” in Help and Support Center for Windows Server 2003.

GPResult.exe

There are two versions of GPResult.exe.

- The Windows 2000 version shipped in the *Windows 2000 Resource Kit*, and is also available as a free download on the [Windows 2000 downloads site](http://go.microsoft.com/fwlink/?LinkId=12920) (<http://go.microsoft.com/fwlink/?LinkId=12920>). It estimates the Group Policy settings that would be applied at a specific computer. For more information, see the readme file included with the download.
- The Windows Server 2003 version is included with Windows Server 2003 operating systems. It gathers and reports the RSoP data available from computers running Windows XP or Windows Server 2003. The report is similar to what you would get by generated a Group Policy Results report in GPMC. For more information, see “Gpresult” in Help and Support Center for Windows Server 2003.

GPMonitor.exe

The Group Policy Monitor tool, `gpmonitor.exe`, collects information at every Group Policy refresh and sends that information to a centralized location that you specify. There are two parts to this tool, the `gpmonitor` service, which collects the data at the client and sends it to the central location, and a viewer that you can use to examine the data. Both portions are wrapped in a Windows Installer package.

`Gpmonitor` is included in the *Windows Server 2003 Deployment Kit*. For more information, see the `Gpmonitor` Help.

GPOTool.exe

`GPOTool.exe` is a command-line tool to be used in replicated domains—domains that contain more than one domain controller. It traverses all of your domain controllers and checks each for consistency between the Group Policy container (information contained in the directory service) and the Group Policy template (information contained in the `SYSVOL` share on the domain controller). The tool also determines whether the policies are valid and consistent between all of your domain controllers and displays detailed information about the Group Policy objects (GPOs) that have been replicated between your domain controllers.

If you suspect you are having problems with replication of Group Policy information, this tool will help you diagnose and isolate where Group Policy is not being replicated properly. Additional features let you do the following:

- Search for specific GPO information, based on the name or the globally unique identifiers (GUIDs) of that GPO.
- Limit your checking to specific or preferred domain controllers.
- Go to other domains and verify that policies are replicating across these domains—other than the domain you are currently working in.

GPOTool can do any of the following:

- **Check Group Policy object consistency.** The tool reads mandatory and optional directory services properties, version, friendly name, extension, GUIDs and SYSVOL data, compares directory services and SYSVOL version numbers, and performs other consistency checks. Functionality version must be 2 and user/computer version must be greater than 0 if the extensions property contains any GUID. The tool also checks the timestamps of GPOs in the SYSVOL folder.
- **Check Group Policy object replication.** It reads the Group Policy object instances from each domain controller and compares them (selected Group Policy container properties and full recursive compare for the Group Policy template).
- **Display information about a particular Group Policy object.** This includes properties that can't be accessed through the Group Policy snap-in such as functionality version and extension GUIDs.
- **Browse Group Policy objects.** A command-line option can search policies based on friendly name or GUID. A partial match is also supported for both name and GUID.
- **Use preferred domain controllers.** By default, all available domain controllers in the domain will be used; this can be overwritten with the supplied list of domain controllers from the command line.
- **Provide cross-domain support.** A command-line option is available for checking policies in different domains.
- **Run in verbose mode.** If all policies are fine, the tool displays a validation message; in case of errors, information about corrupted policies is printed. A command-line option can turn on verbose information about each policy being processed.

GPOTool.exe ships with the *Microsoft Windows® 2000 Server Resource Kit* and is also available as a free download at [Gpotool.exe: Group Policy Verification Tool](http://go.microsoft.com/fwlink/?LinkId=17911) (<http://go.microsoft.com/fwlink/?LinkId=17911>). For more information see the *Windows 2000 Server Resource Kit*.

Software Installation Diagnostics Tool (addiag.exe)

The *Windows 2000 Server Resource Kit* includes an advanced troubleshooting tool, Software Installation Diagnostics (addiag.exe) that you can use to gather additional diagnostic information when troubleshooting Software Installation policy issues.

The binary executable for this tool is Addiag.exe. Running `addi ag. exe /?` from a command prompt provides the usage syntax.

This tool displays detailed information about the applications visible in Active Directory and installed for the current user, as well as general diagnostic information and related Event Log entries.

Tools for Troubleshooting External Issues

Sonar.exe

Sonar is a command-line tool that allows administrators to monitor key statistics and status about members of a file replication service (FRS) replica set. Use Sonar to watch key statistics on a replica set in order to monitor traffic levels, backlogs, and free space. Sonar is available as a free download from [Sonar.exe: FRS Status Viewer](http://go.microsoft.com/fwlink/?LinkId=16719) (<http://go.microsoft.com/fwlink/?LinkId=16719>).

Active Directory Support Tools

Help and Support Center in Windows Server 2003 provides a list of Active Directory support tools in the topic “Active Directory support tools”. Use these tools to troubleshoot Active Directory issues.

Other Windows Server 2003 Command-Line Tools

Windows Server 2003 includes a number of command line tools including ping.exe, netdiag.exe, and dcdiag.exe. For a complete reference of the tools included with Windows Server 2003, see “Command-line Reference A-Z” in Help and Support Center for Windows Server 2003.

Appendix: Group Policy Log Files

If other tools do not provide the information you need to identify the problems affecting Group Policy application, you can enable verbose logging and examine the resulting log files. Verbose logging can reduce performance and consume significant disk space, so as a best practice enable verbose logging only when necessary.

Client Log Files

Log files can be generated by the core client engine (UserEnv) and by every CSE except the Scripts CSE. Scripts processing is logged in the Application log on the client with source=UserInit. Use Event Viewer to view the Application log on the client, or look for these entries on the **Policy Events** tab of the Group Policy Results report.

The **Policy Events** tab in Group Policy Results reports generated in GPMC displays the Group Policy-related events that you would see if you used Event Viewer to view these events in the Application log on the client for which you generated the report.

Table 4 lists several log files you can generate at the client that relate to Group Policy troubleshooting.

Table 4 Client Log Files for Troubleshooting Group Policy -

Output from:	Is located in this file:	Enable verbose logging by adding this key or value...	...to this registry key
Group Policy core (UserEnv) and registry CSE	%windir%\debug\usermode\UserEnv.log	UserEnvDebugLevel = REG_DWORD 0x10002	HKEY_LOCAL_MACHINE \Software \Microsoft \Windows NT \CurrentVersion \Winlogon
Security CSE	%windir%\security\logs\winlogon.log	ExtensionDebugLevel = REG_DWORD 0x2	HKEY_LOCAL_MACHINE \Software \Microsoft \Windows NT \CurrentVersion \Winlogon \GpExtensions \{827d319e-6eac-11d2-a4ea-00c04f79f83a}\
Folder Redirection CSE	windir%\debug\usermode\fddeploy.log	FdeployDebugLevel = Reg_DWORD 0x0f	HKEY_LOCAL_MACHINE \Software \Microsoft \Windows NT \CurrentVersion \Diagnostics
Software Installation CSE	%windir%\debug\usermode\appmgmt.log	Appmgmtdebuglevel=dword:0000009b	HKEY_LOCAL_MACHINE \Software \Microsoft \Windows NT \CurrentVersion \Diagnostics
Windows Installer (deployment-related actions)	%windir%\temp\MSI*.log	Logging = voicewarmup Debug = DWORD: 00000003	HKEY_LOCAL_MACHINE \Software \Policies \Microsoft \Windows \Installer
Windows Installer (user-initiated actions)	%temp%\MSI*.log	Logging = voicewarmup Debug = DWORD: 00000003	HKEY_LOCAL_MACHINE \Software \Policies \Microsoft \Windows \Installer

Notes

The UserEnv logs entries pertaining to profiles as well as Group Policy core processing and registry (.adm) processing on the client. The entries pertaining to profiles are intermingled with the Group Policy entries and not easily distinguished from them.

Use Wilogutl.exe to analyze the Windows Installer log files. For more information see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/wilogutl_exe.asp (<http://go.microsoft.com/fwlink/?LinkID=16156>).

Server Log Files

You can enable logging of events generated by the Group Policy Object Editor on the Server. There are two different log files, one for events relating to core Group Policy processing and the registry CSE, and another for events relating to all other CSEs.

Table 5 lists several log files you can generate at the server that relate to Group Policy troubleshooting.

Table 5 Server Log Files for Troubleshooting Group Policy

Output from:	Is located in this file:	Enable verbose logging by adding this keyword...	...to this registry key
GPMC: error logging only	%temp%\gpmgmt.log	gpmgmttracelevel=1	HKEY_LOCAL_MACHINE \\Software \\Microsoft \\Windows NT \\CurrentVersion \\Diagnostics
GPMC: error and verbose logging	%temp%\gpmgmt.log	gpmgmttracelevel=2	HKEY_LOCAL_MACHINE \\Software \\Microsoft \\Windows NT \\CurrentVersion \\Diagnostics
GPMC: Output only to log file (not to debugger)	%temp%\gpmgmt.log	gpmgmtlogfileonly=1	HKEY_LOCAL_MACHINE \\Software \\Microsoft \\Windows NT \\CurrentVersion \\Diagnostics
Group Policy Object Editor: Core-specific entries	%windir%\debug\usermode \gpedit.log	GPEditDebugLevel = REG_DWORD 0x10002	HKEY_LOCAL_MACHINE \\Software \\Microsoft \\Windows NT \\CurrentVersion \\Winlogon
Group Policy Object Editor: CSE-specific entries	%windir%\debug\usermode \gptext.log	GPTTextDebugLevel = REG_DWORD 0x10002	HKEY_LOCAL_MACHINE \\Software \\Microsoft \\Windows NT \\CurrentVersion \\Winlogon

Appendix: Migrating from Windows NT 4.0

If the client computer is running Windows 2000 Professional, Windows XP Professional, or Windows Server 2003, and if the computer and user accounts both belong to Windows NT 4.0-based domains, that client will continue to receive system policy. If the domain is running Windows 2000 or Windows Server 2003, the client will only receive Group Policy.

If the user account is in Active Directory and the system account is in Windows NT 4.0, then the computer gets system policy and the user gets Group Policy—and vice-versa.

If you are planning on using sites, keep in mind that if a site is determined by the IP subnet a computer is in, Group Policy will only be applied if the computer is running Windows 2000 or later and the computer is in a Windows 2000 or Windows Server 2003 domain that is using Active Directory.

Note

The local GPO is processed regardless of the configuration. For details about how Group Policy is applied with various configurations, see Table 6.

Table 6 Migrating from Windows NT 4.0: Group Policy Application

Backend	Account Object Location	What Affects the Client
Windows NT 4.0	Computer: Windows NT 4.0	At computer startup: Computer local Group Policy (only if changed). Every time the user logs on: Computer System Policy.
“	Computer refresh	Before Control-Alt-Delete: Computer local Group Policy only. After the user logs on: Computer local Group Policy and computer System Policy.
“	User: Windows NT 4.0	When the user logs on: User System Policy. If local Group Policy changes: User local Group Policy and user System Policy.
“	User refresh	User local Group Policy and user System Policy.
Mixed (migration)	Computer: Windows NT 4.0	At computer startup: Computer local Group Policy (only if changed). Every time the user logs on: Computer System Policy.
	Computer refresh	Before Control-Alt-Delete: Computer local Group Policy only. After the user logs on: Computer local Group Policy and computer System Policy.
	User: Windows 2000 later.	When the user logs on: Group Policy is processed after computer System Policy.
	User refresh	User Group Policy.
Mixed (migration)	Computer: Windows 2000 or later	During system startup: Group Policy.
	Computer refresh	Computer Group Policy
	User: Windows NT 4.0	When the user logs on: User System Policy. If local Group Policy changes: User local Group Policy and user System Policy.
	User refresh	User local Group Policy and user System Policy.
Windows 2000 or later	Computer: Windows 2000 or later	During computer startup and when the user logs on: Group Policy.
	User: Windows 2000 or later	
Windows 2000 or later in a workgroup (without Active Directory)	Local	Local Group Policy only.

If your computer/user account is in a Windows 2000 domain that cannot be reached (for example, you are logging on with cached credentials), then all Group Policy processing, including the local GPO, will not be processed.

Appendix: Group Policy and Roaming User Profiles

Roaming User Profiles (RUP) provide users the same desktop experience regardless of which computer in the domain they log on to. This is done by storing the profile information on a server and copying them to the local computer when the user is authenticated, unless the local copy of the profile for that user is more recent. The RUP includes Group Policy settings for user configuration in addition to any modifications the user makes to the user's own profile.

Troubleshooting

- Roaming user profiles, like Software Installation settings, can only be applied during logon. On computers running Windows XP with logon optimization enabled, this can mean that the user needs to log on more than once before the setting takes effect. For more information see "[Asynchronous Processing and Logon Optimization in Windows XP](#)" earlier in this paper.
- If the server is not available when the user logs on, both of the following occur:
- The local cached copy of the user's profile is used. Or, if there is no local profile for this user, a new local user profile is created.
- The profile on the server is not updated when the user logs on.
- A new setting in Windows Server 2003, **Only allow local user profiles setting**, can be used to prevent roaming user profiles from being applied at specific computers. You can check for this setting on the **Settings** tab of the Group Policy Results or Group Policy Modeling report.

Appendix: Resources

This section contains links to more information about Group Policy and related technologies.

- [Microsoft.com Group Policy Home Page](http://go.microsoft.com/fwlink/?LinkId=17530) (http://go.microsoft.com/fwlink/?LinkId=17530). Provides an entry point for Group Policy documentation on the Web. Includes links to documentation, knowledge base articles, support information, and newsgroups.
- [Windows Server 2003 Deployment Kit, Designing a Managed Environment Book](http://go.microsoft.com/fwlink/?linkid=15311) (http://go.microsoft.com/fwlink/?linkid=15311). Describes the technologies in Windows 2003 associated with deployment of a managed environment. Has significant coverage of Group Policy and related IntelliMirror technologies. Includes planning, designing and implementation guidance.
- [Help and Support Center for Windows Server 2003](http://go.microsoft.com/fwlink/?LinkId=4299) (http://go.microsoft.com/fwlink/?LinkId=4299). Point-of-use information for administrators of networks based on Windows Server 2003.
- “[Group Policy Administration using the Group Policy Management Console](http://go.microsoft.com/fwlink/?LinkId=14320)” whitepaper (http://go.microsoft.com/fwlink/?LinkId=14320). Provides technical details of functionality in GPMC.
- “[Migrating GPOs Across Domains Using the Group Policy Management Console](http://go.microsoft.com/fwlink/?LinkId=14321)” white paper (http://go.microsoft.com/fwlink/?LinkId=14321). Explains how to move GPOs from one domain to another using GPMC.
- “[Windows Server 2003 Group Policy Infrastructure](http://go.microsoft.com/fwlink/?LinkId=14950)” white paper (http://go.microsoft.com/fwlink/?LinkId=14950). Describes a range of topics related to Group Policy at both the server and the client level. Includes detailed Group Policy processing as well as many best practices useful to the Group Policy administrator.
- [Group Policy Management Console Software Development Kit \(SDK\)](http://go.microsoft.com/fwlink/?LinkId=17912) (http://go.microsoft.com/fwlink/?LinkId=17912). Provides information about how to use the COM interfaces of Group Policy Management, which support scripting many of the operations supported by Group Policy Management Console.
- “[User Data and Settings Management](http://go.microsoft.com/fwlink/?LinkId=15288)” (http://go.microsoft.com/fwlink/?LinkId=15288) white paper
- [Windows 2000 Server Resource Kit](http://go.microsoft.com/fwlink/?LinkId=458) (http://go.microsoft.com/fwlink/?LinkId=458). Delivers reference and tools for Windows Server 2003.

Feedback on this Paper

If you have any comments about this paper, contact <mailto:gpdocs@microsoft.com>.

Newsgroups About Group Policy

If you have a question about Group Policy, you can post to the newsgroup “microsoft.public.windows.group_policy.”