



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials Bootcamp Style (Security 401)"  
at <http://www.giac.org/registration/gsec>

## **Management Challenges of Windows 2000 Group Policy**

Mark Sanders

December 13, 2001

### **Introduction**

Group Policy is the primary tool for change and configuration management (CCM) in Windows 2000. It carries out its functionality through the use of Group Policy Objects (GPOs). GPOs leverage Windows 2000 Active Directory (AD) to allow administrators to control the behavior of their servers and workstations. Group Policy Objects can contain hundreds of settings ranging from user rights to system services, and can be applied in a hierarchical fashion to Organization Units (OUs) in AD.

Although these very granular policies can be easily created, the tools provided by Microsoft to maintain and troubleshoot Group Policies are less than adequate. There are however third party tools available, such as FAZAM 2000, which help with some of the features which are native GPO tools are lacking.

### **Native Group Policy Management Tools**

Windows 2000 provides the following native tools for managing and troubleshooting the application of GPOs in an enterprise.

#### GPResult

This group policy results tool displays the policies that have been applied to the computer on which the command was run on, as well as the policies that have been applied to the user that is currently logged on. The /c and /u switches can be used to display the basic computer or user policies, while the /v and /s switches expand the level of detail of the policy results.

According to Microsoft's website,

<http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/gpresult-o.asp>, the basic level of group policy results include the following:

- Operating System
- Type (Professional, Server, Domain Controller)
- Build number and Service Pack details.
- Whether Terminal Services is installed and, if so, the mode it is using.
- User Information
- User name and location in Active Directory (if applicable).
- Domain name and type (Windows 2000 or Windows NT).
- Site name.
- Whether the user has a local or roaming profile and location of the profile.
- Security group membership.
- Security privileges.
- Computer Information.

- Computer name and location in Active Directory (if applicable).
- Domain name and type (Windows 2000 or Windows NT).
- Site name.

In addition, the expanded group policy results include the following:

- The last time policy was applied and the domain controller that applied policy, for the user and computer.
- The complete list of applied Group Policy Objects and their details, including a summary of the extensions that each Group Policy Object contains.
- Registry settings that were applied and their details.
- Folders that are re-directed and their details.
- Software management information detailing assigned and published applications.
- Disk quota information.
- IP Security settings.
- Scripts.

### GPOTool

This group policy verification tool is used to test the status of GPOs on domain controllers (DCs). Running the tool without switches displays a list of the Group Policy Objects by their globally unique identifiers (GUIDs) and the status of each. The /verbose switch displays the friendly name of the GPO, its created and modified dates, version IDs, and machine and user Group Policy Extension GUIDs. Gpoutil.exe is especially useful for verifying properties such as replication of Group Policy Objects between domain controllers, because it reads the GPO instances from each DC in the domain and runs a recursive comparison of the content. It can be used to display information such as functionality version and extension GUIDs, as well as search GPOs based on friendly name or GUID.

### Security Configuration and Management Snap-in

From Microsoft's website, <http://www.microsoft.com/ntserver/techresources/security/SecurConfigToolSet.asp>, the Security Configuration and Analysis snap-in provides administrators with a single graphical utility that can be used to configure and analyze virtually every aspect of a system that relates to security.

The snap-in can first be used to analyze a local system against a pre-defined security template. The results of this analysis are stored in a security configuration database. Once this is done, the database can be opened and viewed to see the differences in the policy defined in the template and the policies applied to the system.

This analysis can be used to verify that the settings in the policy are actually being applied to the local system. This will not always be the case, especially if there are a hierarchy of GPOs being pushed down by Active Directory to the local system, since generally the last setting applied wins out. For this reason, it is important to be able to determine a Resultant Set of Policies of a particular system, rather than just the comparison of one template to the effective policy settings.

## Issues with Native Management Tools

The tools provided with Windows 2000 provide some management and troubleshooting features, but there are also several important features that seem to have been left out.

### Documentation of GPO Settings

Each Group Policy Object has over 680 computer and user settings, including:

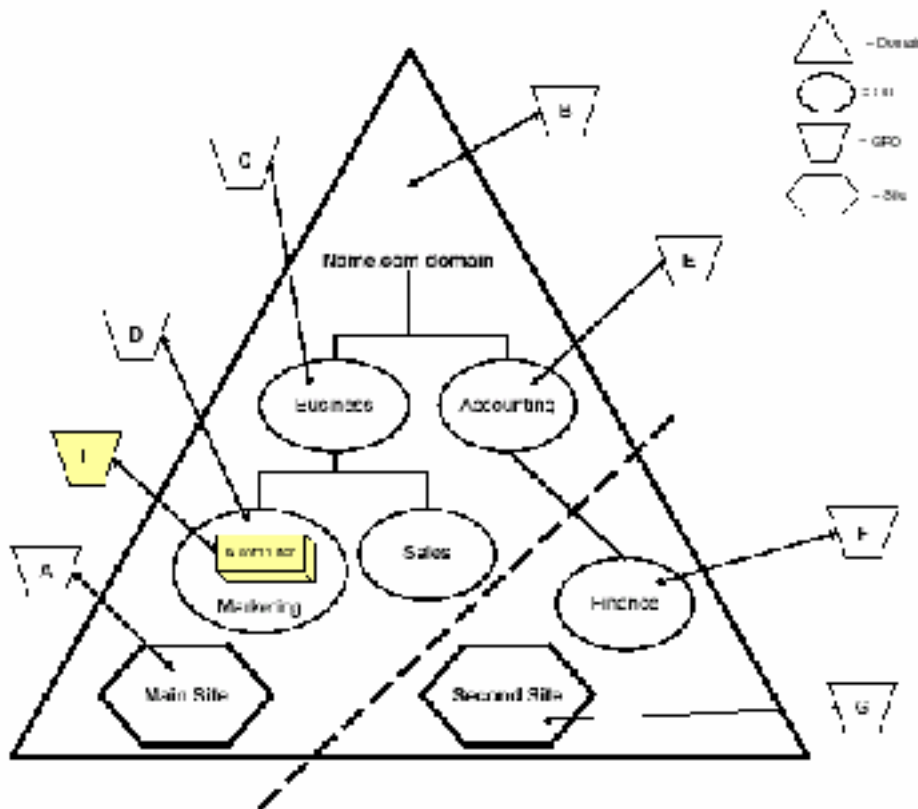
- Account Policies
- Local Policies
- Event Log Policies
- Restricted Groups
- System Services
- Registry Permissions
- File System Permissions

Although it is fairly easy to view the settings of a GPO with native Windows 2000 tools, there is no simple way to export them into a report. The only mechanism for doing this is by saving each subsection of the policy off individually with the Security Configuration and Management Snap-in pasting them together in a text document or spreadsheet. Not only is this a very tedious process when dealing with numerous GPOs, the process only works for the standard policy settings and not for Registry or File System permissions. Therefore, it is impossible with the native tools to easily and accurately track the settings contained within each GPO.

### Resultant Set of Policies (RSOP)

As stated from Full Armor's website, [http://www.fullarmor.com/pdf/EliminatingGPMgmtChallenges\\_v11\\_010119.pdf](http://www.fullarmor.com/pdf/EliminatingGPMgmtChallenges_v11_010119.pdf), Group Policies are a collection of numerous computer and user settings. They can be applied alone or in combination at several different levels within an organization: across an entire domain, to individual organization units (OUs) within the domain, or even to specific portions of the physical network (known as sites). Since policy objects can have their own access control lists (ACLs), it is possible to assign policy to specific groups in the organization.

A resultant set of policies (RSOP) is the effective policies which a specific user at a specific machine will receive. Since policies can be applied at many different levels of OUs in Active Directory, it is very important to know exactly which policy settings may be overwritten by other GPOs. This is based on the LSDOU (Local, Site, Domain, OU) hierarchy of policy evaluations used by Windows 2000. The figure below, taken from the Full Armor website, illustrates the hierarchical nature of Group Policies in Active Directory.



Based on this figure and the formula Local + Site + Domain + OUs, a user in the Marketing OU would receive a RSoP of L + A + B + (C+D), while a user's in the Finance OU would be (none) + G + B + (E+F).

While the Security Configuration and Management Snap-in can compare one policy to that of the effective policies on a system, it cannot determine the RSoP on an OU. For both planning and troubleshooting GPO issues, a quick way to view or analyze RSoPs is an operational necessity.

### GPO Management

Although GPOResult and GPOTool provide ways to view policy attributes of a local system, neither will work to determine the state of GPOs on a remote system. In an enterprise environment, it is essential to be able to monitor and troubleshoot Group Policy issues remotely.

With over 680 settings, Group Policy Objects could potentially take months to develop, and the ability to backup and restore Group Policy Objects is an essential feature. This can also be helpful while migrating GPOs from a test domain to a production domain. However, Windows 2000 only allows for backing up and restoring of the entire Active Directory.

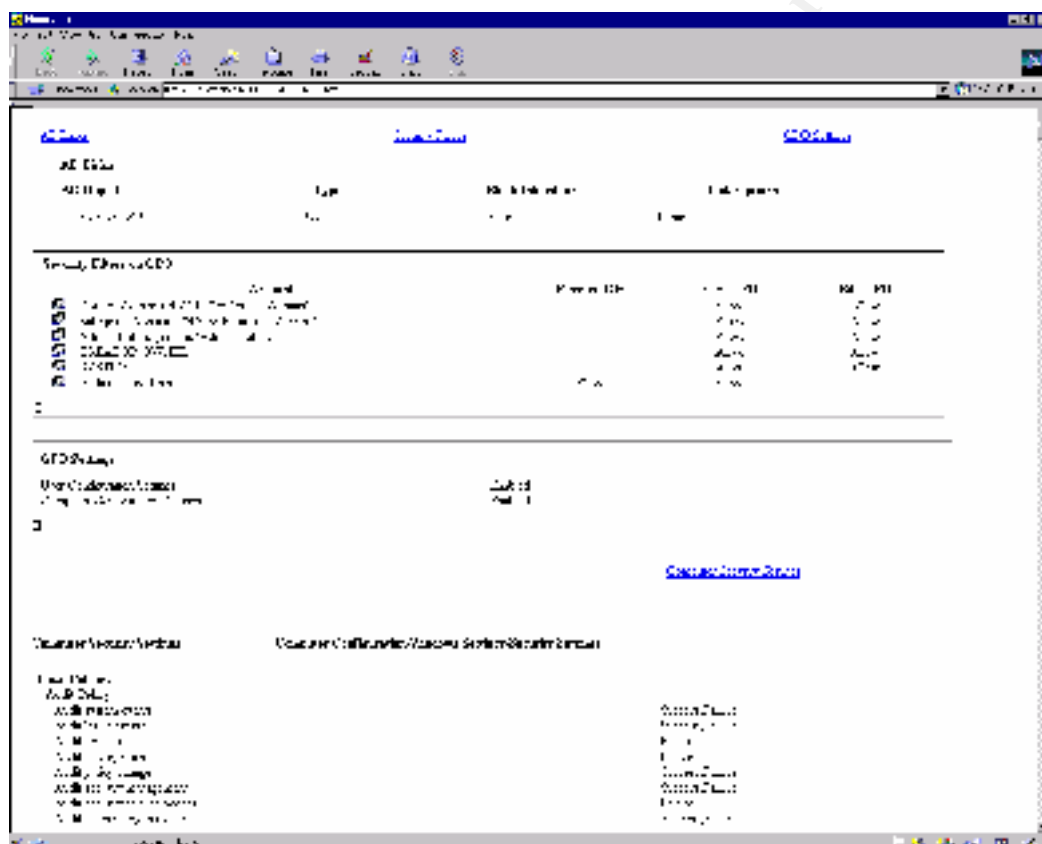
### **FAZAM 2000**

Third party products are available to enhance the native Windows 2000 group policy tools. One in particular, which is actually endorsed by Microsoft, is Full Armor's FAZAM 2000 (Full Armor Zero Administration). Their product was designed to complement and extend Microsoft's native policy management tools to cover the previously mentioned issues.

### Documentation of GPO Settings

FAZAM 2000 provides extensive reporting capability of GPO settings. Each setting of a Group Policy Object that has been set is displayed on the FAZAM report, including settings made in the Administrative Templates, Registry, and File System subsections. They contain descriptive information about policy settings that have been enabled or disabled and the actual registry key names and their values, respectively. The reports can also be easily exported to a MS Access database, where settings can be queried or compared, or as an HTML file.

The following figure is an example of a GPO report exported as an HTML file:



### Resultant Set of Policies (RSOP)

FAZAM allows for the use of RSOP. This becomes essential for administrators to carry out policy enforcement and management tasks. From a planning perspective, FAZAM provides a way for previewing the result of a set of Group Policies to a user or computer before they are actually applied in Active Directory. Natively, the policies must first be applied to AD before

the effective settings can be verified. This inability to plan the application of multiple policies before they are added to AD would likely result in additional time and effort required to fix the problems afterwards.

From a troubleshooting perspective, the RSoP is an effective tool for help desk use as well. This would allow for the help desk personnel to determine exactly what policies have been applied to a particular system that may be causing problems due to conflicting GPO settings.

## GPO Management

As stated from Full Armor's website , [http://www.fullarmor.com/pdf/Man\\_Enterprise\\_Pol\\_FAZAM2000.pdf](http://www.fullarmor.com/pdf/Man_Enterprise_Pol_FAZAM2000.pdf) , FAZAM 2000 Remote Diagnostics feature provides the ability to connect and carry out diagnostics on a remote machine. On connecting to the remote machine, the FAZAM diagnostics console interacts with a client agent to provide information on GPOs that were downloaded and applied on that machine by virtue of machine and user policies. The Remote Diagnostics feature displays the GPO information for not only the current user logged on to the machine, but for all user accounts that have logged on from that machine as well.

FAZAM also offers backup and restore functions for GPOs. These functions include backing up and restoring the following:

- GPO settings
- Links to AD objects
- Security information

## **Conclusion**

Although the native Windows 2000s Group Policy tools offer some great features to manage Group Policy Objects, there are many limitations with the native tools used for administering the GPOs. These limitations mainly consist of GPO management features, reporting features, and ability to provide a resultant set of policies. Therefore, though the use of some Windows 2000 third party tools, such as FAZAM 2000, administrators can be better equipped to manage Group Policy in their enterprise.

Realizing this, Microsoft is now incorporating a reduced-functionality version of FAZAM 2000 on the Windows 2000 Resource Kit, and has plans to incorporate the full version in future releases of Windows.

## **References**

'Gpresult.exe: Group Policy Results' Microsoft website  
<http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/gpresult-o.asp>

'Gpotool.exe: Group Policy Verification Tool' Microsoft website  
<http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/gpotool-o.asp>

‘Understanding Microsoft Security Configuration Tool Set’ Microsoft website  
<http://www.microsoft.com/ntserver/techresources/security/SecurConfigToolSet.asp>

‘FAZAM 2000, Reduced-Functionality Version’ Microsoft website  
<http://www.microsoft.com/WINDOWS2000/techinfo/reskit/tools/existing/fazam2000-o.asp>

‘Group Policy and Security’ Windows 2000 Magazine website  
<http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9169>

‘Eliminating Management Challenges’ Full Armor website  
[http://www.fullarmor.com/pdf/EliminatingGPMgmtChallenges\\_v11\\_010119.pdf](http://www.fullarmor.com/pdf/EliminatingGPMgmtChallenges_v11_010119.pdf)

‘Designing Group Policy’ Full Armor website  
<http://www.fullarmor.com/pdf/DesigningGroupPolicyWP.pdf>

‘Managing Group Policy’ Full Armor website  
[http://www.fullarmor.com/pdf/Man\\_Enterprise\\_Pol\\_FAZAM2000.pdf](http://www.fullarmor.com/pdf/Man_Enterprise_Pol_FAZAM2000.pdf)

Jennings, Roger “Admin 911 Windows 2000 Group Policy” Berkely, CA. McGraw-Hill, 2001

© SANS Institute 2000 - 2002, Author retains full rights.



# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event