Report Number: C4-007R-01

Guide to Securing Microsoft Windows 2000® Group Policy

Network Security Evaluations and Tools Division
of the
Systems and Network Attack Center (SNAC)

Author:
Julie M. Haney

Updated: January 2001
Version 1.0

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

410-854-6015
securew2k@dewnet.ncsc.mil

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of January 2001. See Microsoft's web page http://www.microsoft.com/ for the latest changes or modifications to the Windows 2000 operating system.

This Page Intentionally Left Blank

Acknowledgements

The author would like to acknowledge the authors of the "*Guide to Implementing Windows NT in Secure Network Environments"* and the *"Guide to Securing Microsoft Windows NT Networks"* versions 2.0, 2.1, 3.0, 4.0, and 4.1.

The author would also like to acknowledge Mark Sanderson and David Rice whose notes and comments on Group Policy were incorporated into this document.

Some parts of this document were drawn from Microsoft copyright materials with their permission.

Trademark Information

Table of Contents

Table of Figures

Introduction

The purpose of this guide is to inform the reader about the available security settings available through Group Policy as well as recommended practices for ensuring the security of Group Policy. Because Group Policy implementations will vary, this document is designed to provide system administrators and network managers the ability to choose appropriate security settings for their environment.

This document is intended for Windows 2000 network administrators, but should be read by anyone involved or interested in Windows 2000 or network security. **The *Guide to Securing Microsoft Windows 2000 Group Policy* is intended to address the security-related issues of Group Policy and is not a step-by-step instruction on configuring Group Policy**. For more information on implementing Group Policy, there are numerous resources available including the Microsoft white papers "Introduction to Windows 2000 Group Policy" and "Step-by-Step Guide to Understanding the Group Policy Feature Set."

Getting the Most from this Guide

The following list contains suggestions to successfully secure Windows 2000 Group Policy according to this guide:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations:
  - Perform a complete backup of your system before implementing any of the recommendations in this guide.
  - Ensure that the latest Windows 2000 service pack and hotfixes have been installed. For further information on critical Windows 2000 updates, see the Windows Update for Windows 2000 web page http://www.microsoft.com/windows2000/downloads/default.asp.
- Follow the security settings that are appropriate for your environment.

About the Guide to Securing Microsoft Windows 2000 Group Policy

This document consists of the following chapters:

Chapter 1, "Group Policy Overview," describes some of the available Group Policy settings and Group Policy links.

Chapter 2, "Group Policy Processing," addresses how Group Policy is processed, including conflicts, inheritance modifications, synchronous processing, and refresh rates.

Chapter 3, "Group Policy Delegation," discusses how management of Group Policy can be delegated to non-administrative users.

Chapter 4, "Group Policy Security Settings," describes how the use of Security Settings can enhance a network.

Chapter 5, "Design and Other Group Policy Issues, " addresses Group Policy design considerations, Local Group Policy Objects, Loopback processing, and support for legacy clients.

Appendix A, "References," contains a list of resources cited.

Chapter

1

Group Policy Overview

Group Policy is an Active Directory-based mechanism for controlling user and computer desktop environments in Windows 2000 domains. Settings for such items as security, software installation, and scripts can be specified through Group Policy. Group Policy is applied to groups of users and computers based on their location in Active Directory.

Group Policy settings are stored in Group Policy objects (GPOs) on domain controllers. GPOs are linked to containers (sites, domains, and Organizational Units – OUs) within the Active Directory structure. Because Group Policy is so closely integrated with Active Directory, it is important to have a basic understanding of Active Directory structure and security implications prior to implementing Group Policy. See the *Guide to Securing Microsoft Windows 2000 Active Directory* for more information.

Group Policy is an essential tool for securing Windows 2000. It can be used to apply and maintain a consistent security policy across a network from a central location.

This chapter provides a basic overview of Group Policy concepts.

Computer and User Configurations

As mentioned previously, Group Policy provides both computer and user configuration control. **Figure 1** Group Policy Snap-in shows the Group Policy snap-in with associated extensions.

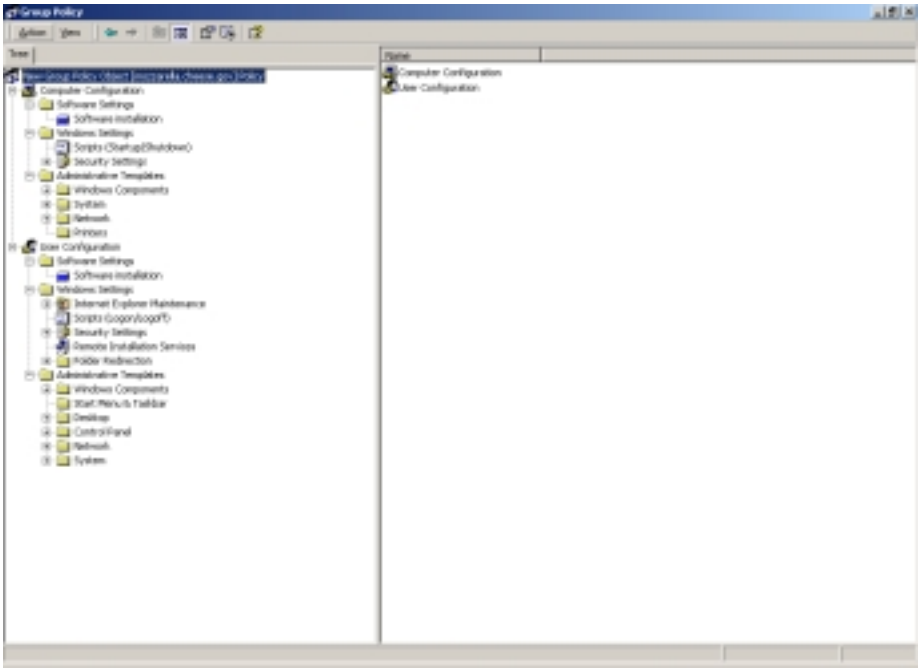

Figure 1 Group Policy Snap-in

Computer Configuration allows control of operating system behavior, desktop behavior, security settings, computer startup and shutdown scripts, computer-assigned application options, and application settings. This configuration is applied when the operating system starts up and during the periodic refresh cycle

User Configuration provides settings for operating system behavior, desktop settings, security settings, assigned and published application options, application settings, folder redirection options, and user logon and logoff scripts. It is applied when users log on to the computer and during the periodic refresh cycle.

Among the configuration categories for Group Policy are:

- **Administrative Templates** – includes all registry-based Group Policy information
- **Security Settings** – includes security-related settings for computers. Because of the importance of this topic, an entire chapter is dedicated to it later in this document
- **Software Installation** – used to assign and publish software to groups of users

  NOTE: It is recommended to use a hidden folder for a software distribution point in order to prevent users from browsing the contents of the share point
- **Scripts** – includes startup/shutdown and logon/logoff scripts
- **Folder Redirection** – redirects several common folders in a user profile to other locations
- **Internet Explorer Maintenance** – contains IE settings

For more information on these extensions as well as other available settings, please see Microsoft's *Windows 2000 Group Policy* white paper.

Creating a GPO

GPOs can be created and/or edited in one of two ways:

- In the MMC, load the Group Policy snap-in
- In the Active Directory Users and Computers or Active Directory Sites or Services tools, specify a new group policy for a container

The latter is the preferred method as it clearly shows and maintains the GPO scope.

Group Policy Object Links

Linking a GPO to a site, domain, or OU causes the settings in the GPO to affect computer or user objects in that container. GPO linking to Active Directory container objects is flexible. A single GPO can be linked to multiple sites, domains and OUs. Also, multiple GPOs can be linked to a single site, domain or OU.

When a GPO is created, it is automatically linked to the container in which it is created. None of the 400-plus settings is initially defined. GPOs linked to domains and OUs are created using Active Directory Computers and Users. GPOs linked to sites are created using Active Directory Sites and Services.

When deciding to unlink a GPO from a container, it is recommended that only the link, and not the entire GPO, be deleted. This allows the GPO to be relinked later in case there is a problem.

It is possible to create an unlinked GPO for a given domain using the Group Policy MMC snap-in and link it to an Active Directory container object at some future time.

Linking a GPO to a Site

Linking a GPO to a site is a way to assign a Group Policy to more than one domain. Any given site may contain computers from one or more domains. If a site contains users and computers from more than one domain, the site GPO settings will apply to all users and computers in that site, regardless of the domain in which the user or computer resides. However, linking GPOs to sites introduces a number of considerations, such as:

- **Site GPO permissions** - With a GPO linked to a site, anyone with read and write permissions to that GPO could make changes to the GPO. Because the GPO is linked to a site, its policies would propagate to the entire site, possible affecting computers in multiple domains.
- **Network traffic patterns** - By default, the GPO for a site is created in the root domain of the forest. GPO implementation uses some amount of network bandwidth. Placing a GPO in the domain root could have a negative effect on inter-domain traffic and perhaps GPO refresh.
- **User rights troubleshooting** - Because of the flexibility in Active Directory to layer GPOs combined with GPO inheritance, troubleshooting user rights problems can become a difficult issue. Also, since Active Directory object permissions are not inherited among domains, receiving a domain or OU GPO from a site may be an unusual concept for some administrators.

To reduce unnecessary complexity and avoid misconfiguration, it is recommended that GPOs generally not be linked to sites.

Linking a GPO to a Domain or Organizational Unit

A GPO linked to a domain applies to all users and computers in the domain. By inheritance, it is also applied to all users and computers in child OUs.

Within a domain tree, Group Policy is **not** inherited between domains. For example, a GPO in a parent domain will not apply to its child domains.

A GPO linked to an OU is applied to all users and computers in the OU. By inheritance, the GPO is also applied to all child OUs under the parent OU.

Link Permissions

By default, only *Domain Admins* and *Enterprise Admins* have the authority to link GPOs to domains and OUs, and only Enterprise Admins have the authority to link GPOs to sites. Members of the *Group Policy Creator Owners* group can create and modify GPOs for the domain, but cannot link them. Refer to the **Group Policy Delegation** chapter for information on how to modify which users and/or groups can link GPOs.

Recommendations Summary

- Use a hidden folder for a software distribution point to prevent users from browsing the contents of the share point.
- In general, GPOs should not be linked to sites.
- When removing a GPO link, remove only the link, and not the entire GPO.

Chapter 2

Group Policy Processing

GPOs are cumulative; the last GPO applied overrides previously applied GPOs. When multiple GPOs exist within a container's hierarchy, the following is the order in which they are processed and applied:

- Local GPO (discussed in the **Design and Other Group Policy Issues** chapter of this document)
- Site GPO
- Domain GPO
- Organizational Unit GPO
- Child OU GPO

This chapter discusses how modifications can be made to the hierarchical processing order, as well as refresh frequencies of Group Policy.

GPO Conflicts

Group Policies are cumulative, so long as they do not conflict. In other words, if a given container object links to multiple GPOs, the non-conflicting settings from all of the GPOs will affect that container.

There is one exception to the accumulation rule as follows:

When processing IP Security or User Rights settings, the last GPO processed overwrites any previous GPOs.

When GPOs conflict, the last setting to be processed generally applies. The two clear-cut cases for this rule are parent-child settings and settings from multiple GPOs linked to the same container. When settings from different GPOs in the Active Directory parent-child hierarchy conflict, the child container GPO settings apply. When settings from multiple GPOs linked to the same container conflict, the settings for the GPO highest in the list apply. Administrators can rearrange this list to raise or lower the priority of any of the GPOs in the list.

Inheritance Modifications

Strict hierarchical GPO application can be modified using either inheritance blocking options or security group filtering.

Block Inheritance and No Override

There are two ways to alter the GPO inheritance model: Block Inheritance and No Override. When blocking inheritance, application of all GPOs from parent containers is blocked. Blocking inheritance cannot be used to selectively block specific GPOs.

No override can be used to enforce GPO settings for child containers regardless of whether block inheritance is set. No override also overrides GPO conflicts. The no override is set on the GPO link and not on the actual GPO. If a GPO is linked to multiple containers, the no override option can be configured individually for each container link.

To access the Block Inheritance and No Override options:

- Right-click on the container
- Select **Properties** from the pull-down menu
- Click the **Group Policy** tab
- The **Block Policy Inheritance** checkbox appears at the bottom of the window as shown in **Figure 2** Block Policy Inheritance.
- To access the No Override option, click the **Options** button. **Figure 3** No Override Option shows the available options.

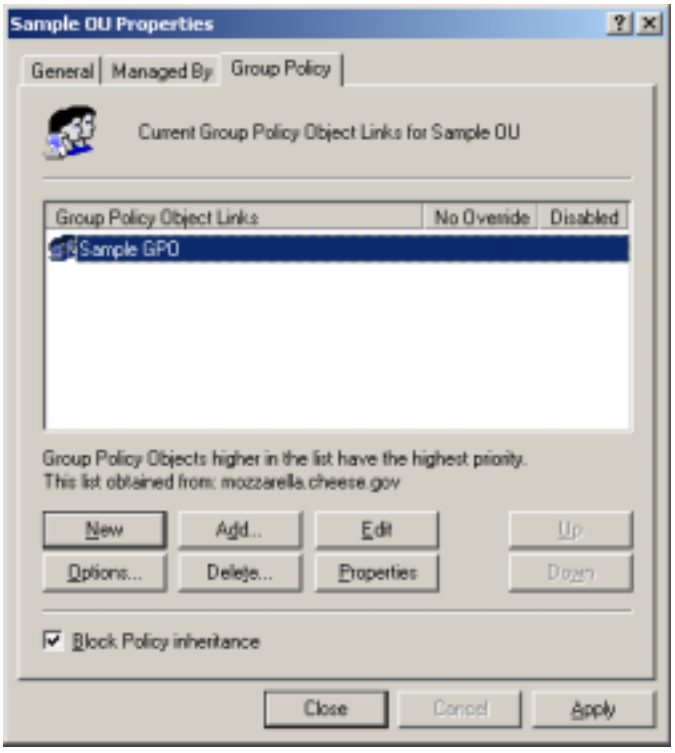

Figure 2 Block Policy Inheritance

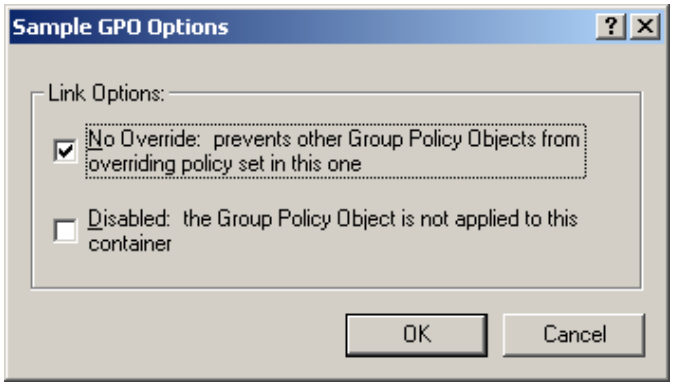

Figure 3 No Override Option

Use of the No Override and Block Inheritance options can make troubleshooting difficult. Therefore, it is recommended that use of the No Override and Block Inheritance options be minimized.

Discretionary Access Control and Filtering

Like the Windows 2000 file system, GPOs have associated Discretionary Access Control Lists (DACLs) that govern the type of access users, groups, and even computers have to the object. The DACL can be accessed via the **Security** tab of a GPO. The available access types for GPOs are:

- Full Control
- Read
- Write
- Create All Child Objects
- Delete All Child Objects
- Apply Group Policy

NOTE: Clicking the Advanced button in a GPO's Security tab allows for setting more granular permissions and auditing options for the GPO.

Group policies require both the Read and the Apply Group Policy DACL permissions to be effective. Therefore, Group Policy settings can be filtered by explicitly denying the Apply Group Policy permission to a user or group or by omitting an explicit Apply Group Policy permission.

On a newly created GPO, by default, the Authenticated Users group has Read and Apply Group Policy permissions. Enterprise Admins, Domain Admins, and SYSTEM have Read, Write, Create All Child Objects, and Delete All Child Objects permissions.

Tracing inherited rights back to their source and troubleshooting can be difficult. Filtering adds another level of complexity. Therefore, the filtering of permissions on GPOs is generally not recommended.

Excluding Administrators from GPO Application

As stated above, by default, the Authenticated Users group is given Read and Apply Group Policy permissions. All administrators in that container are included in the Authenticated Users group. Sometimes administrators within a container should not be subject to a GPO. For example, a GPO that restricts the desktop of normal users may not be convenient or feasible for administrators. To access the DACL of a GPO:

- Open a GPO in the Group Policy snap-in or by accessing a GPO through a container's **Properties → Group Policy** tab
- Right click the GPO and select **Properties** from the pull down menu
- Click the **Security** tab

To exclude administrators from a GPO, there are two options:

- Remove the Authenticated Users group from the GPO DACL and replace it with a group containing only those users needing Read and Apply Group Policy permissions.

or

- Set the Apply Group Policy permission to Deny for Domain Admins, Enterprise Admins, and Creator Owner (if the GPO should not be applied to the user who created it). Deny permissions take precedence over Allow permissions.

If a GPO is not applied to administrators in a container, it is recommended that a GPO be created specifically for administrators, or that administrators be placed in a separate OU with their own Group Policy.

Synchronous vs. Asynchronous Processing

The processing of Group Policy can be either synchronous or asynchronous. Synchronous processing processes each thread of the computer startup and user logon in order, waiting for each process to complete before running the next. Asynchronous processing allows startup and logon threads to run in an arbitrary order. By default, the processing of Group Policy is synchronous. An administrator can change the processing to be asynchronous by using a Group Policy setting for both computers and users.

To view or configure Group Policy processing settings:

- Open a Group Policy snap-in from the MMC
- Navigate to the **Computer Configuration/Administrative Templates/System/Logon and Group Policy settings** and to the **User Configuration/Administrative Templates/System/Logon/Logoff** settings

A number of settings can be viewed such as:

- Run logon scripts synchronously
- Run startup scripts asynchronously
- Apply Group Policy for computers asynchronously during startup
- Apply Group Policy for users asynchronously during logon

If these policies are not configured or are set to run synchronously, each of the related processes will run in order, one by one.

Because asynchronous processing could lead to unpredictable and possibly dangerous results, synchronous processing of Group Policy is recommended.

Refresh Frequency

Within Active Directory, computers refresh GPO settings at established intervals. The default Group Policy refresh intervals are:

- 90 minutes for computers running Windows 2000 Professional and for member servers running Windows 2000 Server
- 5 minutes for domain controllers

Changing the Refresh Rate

An administrator can change the default refresh values by modifying the template settings for the user or computer configuration. GPO refresh cannot be scheduled to occur at a specific time.

It is recommended that the default refresh rates not be significantly decreased or increased.

Forcing a Refresh from a Client

By default, clients only process GPO settings that have changed since the last refresh. This feature is designed to improve performance. This means that certain settings could remain un-refreshed for an extended period. For example, if a user changes a desktop setting during a session and that desktop setting is not changed in the GPO, the user's change will not be reversed when Group Policy is refreshed.

Group Policy refreshes cannot be activated on demand from a domain controller to clients. However, a client may initiate a forced refresh by executing the following commands for the computer and user configurations respectively:

- secedit /refreshpolicy MACHINE_POLICY [/enforce]
- secedit /refreshpolicy USER_POLICY [/enforce]

NOTE: The /enforce option causes settings for the Security and Encrypted File System (EFS) extensions to refresh regardless if they have changed.

Recommendations Summary

- Group Policy template settings should be configured to process unchanged Group Policy settings.
- Be sure that a GPO has fully replicated before making further changes to it.
- Use of the No Override and Block Inheritance options should be minimized.

- Filtering of permissions on GPOs is generally not recommended.
- Even if administrators are exempt from a GPO affecting normal users, they should be subject to some specialized GPO that governs security settings.
- Synchronous processing of Group Policy is recommended over asynchronous processing.
- The default Group Policy refresh rates should not be significantly decreased or increased.

Chapter 3

Group Policy Delegation

With Active Directory comes the ability for administrators to delegate control of administrative tasks to other users and groups. Active Directory allows administrators to manage and delegate control over Group Policy in the following ways:

- Manage Group Policy links for a container object
- Create GPOs
- Edit GPOs
- Restrict access to certain snap-ins (Group Policy related and other)

This chapter discusses the issues involved in delegating specific functions of Group Policy and how to maintain tighter security of Group Policy administrative tasks.

Managing GPO Links

Each container (site, domain, OU) stores information on the GPOs that are linked to it (the gPLink property) as well as any inheritance-blocking options that are set on it (the gPOptions property). A user or group must have Read and Write permissions on both the gPLink and gPOptions properties in order to manage a container's link. As stated earlier, by default, only *Domain Admins* and *Enterprise Admins* have the authority to link GPOs to domains and OUs, and only Enterprise Admins have the authority to link GPOs to sites.

The ability to link a GPO to a site, domain, or OU can be delegated to other users or groups. When delegating a task, it is highly recommended that administrators delegate to security groups versus individual users. The use of security groups allows an easy way to add and delete members at any given time and provides greater administrative control.

Also, caution should be taken when delegating Group Policy management to non-administrative users and/or groups. Only grant this ability if absolutely necessary.

To grant a group the ability to manage a domain or OU's Group Policy links, perform the following actions:

- **Start → Programs → Administrative Tools → Active Directory Users and Computers**
- Right click on the container that you wish to delegate
- Select **Delegate Control** from the pull-down menu
- Click **Next**
- Click the **Add** button to add users and/or groups

- Select the group(s) that will be given the ability to manage links, clicking **Add** for each one
- Click **OK**
- Click **Next**
- Ensure that the **Delegate the following common tasks** radio button is selected
- Click the **Manage Group Policy Links** check box. **Figure 4** Delegation of Control Wizard shows this option selected
- Click **Next**
- Click **Finish**

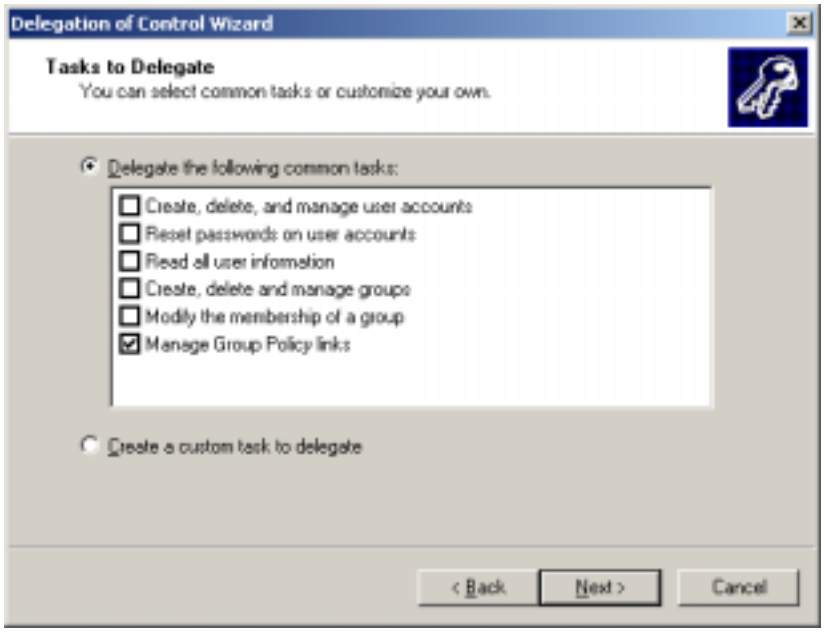

Figure 4 Delegation of Control Wizard

Modifying DACLs to Delegate

The assignment of access control entries to specific security groups is an effective way of controlling and delegating management of GPOs.

Creating GPOs

By default, Domain Admins, Enterprise Admins, SYSTEM, and the Group Policy Creator Owners groups can create a new GPO. In order for other users or groups to be able to create GPOs, they must be added to the Group Policy Creator Owners group. Users and/or groups can be added to the Group Policy Creator Owners group through the Active Directory Users and Computers snap-in.

Once a member of the Group Policy Creator Owners group creates a new GPO, that user becomes the Creator Owner with full control of the GPO. The user can then edit the GPO. Being a member of the Group Policy Creator Owners group only gives Creator Owner status over those GPOs specifically created by the user; the membership does not automatically grant control over other GPOs.

NOTE: When an administrator creates a GPO, the Domain Admins group becomes the Creator Owner of the GPO.

If granting a user or group the ability to create GPOs in a container, the user or group should probably also be given the ability to manage GPO links for that container.

Editing GPOs

In order to edit an already-existing GPO, a user and/or group needs both Read and Write access to the GPO. Domain Admins, Enterprise Admins, SYSTEM, and Creator Owner can by default edit the GPO. Other users and/or groups can be granted edit access to a GPO by performing the following steps:

- Open a GPO in the Group Policy snap-in or by accessing a GPO through a container's **Properties → Group Policy** tab
- Right click the GPO and select **Properties** from the pull down menu
- Click the **Security** tab
- Click **Add** to add a user and/or group to the ACL. Grant the user or group both Read and Write permissions in the **Allow** column for the GPO
- Click **OK**

Restricting the Use of Sensitive Snap-ins

The security of Group Policy settings can be further enhanced by controlling who has access to MMC snap-ins. Administrators may specify which snap-ins users affected by the GPO may or may not be allowed access.

To permit or allow access to certain snap-ins, the following group policy setting must first be set:

- Open a GPO in the Group Policy snap-in via the MMC or access a linked GPO through a container's **Properties → Group Policy** tab.
- If accessing through the **Group Policy** tab, highlight the desired GPO and click the **Edit** button to access the Group Policy snap-in
- Navigate down to the **User Configuration\Administrative Templates\Windows Components\Microsoft Management Console** node
- Double-click on the **Restrict users to the explicitly permitted list of snap-ins** setting in the right pane
- Click the **Enabled** radio button if you plan to disallow most snap-ins and allow only a few. Click the **Disabled** radio button if you plan to allow most snap-ins and disallow only a few

To restrict or allow access to a specific snap-in, perform the following steps within the Group Policy snap-in:

- Navigate down to the **User Configuration\Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins** node
- Double click on the desired snap-in in the right pane

- Click the **Enabled** radio button if explicitly allowing access to the snap-in or click the **Disabled** button if explicitly denying access
- If desiring to restrict access to a Group Policy extension, double-click the **Group Policy** node and select a snap-in from the list and either enable or disable it

Deciding which snap-ins to allow for a given group of users is often environment and network specific. For example, normal users are restricted from accessing several snap-ins by default, but may need greater restriction. In the case of non-administrative users, it may be easier to define which snap-ins they CAN access and implicitly deny access to all other snap-ins. Groups of administrative users that were delegated Active Directory abilities can also be limited to certain tasks.

At a minimum, it is recommended that normal, non-administrative users not be allowed access to the **Security Templates** and **Security Configuration and Analysis** snap-ins. Access to these templates could allow a user to view all of the intended security settings of a system and perform an analysis to determine if the system is vulnerable to attack.

Recommendations Summary

- Use caution when delegating Group Policy to groups other than administrators.
- Assign Group Policy permissions to security groups and not individual users.
- Full Control is not necessary to manage links or modify GPOs; assign the fewest permissions needed.
- Limit the use of sensitive snap-ins, such as the Group Policy, Security Templates, and Security Configuration and Analysis snap-ins.
- In the case of non-administrative users, define GPOs that deny access to all snap-ins except those deemed necessary and explicitly listed as permitted.

Chapter 4

Group Policy Security Settings

From a security perspective, one of the most important parts of Group Policy is the Security Settings extension. Security Settings allow administrators to consolidate many security-related items and apply them to any number of Windows 2000 computers via Group Policy and the Active Directory.

This chapter presents an overview of Security Settings and provides recommendations on how to effectively use this extension.

Overview

The Security Settings extension of Group Policy is located under **Computer Configuration\Windows Settings\Security Settings** within a GPO and can be accessed via the Group Policy snap-in. Security Settings are computer, not user, specific. Expanding the Security Settings node reveals the following security areas:

- **Account Policies** – includes Password Policy and Account Lockout Policy. Account Policies are set in the Default Domain Policy GPO for the domain container and affect all domain users. If different account policies are required for different sets of users, a multiple-domain architecture may be in order. Account policies set at the OU level will be applied if a user is logging onto the local computer, not the domain. Setting account policies at the OU level is still recommended in case a local logon occurs.
- **Local Policies** – includes Audit policy, User rights assignment, and Security Options (registry-specific security settings)
- **Event log** – includes settings for event logs
- **Restricted Groups** – includes membership restriction for sensitive groups
- **System Services** – includes startup options for services
- **Registry** – DACLs for specified registry keys
- **File System** – DACLs for specified files and folders
- **Public Key Policies** – includes Encrypted Data Recovery Agents, Automatic Certificate Request Settings, Trusted Root Certification Authorities, and Enterprise Trust
- **IP Security Policies on Active Directory** – includes settings for IPSec

All but the last two items listed above can be initially configured via the Security Templates snap-in. The Security Templates snap-in allows the settings to be saved in a template, or INF file, and then be imported into a GPO via the Group Policy

snap-in. For more guidance on how to configure security templates, refer to the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset*, which provides a detailed description on how to create security template files and gives security recommendations for each of the settings.

Public Key Policies and IP Security Policies can only be applied via Group Policy and will be addressed in the PKI and IPSec mini-guides, respectively.

Account Policies are set in the Default Domain Policy GPO and affect all domain users. If different account policies are required for different sets of users, a multiple-domain architecture may be in order. Account policies set at the OU level will be applied if a user is logging onto the local computer, not the domain. Setting account policies at the OU level is still recommended in case a local logon occurs.

Importing a Security Template into a GPO

To import an already-existing security template into a GPO, perform the following steps:

- In the Group Policy snap-in, navigate to the **Computer Configuration\Windows Settings\Security Settings** node
- Right-click **Security Settings**
- Select **Import Policy** from the pull-down menu
- The **Import Policy From** window will initially display all inf files in the %SystemRoot%\security\templates folder. Select a template from this folder or browse to find the appropriate template
- Click **Open**
- The settings in the selected template file will now be imported into the Security Settings node. You may view these settings by navigating down through the Security Settings tree

Design Considerations for Security Settings

The Security Configuration Toolset mini-guide provides templates for Windows 2000 servers and workstations. Each template is unique since the security needs for servers and workstations can be different.

It is recommended that computers within a Windows 2000 domain be grouped into separate OUs based on their role in the domain. For example, workstations will be in their own OU, member servers in another OU, and domain controllers in the Default Domain Controllers OU. Within this type of organization, GPOs containing security settings individualized for each type of computer can be easily applied.

Recommendations Summary

- Import the security templates from the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset* into GPOs.
- Account policies applied at the domain level will affect all users in a domain. If separate account policies are required, consider a multiple-domain architecture.

- Apply the same account policies at the OU level as at the domain level so that users logging on locally to computers will still maintain a strong account policy.
- Computers fulfilling different roles should be grouped into separate OUs. This allows for application of computer-specific security settings based on computer type.

This Page Intentionally Left Blank

Chapter 5

Design and Other Group Policy Issues

This chapter discusses some design issues related to Group Policy as well as additional policy security-related items.

Design Considerations

The default Users, Computers, and Builtin containers in Active Directory are not OUs. Therefore, GPOs cannot be linked to them. For this reason, user and computer objects should be moved into separate OUs in a target OU structure so that GPOs can be applied.

A Default Domain Policy GPO is automatically applied to each domain. This GPO contains very few security settings. However, it does include some Public Key and IPSec policies and important Account Policies settings that affect the entire domain. All domain-wide Account Policies settings and other settings should be included in a GPO at the domain level.

It is also recommended to limit the number of GPOs applied to users and computers. Too many GPOs can result in an administrative nightmare, making it difficult to track effective policy settings and troubleshoot policy problems.

Domain Controller Group Policy

The Domain Controllers container is also created by default. All domain controllers are placed in this container as they are added. A GPO called Default Domain Controllers Policy is linked to the container. It is recommended that a domain controller specific security template be imported into the new GPO.

Domain controllers share a common domain account database. Therefore, some security settings must be the same for all domain controllers. Group Policy accomplishes this by applying certain security settings in the domain Group Policy on all domain controllers, regardless of whether they are located in the Default Domain Controllers OU or have been moved to another OU. The following settings from the domain Group Policy are applied to domain controllers:

- All settings in **Computer Configuration\Windows Settings\Security Settings\Account Policies**
- The following settings in **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**:
  - **Automatically log off users when logon time expires**

- **Rename administrator account**
- **Rename guest account**

For more information on this topic, see Knowledge Base article Q259576, Group Policy Application Rules for Domain Controllers http://support.microsoft.com/support/kb/articles/Q259/5/76.asp.

Group Policy Management

By default, when a new GPO is created, the domain controller that holds the PDC emulator role performs the management operation. Although other domain controllers can be specified to process GPOs, Microsoft recommends maintaining the PDC emulator for this task in order to prevent data loss.

Local Group Policy Object

Every computer has a Local Group Policy, regardless of whether it is part of a domain. Recall that Local Group Policy is the first policy applied. Although any subsequent policies may override settings in the local policy, any settings specified in Local Group Policy, but not specified in other policies, will remain. Therefore, it is important to configure a solid local policy in addition to Active Directory Group Policy.

The Local Group Policy Object (LGPO) is saved in %SystemRoot%\System32\Group Policy. It can be accessed and viewed by choosing the Local Computer object in the Group Policy snap-in or by selected the Local Security Policy option under the Administrative Tools menu.

The LGPO does not have the full number of settings available with Active Directory Group Policy. For example, under the Security Settings node, only Account Policies and Local Policies are available.

Loopback

Loopback GPO processing allows policy to be applied to users based upon which computer they are logged on, i.e. all users logging onto a specific computer will receive the same policy settings. This feature is designed to prevent applications that are normally assigned to a user from automatically being available on a special-purpose machine. The two modes for loopback processing are:

- **Replace mode** - processes only the GPOs that apply to the computer.
- **Merge mode** - first processes the GPOs that apply to the user object, and then the GPOs that apply to the computer object. If settings conflict, the computer object settings override the user settings.

In general, loopback should be used only when absolutely necessary.

Support for Windows NT and 9x Clients

For all intents and purposes, Group Policy replaces the System Policy that was available in Windows NT. However, Group Policy it is not backward compatible with System Policy and does not support legacy clients. If upgrading from Windows NT

clients to Windows 2000 clients, system policies must be manually duplicated or approximated in Group Policy.

It is recommended that legacy clients not be used in Windows 2000 networks. However, if maintenance of these clients is necessary, it is important to understand that **Windows NT and 9x clients residing in a Windows 2000 domain cannot use Group Policy**. However, a system policy can be pushed out to these clients from Windows 2000 domain controllers. Refer to the *Guide to Securing Microsoft Windows NT/9x Clients in a Windows 2000 Network* for more information on migrating system policy for Windows NT and Windows 9x clients on Windows 2000 networks.

Monitoring and Troubleshooting Group Policy

Group Policy event logging can be enabled via several registry settings. The two types of event logging are diagnostic and verbose. Diagnostic logging writes detailed Group Policy events into the Event Log. Verbose logging tracks Group Policy changes and settings applied to the local computer and to users who log onto the computer. The verbose log file is %SystemRoot%\Debug\UserMode\Userenv.log.

Enabling Diagnostic Logging

To enable diagnostic logging, add the following registry key and value:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\WindowsNT\CurrentVersion\Diagnostics
Name: RunDiagnosticLoggingGlobal
Type: REG_DWORD
Value: 1

Using this function will write Group Policy events to the Application log. Because the number of events will probably be large, the size of the Application log may need to be increased. This function should be used temporarily for troubleshooting and disabled when not needed.

Enabling Verbose Logging

To enable verbose logging of local computer and user GPO changes and settings, add the following registry key value:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name: UserEnvDebugLevel
Type: REG_DWORD
Value: 30000 (decimal) – logs nothing
30001 (decimal) – enables logging of errors
30002 (decimal) – enables verbose logging

Troubleshooting Tools

The following Windows 2000 Resource Kit command-line tools can be used to troubleshoot Group Policy:

- **Gpotool.exe** - checks the health of Group Policy objects on the domain controller
- **Gpresult.exe** - displays information about the cumulative effect of Group Policy on the current computer and logged-on user

For more information on the use of these tools, see the Resource Kit documentation.

Recommendations Summary

- ❑ Remove users and computers from the built-in Users and Computers containers and place in OUs.
- ❑ Set Account Policies and other domain-wide settings in a GPO linked to the domain container.
- ❑ Minimize the number of GPOs associated with user or computers.
- ❑ Group related settings in a single GPO.
- ❑ Maintain the PDC emulator domain controller as the Group Policy manager.
- ❑ Set a strong Local Group Policy for computers that are not part of a domain. For domain computers, a good LGPO can compensate for holes in subsequently applied Active Directory GPOs.
- ❑ Use loopback processing only when necessary. Place all computers affected by loopback in the same OU.
- ❑ Do not use legacy clients in a Windows 2000 network. However, if these clients are necessary, investigate how to apply a System Policy to them.
- ❑ Enable Group Policy diagnostic logging temporarily when troubleshooting is required.

Appendix

A

References

Bartock, Paul, et. al., "Guide to Securing Microsoft Windows NT Networks," Version 4.1, National Security Agency, September 6, 2000.

"Designing a Secure Microsoft Windows 2000 Network," Microsoft Official Curriculum course 2150ACP, 2000.

Haney, Julie, "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set," Version 1.0, National Security Agency, May 2001.

"Introduction to Windows 2000 Group Policy," http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicyintro.asp, Microsoft white paper, 1999.

McLean, Ian, *Windows 2000 Security Little Black Book*, Coriolis Group: Scottsdale, Arizona, 2000.

Microsoft Web Site, http://www.microsoft.com/.

"Step-by-Step Guide to Understanding the Group Policy Feature Set," http://www.microsoft.com/windows2000/techinfo/planning/management/groupsteps.asp, Microsoft, January 2000.

"Windows 2000 Group Policy," http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp, Microsoft white paper, 2000.