

# Hardening Windows 2000 in the Enterprise Part Three: Seeing the Forest in Spite of the Trees

*Timothy M. Mullen* 1980-01-01

## Hardening Windows 2000 in the Enterprise: Seeing the Forest in Spite of the Trees Part Three

by *Timothy M. Mullen*

last updated July 18,2001

---

Well, we are finally here. Over the first two installments of this series, we've been building up to this part, and I must say, I'm excited. Though we've covered quite a bit in the way of security settings on Win2k, we have really only scratched the surface of a deeply powerful policy management system. The Local Security Policy can take us part of the way, but it can't deliver us safely to where we really want to go: a place called "security". Of course, security is a relative term: it doesn't really mean anything by itself - we have to compare it to something. For these discussions, it will be a "before and after" comparison of our systems of when they come out of the box and how they are after an effective Group Policy is applied.

### Group Policy

What exactly is Group Policy? Well, let's take all the Computer Configuration settings that can be set in the Local Security Policy of a box, add the additional Computer Configuration settings that can be added in domains, sites, and Organizational Units, throw in the Security Policy, and then load User Configuration Policy options. Then we'll throw in mechanisms to apply file system ACL's, control the behavior and security context of system services, and finally create a method of automatically controlling group membership. What we end up with is Group Policy.

It sounds simple when put like that, but it can take a lot to design an effective Group Policy. Once you do the legwork and get your security layout completed, deploying it can be a breeze. By the same token, you should be aware that it is also just as easy to jeopardize the entire domain by rolling out a setting that you are not familiar with. This action is typically preceded by a little voice in your head saying, "I wonder what this setting does?" Beware of that little voice! Make sure you research and test your configurations before hitting 'apply' at the domain level. I learned this the hard way when I first decided to mandate NTLMv2 at the domain level a few years back.

In the last installment of this series, we left off at the Computer Settings that one can roll out via Local and Domain Security policies. These dealt primarily with settings that affected the box itself, such as how secure channels will be set up and how to handle anonymous sessions. Domains, sites and OU's can have additional settings imposed, and are quite cool. After we look at those, we will examine the other part of the equation in our networks: the user.

## Computer and User Configuration

The settings available via the full-blown computer configuration (as opposed to only those available at the local level) and user configuration are extensive. Though the sheer volume of settings to consider complicates the design process, it is a good thing in the end. The more options we have when customizing the computing environment of our users, the better we can control possible security issues. Remember, your servers are not the only place that lock-downs need to be in place: it was not that long ago that the ILOVEYOU virus flooded e-mail servers and wiped out .jpg documents all over the network simply because someone could immediately launch the .vbs app from Outlook.

As with the Computer Configuration settings, these too can get "fangy". (Hey Mike, that's twice! One more use of "fangy" and I will win that scrabble game!!!) In fact, some of these options have sub-options that then have multiple configuration settings of their own, such as the Security Zones settings. Since the length of this discussion will keep me from drilling down to each individual setting, in these cases I will give you an overview of what the main hive does. As in the [last article](#), I have included some personal commentary in this overview of the settings, which are inserted between the <.02> </.02> brackets.

---

## The Controls: Computer Configuration

### Windows Settings

**Restricted Groups** Allows you to set which users can be members of which groups, as well as what other groups the group can belong to. <.02>

Use this - it is very powerful! When the policy is applied, accounts in a group that should not be there are automatically removed. The default for DC policy application is 5 minutes, so even if someone hacked into your machine and made themselves an admin, which is far more common

than hacking the admin account itself, then they would be removed automatically! <.02>

**System Services** Allows you to set the way a service starts, as well as the security context that the service lives in. <.02>

Use this! Having a server running unneeded services is a security hole and a drain on system resources. This setting can save your butt. Check out what services your server (based on application type) need to run. If it is a web server, check out the IIS checklist on [TechNet](#), or load the Security Templates Snap-In and check out the templates that ship with the OS as a guideline. This is where breaking our OUs into application-based units can really streamline policy deployment. <.02>

**Registry Permissions** In domains, sites, and OUs, you can set the registry key permission DACLs (Discretionary Access Control Lists) that you want to with this node. <.02>

NT really had some issues with poor default security on important registry keys. Though the defaults on Win2k are stronger in many instances, you will still want to review your options here. <.02>

**File System** Allows you to specify directory structures and the DACLs that you want set on them, as well as audit options. <.02>

Hallelujah! Finally, a way to automatically set DACLs on the file system without having to refer to third party stuff. Use this guy too, particularly on your Web and SQL servers. Lots of issues came out of cracks where the IUSR had permissions on the box. Don't let it happen to you. <.02>

**Account and Local Policies** These are a mirror of the options available in the Local Policy of a box (the ones we covered last time.) Click [here](#) to view those guys.

**Event Log Settings-** (available for domains, sites, and OUs. )

**Maximum Log size** (keys for Application, Security, and System log) Duh. Sets the maximum log size (file size) for the respective log type.

**Restrict Guest access to log** (keys for Application, Security, and System log) Duh. Restricts the guest account from accessing the logs. Enabled by default.

**Retain Log** (keys for Application, Security, and System log) If you archive the logs, and the retention method is set to 'by days', this specifies the number of days that entries should be retained, up to the maximum log size.

**Retention Method** (keys for Application, Security and System log) Allows you to set the way the log retains entries, depending on if you archive or not, and if you need to keep all entries. If you do interval archiving, set this to 'Overwrite By Days' with the appropriate 'Retain Log' setting. If you don't want items to be overwritten as needed, where they fall off the log as necessary, then set this to 'Do Not Overwrite,' which will require you to manually clear the log.

**Shutdown computer when security log is full** Rather than using this setting, which will only shut down the system when the log is full, you should use the 'Shutdown computer immediately if unable to log security audits' policy element, which will cover you in other cases where a log entry cannot be made (not just when it is full). <.02>

For obvious reasons, be careful here. If you set this option, you'd better have a large drive set aside for log entries. The purpose of this entry is to provide a mechanism to bring down the system if an attack is logging a very high number of violations. Setting this option with 'Overwrite As Necessary' really doesn't buy you anything. This should be a last ditch attempt to protect yourself. Your IDS should be set up to alert you of attacks rather than a machine shutdown. <.02>

## Administrative Templates

(Windows Components, System, Network, Printers)

These options still live under the Computer Configuration hive, not User Configuration. Some, such as Net Meeting, are covered under both, which differ in options as appropriate.

### Windows Components

#### NetMeeting

Allows you to set the desktop sharing capabilities of Net Meeting.

#### Internet Explorer

Contains sub-options that allow you to set how security zones and proxy settings are set in regard to per user or per machine, and allows you to set how automatic updates are performed.

### **Task Scheduler**

Contains sub-options that allow you to set interface options in the task scheduler, such as disabling advanced settings or preventing lists of schedules from being displayed, as well as allowing task items to be manually started.

### **Windows Installer**

Contains sub-options that allow you to control aspects of the Windows Installer such as how elevated permissions are used, if users can browse installation packages while in the elevated context or select media sources, and logging options.

## **System**

### **Remove security option from Start menu (Terminal Services only)**

Removes 'Windows Security' from Terminal Server clients, forcing them to do a Ctrl+Alt+Del to get the dialog box.

### **Remove Disconnect item from Start menu (Terminal Services only)**

Prevents users from using the 'disconnect' menu item to disconnect from a Terminal Services Client.

### **Disable Boot / Shutdown / Logon / Logoff status messages**

Keeps users from seeing status messages during startup, shutdown, logon or logoff.

### **Verbose versus normal status messages**

Determines if users get detailed status messages or normal status messages.

### **Disable Autoplay**

Prevents a system from automatically launching AutoPlay features on media and network drives.

### **Don't display welcome screen at logon**

For workstations, this prevents the 'welcome' splash screen from being displayed.

### **Run these programs at user logon**

Determines which programs or files are to be launched when users log on.

### **Disable the run once list**

Keeps any item in the run-once list from being launched.

### **Disable legacy run list**

Causes the run list for NT and earlier to be ignored.

### **Do not automatically encrypt files moved to encrypted folders**

Prevents Windows from automatically encrypting files that are moved into an encrypted folder (on the same volume).

**Download missing COM components** Causes missing COM components that a program may need to be automatically scanned for and downloaded if possible.

**Logon** Contains sub-options that control logon, startup, and shutdown script behavior, and profile settings.

**Quotas** Contains sub-options for Disk Quotas.

**DNS Client** Allows you to specify the primary DNS suffix via policy rather (except for Domain Controllers).

**Group Policy** Contains sub-options that control the mode of the application of user and group

policy, the interval at which group policy is imposed, as well as IPSec and EFS policy application intervals, and slow network parameters.

**File Protection** Contains sub-options that set Windows File Protection options.

## Network

**Offline Files** Contains sub-options that define off-line file storage options such as synchronization options, cache sizes, end-user configuration limitations, and reminder balloon settings.

**Network and Dial-up Connections** Determines whether sets sharing can be established and configured.

**Printers** Contains printer configuration options such as Active Directory publication, browse master publication, and pruning settings.

## User Configurations

### Windows Components

**NetMeeting** Contains sub-options to configure user-oriented settings such as call security, restrictions on sending and receiving files, chat, white-board, and sub-sub-menu for Application Sharing, Audio and Video, and Options

**Internet Explorer** This is an important node. It contains benign settings such as color, history, and fonts styles as well as the more important security settings like locking down proxy settings, ratings settings, and certificate settings. A sub-option, Internet Control Panel, allows you to disable the General, Security, Content, Connections, Programs, and Advanced tabs altogether. Off-line Pages, Browser Menus, Toolbars, Persistence Behavior, and Administrator Approved Controls are other sub-options of the Internet Explorer node that control settings in those areas.

**Windows Explorer** Contains sub-options to handle Explorer specific settings such as the removal of folder options, 'file' menus, 'Map Network Drive', and options to only allow approved shell extensions and network browser settings.

**MMC** Contains sub-options to restrict authoring mode on any plug-in, or to restrict/permit usage of other plug-ins and extension snap-ins.

**Task Scheduler** Allows you to set user-based options for the Task Scheduler, similar to the options you can set on a computer-by-computer basis.

**Windows Installer** Windows Installer options set on a user basis such as privilege and media source.

**Start Menu and Taskbar** This node contains many sub-options that allow the restriction of the start menu and the taskbar. You can remove the run, help, network/dial-up, logoff, documents and other common options normally seen on the task bar. You can also set document history options, shell command search options and the drag-and-drop context menus on the Start Menu.

**Desktop** Similar to the Start Menu and Taskbar node, these Desktop settings allow you to customize what appears on the user's desktop. You can disable changes to the taskbar, the 'My Network Places' icon, the 'My Documents' icon, or all icons for that matter. Sub-options exist for Active Desktop and Active Directory as well.

**Control Panel** These sub-options allow you to specify (per user) which control panel applets are displayed, whether to disable the control panel altogether. Sub-options allow you to customize Add/Remove Program options, display options (like Screen Saver and Appearance), Printer options, and Regional Options.

**Network** Sub-options here allow you to configure off-line file options, and Network and Dial-up lockdown settings. These are similar to the Network options under the Computer Configuration, except that these are per-user settings.

**System** These are very important settings. Here, you can disable registry editing tools, specify that a user can only run particular Windows programs, and set COM component options. Logon/Logoff and Group Policy sub options are also available to set per-user options in those areas.

There. That should keep you busy for a while.

**Deployment** Group Policy can be deployed at a number of different levels. By default, there is a Domain Group Policy object that is imposed on the entire domain. Customizing this may be all you need to lock your systems down. However, you can also deploy Group Policy objects at the site level, or at the organizational unit level. Let's talk about organization units again, as they can be a powerful management tool for your policy deployment.

You have full control over how you want to structure your organizational units. Some people model their OUs after an administrative model. They create a Sales OU, a Management OU, a Human Resources OU, and move users and computers into their respective container. Others go the "physical" route - they create a Hanger OU, an Offices OU, a Fuel Depot OU, etc based on what buildings or sector the users and machines were in. I tend to go for the "hybrid" model, and do a little of both. I have administrative/departmental OU's for the users and their respective boxes, but then have applicational OU's for my servers. This really works well, as from a security standpoint, as you can pretty much treat the workstations in the accounting department the same as the workstations in the sales department. However, your Web Server will be secured much differently than a Domain Controller or Terminal Server will be. This hybrid structure lends itself to this type of policy deployment well. You can have a particular Group Policy with settings specific to the application pushed out to only those computers in that group. Then, when you add another application server to your organization, just move it into that OU and you are good to go.

OUs can also contain other OUs, for an even more granular approach to policy distribution. But it becomes more complex, and harder to administer as you go deeper into nested OU levels. I try to keep things simple and stay within a couple of levels or so whenever possible.

Additionally, you can have multiple Group Policy objects pushed to the same OU if you want to. Be aware though, that when you start breaking policies up into little pieces, you can introduce conflicts in the policy application (for instance, if you set an item one way in one policy, and another in a different policy, but apply them to the same computer.) So, you can see that within the structure of the Group Policy itself, we can have a simple, single object policy that pushes out to all the boxes in the domain, or we can create many different Policy Object nodules, each responsible for a particular part of our overall security goals, and have them applied to multiple OUs within other OUs. Pretty powerful stuff.

As with most tools, there are some considerations that you need to be aware of. Depending on the size and structure of your policies, there could be some performance issues on the LAN, so

you may need to learn how to tune those policies accordingly. You will also need to do a bit of research and check out some more advanced options like blocking policy inheritance and loop-back processing mode. The Win2k Resource Kit has a great reference on Group Policy including an entire Group Policy Reference Table with succinct descriptions and the actual registry locations of the options, so get hold of that if necessary.

---

So there you have it: Group Policy 101. These security configuration options are clearly the most powerful ever offered by any Windows OS, and can be used to secure your systems not only from known threats and vulnerabilities, but ones that we have not even discovered yet; and that is strong. It also promotes a more in-depth and security conscious approach to protecting systems than the knee-jerk reaction of firing Hot Fixes downrange at the seemingly neverending flow of vulnerabilities that advance upon us.

Be secure.

[Privacy Statement](#)

Copyright 2006, SecurityFocus