



realtimepublishers.com™

*The Definitive Guide™ To*

# Windows Desktop Administration

**SCRIPTLOGIC**

*Bob Kelly*

Chapter 5: Desktop Security .....	110
Written Security Policy .....	110
Defining Your Security Policy.....	110
Enforcing Your Security Policy.....	111
Benefits of a Locked Down Environment .....	112
Provide Desktop Damage Control .....	112
Prevent Installation of Personal Software.....	113
Eliminate Unauthorized Installation of Company Software.....	113
Stop Software Theft .....	113
Enforce Proper Usage .....	114
Playing Games “On the Clock” .....	114
Conducting Personal Business.....	114
Conducting Illegal Activities .....	114
Decrease Proliferation of Viruses .....	114
Principal of Least Privilege.....	115
Protect Data.....	115
Drawbacks of a Locked Down Environment.....	115
Application Failures.....	115
Failure to Save Settings .....	116
Failures When Saving Data .....	116
First Launch .....	116
Complex Deployments.....	117
Political Considerations .....	117
Modifying File and Registry Access and User Rights.....	117
Registry Security.....	118
Group Policy .....	118
RegINI.....	120
RegDmp .....	121
SecAdd.....	121
File Security .....	121
Group Policy .....	121
CACLS.....	122
XCACLS.....	122

User Rights.....	123
Group Policy .....	123
NT User Manager .....	123
NTRights.....	124
Changing Security Context.....	125
The Switch User Utility (SU.EXE).....	125
TqcRunas .....	125
Controlling Removable Media and Restricting Device Access.....	126
Disable PnP and Other Devices .....	126
The <i>Load and unload device drivers</i> Right.....	127
SecureNT .....	127
General Security Recommendations.....	128
Rename Local Administrator Account .....	128
Enforce Complex Passwords .....	128
Disable Guest Account .....	129
Replace the Everyone Group with Authenticated Users on File Shares.....	129
Employ Logon Warning Messages.....	130
Hide Last Logged On User Name.....	130
Password Protect the Screensaver.....	130
Enable Auditing .....	131
Use RunAs .....	131
Examining Your Security .....	131
Microsoft Baseline Security Analyzer .....	131
Security Configuration and Analysis .....	133
SecEdit.....	134
Event Log Management.....	135
Configuring Event Logs' Retention.....	135
Archiving Event Logs.....	136
Summary.....	137

## Copyright Statement

© 2003 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimedpublishers.com and the Realtimedpublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at [info@realtimedpublishers.com](mailto:info@realtimedpublishers.com).

## Chapter 5: Desktop Security

In the last chapter, we covered the packaging and deployment of new software and updates. With your baseline established, user environment customized, and applications and updates rolling, we will address the security options available for maintaining the control and configuration of your network. However, it goes without saying that it is best to have your security policy and enforcement methods well established before the first user sits in front of a computer. In this chapter, we will discuss security policy, tools, things to watch out for, and the benefits and drawbacks of implementing a locked down environment.

Security is a topic that has been steadily moving into the spotlight for the past several years. Viruses, hackers, data theft, and piracy are on the minds of most organizations today. Security is also a very broad topic. As such, we will focus on those issues that cause the most concern to you, the desktop administrator. The first of which is the establishment of a security policy.

### Written Security Policy

A written security policy is the documentation used to define the rules for the use of computer systems in your organization. Without established, clearly written, and readily available documentation, ignorance will prevail as the reason for all security violations. A written security policy is often overlooked until the damage has been done. To protect your organization from data loss through misuse or from a lawsuit as the result of license violations or administrative action, it is important that a written security policy be defined and enforced.

Keeping in mind that desktop security is only a part of an organization's overall security policy and that the level of restrictions imposed is often based on a user's job, it is unlikely that you should be drafting this policy yourself. There should be several people from management in various departments involved in the creation and review of your organization's security policy.

### Defining Your Security Policy

We will discuss the benefits and drawbacks that come with written security restrictions later in this chapter. For now, I'll summarize considerations to keep in mind when establishing this documentation.

- Keep it realistic—In some government networks or other environments in which data is very sensitive, extreme security measures are understandably a necessity. However, too strong a security policy can impede users' effectiveness and might add complexity to desktop administration. This management concept is called *convergence*, when multiple management goals, such as productivity and security begin to conflict. You will need to determine what is important to your business, then use that definition as your middle ground. When it comes to security, it is important to find a middle ground from which you can protect your data and systems without putting an unnecessary burden on those forced to abide by these rules.



Are the rules being laid down enforceable? We will discuss many of the tools available to enforce your security policy. However, you must also keep in mind that enforcement and backing by management are vital to a security policy that is of any value. There must be a means of ensuring that the policy is followed and consequences result if they are not.




- Keep it simple—Can those who must read and abide by the security policy understand it? As a technical person, it is easy to assume an unrealistic level of technical knowledge and to use terms that not everyone will understand. Everyone must understand the security policy, and although it is painful to dumb things down to the lowest common denominator, in the case of a document such as this, it is necessary to do so.
- Keep it available—To establish a policy that people do not read defeats the purpose of creating one in the first place. Provide employees with a copy and have them sign a statement that they have read and understand it. Provide an electronic copy of the policy on your network for easy reference—a link from an intranet home page is ideal.

### **Enforcing Your Security Policy**

With your realistic, simple security policy as common knowledge, ensure that all users know how you will be aware of violations and what you will do about them. It is difficult to enforce a rule to which there is no consequence for a failure to comply.

- Employing restrictions—A majority of this chapter will focus on the technologies and tools available to enforce your security policy. If users aren't allowed to introduce media to the network, restrict their ability to do so. If users aren't allowed to install unauthorized software, restrict their ability to do so. And if users are not allowed to save data to their local systems, restrict their ability to do so. See a trend here?
- Monitoring violations—With the right tools and a little persistence, most any restriction imposed can be bypassed. Computer cases can be opened, users might bring in Plug and Play—PnP—storage devices, and users might attempt to guess passwords or access data to which they are not allowed. When you understand the weaknesses in your ability to restrict such behavior, you've reached step two of security policy enforcement—monitoring.
- Imposing penalties—Odds are that you will be the one to point the finger, but not the one to punish offenders. It is, however, important for everyone to understand the consequences of security policy violation. The sensitivity and attention given to security in your organization will dictate the severity of these consequences.

 Get it in writing! Just as if an employee were regularly late for work, if a user has repeatedly violated security policy and a move is made to penalize the user, documented reprimands are imperative. An employee might choose to fight whatever penalty is being imposed, making it difficult to enforce without proper documentation. When a user violates security, the user should be made to sign and date a document clearly stating the violation in order to confirm that the user understands what he or she has done and to establish a trend in the event that repeated violations should arise.

## Benefits of a Locked Down Environment

Each release of Windows provides more and more restrictive default security settings. The reason is partly a result of the increasingly common practice of locking down workstations to the greatest degree possible. One major reason for this practice is because, in business, users need to do their work, get their job done, and that is all. Allowing them to make system-level changes increases the likelihood of configuration problems, which leads to increased Help desk calls and user downtime. If users are permitted to install software that might be damaging or violate licensing agreements, the results could be costly. In recent releases of Windows, you can even restrict specified users from running locally installed software (for more information, see the sidebar “Software Restriction Policies”). Finally, in regards to user data, limiting where users can store data will help you to force data storage to a managed area for which fault tolerance and regular backups are available. In this section, we will discuss some of the key benefits to implementing a locked down desktop environment.

### Software Restriction Policies

Via Group Policy, Software Restriction Policy (SRP) provides the ability to limit which applications can be launched on a system. It is the intention of SRP to confront the problem of regulating unknown or untrusted code. It does so by allowing administrators to identify and specify which applications are allowed to run. The applications can be identified in policy through a hash rule, a certificate rule, a path rule, or an Internet zone rule. The software can run on two levels: unrestricted and disallowed.

Before we go further, let me point out that the use of SRP is restricted to Windows XP and Windows 2003 systems. This capability is very useful, but its minimum OS requirements will keep this feature in the future for many environments. For those of you lucky enough to be in such an environment (the rest of us can use this information as ammunition to push for an upgrade), we will cover this new feature in more detail.

A rule is used to identify one or more software applications and specify whether the application(s) is allowed to run. There are four rules that can be used to identify software:

- Hash rule—A hash rule is a cryptographic fingerprint that uniquely identifies a file regardless of where it is accessed or what it is named.
- Certificate rule—A certificate rule specifies a code-signing, software publisher certificate.
- Path rule—A path rule can specify a folder or fully qualified path to a program. When a path rule specifies a folder, it matches any program contained in that folder and any programs contained in subfolders. Both local and UNC paths are supported.
- Zone rule—A zone rule can identify software from the Internet Explorer (IE) zone from which it is downloaded. This rule applies only to Windows Installer (MSI) packages. It does not apply to software downloaded in IE.

For more information about SRP, read the Microsoft article “Using Software Restriction Policies to Protect Against Unauthorized Software.”

### ***Provide Desktop Damage Control***

In most environments, allowing users full access to their systems is a practice that results in an increased number of Help desk calls, license violations, improper use, and data loss. These results might be accidental or deliberate, but in a locked down environment, users are restricted from either case:


- **Accidental**—Some people just don't know better—or even worse, they *think* they do but they don't. It is these users, that know just enough to do some real damage, that should be your biggest concern. They may mean well—after all, they have a computer at home they tinker with all the time (to which you end up answering endless questions about as well). Restricting users from doing accidental damage to their systems is one of the most common reasons for implementing desktop security restrictions.
- **Deliberate**—You might puzzle as to why someone would deliberately do damage to his or her system. Hopefully, this damage can be largely attributed to “trying things out” without much care for the consequences. Damage that might be considered deliberate includes conscious policy violations such as introducing personal disks to the system.

### **Prevent Installation of Personal Software**

It is natural for users to desire use of software they are familiar with; this often means personal software from home or from another network on which they do business. If the software they would like to have is not available to them on your network, they might attempt to use their own copy. Restricting permissions that result in an inability to install software and restricting access to removable media devices will go a long way to ensuring that this kind of license violation does not occur on your network.

### **Eliminate Unauthorized Installation of Company Software**

Most organizations store copies of software on the network for ease of installation and to ensure a resilient source for Windows Installer setups. If this share is visible and accessible to unauthorized users, they might ignorantly think that it is okay to install. At the very least, they do not have to obtain the software or get it on the network—it is right there calling to them. Keeping installation media locked away in hidden shares or in locations restricted to those with access will greatly reduce the violations that come with unknown installations of software to which you have a limited number of licenses.

 Particularly when users have direct access to the Internet, restricting their ability to install software is a critical first step in maintaining control of your systems.

### **Stop Software Theft**

Does your organization have a network share that contains setup files? Is there a software cabinet to which users have access? Although most users are not likely to steal company-owned software, a much greater number do not have much problem borrowing software to install at home. They might install it on their personal computer and return the software or (even worse) make a copy of the software to bring home and possibly share with others. Restricting access to installation media and removable storage will make such actions more difficult. With any luck, the added effort required to “borrow” software will further remind users that they should not be doing so in the first place.



## **Enforce Proper Usage**

An organization's computers and networks are business assets available to conduct business. Playing games and conducting other personal business on these assets and on company time is usually more than discouraged—it might even be illegal:

### **Playing Games “On the Clock”**

It might seem obvious that if your boss catches you playing Solitaire, it would probably be frowned upon. However, if it was installed as part of the workstation baseline, frowned upon may be as far as it would go. However, if you get caught playing a first person shooter game you bought at the store last week, you can probably expect to be in a bit more trouble. Again, this all comes back to your security policy, but disallowing use of unauthorized software is among the most obvious such policies. Again, the most direct method of restricting such activity is limitations on system access and the use of removable media. Taking it a step further, software inventory or metering software can also play a role in identifying and taking action on such violations.

### **Conducting Personal Business**

Most organizations do not look kindly on employees making fliers for next weekend's cookout, writing long letters to Grandma, or bidding on Star Trek memorabilia on eBay. Although restrictions on such behavior are commonly enforced through casual observation, restricting access to certain Web sites (including Web mail services) is not uncommon.

### **Conducting Illegal Activities**

When you think of illegal activities, you're probably thinking pornography—and you are right. Unfortunately, you hear about this kind of thing way too often and almost everyone knows a story of some kind relating to someone downloading porn at work. Although it is almost a given that you would be deleting the users account soon after getting caught, the organization itself might be liable as well, making this matter very serious. In addition, illegal MP3 files and online gambling services are possible causes for concern in the workplace. Software metering, software inventory, and periodic system scans are common practices to identify such problems.

### **Decrease Proliferation of Viruses**

Though most environments employ a written policy restricting the use of removable media (floppy disks, CD-ROMs, DVDs, zip disks, and other magnetic and optical formats) it is one of the most casually violated security policies. In addition to the options available in restricting access to such devices, a locked down system will limit this kind of proliferation (and in some cases the damage) that a virus will be able to accomplish. Of course, this problem does not end here—you must also remember to address the Internet and email attachments as common methods for viruses to infiltrate your network.

## Principal of Least Privilege

As an administrator (or a user with permissions), a virus has an easier time damaging systems in the user context in which it is executed, both locally and on remote networked systems. An administrator who uses their admin account to process email and download software provides a much bigger risk to the network than that of someone with non-admin access. For this reason, it is common for administrators to have two accounts—the admin account should be used strictly for administration, while their non-admin account can be used for day-to-day work such as reading and responding to email and browsing the Web.

## Protect Data

When users store data on their local systems, it is often not managed and is therefore more likely to be lost. Network shares may be hosted on fault-tolerant drive arrays (protecting it from hardware failure) and backed up on a scheduled basis (protecting it from corruption or deletion). In addition to ensuring a desirable default location for applications to save their data, restricting a users' ability to save data locally will further direct users to a managed location.

## Drawbacks of a Locked Down Environment

As with so many things, although there are many benefits to be gained from a locked down environment, there are also drawbacks. Locking down a desktop environment can result in an environment in which a user cannot operate needed software or perform business-critical tasks. Locked down environments make software deployment and automation more difficult and in the end requires additional (and more thorough) testing to be performed. In this section, we will discuss some of the drawbacks that weigh in the decision to implement a locked down desktop environment.

## Application Failures

As a result of the increased security restrictions that come with Win2K and Windows XP right out of the box, software developers are more conscious of performing actions without regard for user access. Applications that write to the HKEY\_LOCAL\_MACHINE area of a system (outside the actual installation of the application) are one example of a problem that you are far less likely to encounter today. However, there are still many applications that attempt to create and modify files outside of the user profile, where users may have restricted access. An application dependant upon writing to a user restricted area will often result in some sort of error or unexpected behavior, as Figure 5.1 shows.

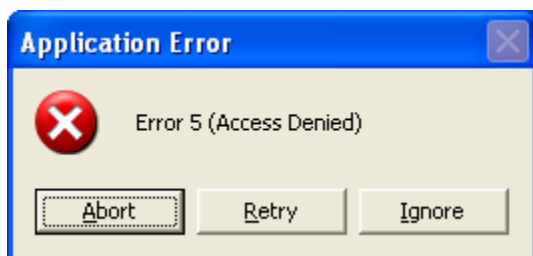



Figure 5.1: A typical error dialog box seen as a result of restrictive access control list settings.


### **Failure to Save Settings**

Some applications attempt to save settings made by a user to a data file instead of the preferred HKEY\_CURRENT\_USER hive of the registry. Particularly common in older applications, such a practice may result in an error when changing preferences or exiting the application (or at whatever point the application attempts to record these settings for future use). Quite often there will be no visible error—the settings will simply fail to be saved.

 I have encountered this failure to save settings several times, but I particularly recall this problem when I was deploying Microsoft FrontPage 98 in a locked down environment. The installation went fine and, not being a user of the application, I did not realize that the application was failing to save its settings. The silent failure to do so was the result of the users' inability to generate two INI files used to store the settings. The files were to be created by the application on first use, and were then to be updated with specified settings as required. Of course, I was following the advice of this book's previous chapter, and quickly discovered this problem in the application testing phase of the package development. The fix was to simply add these two files to the installation package and allow users Change access to the files as part of the deployment.

### **Failures When Saving Data**

A surprising number of applications actually require a fixed local path to create or modify data files. A directory created right off the root of the drive or a subfolder of the program's installation directory are not uncommon “working” directories for many applications. The application may launch and function normally, but when actually working with it to modify or create data, failures may occur. Obviously if you are able to specify a working directory, you may specify an area to which users have necessary access. If the problem is a hard-coded default directory, the simple inability for users to save their work may force them to save to a proper location or it may cause them to lose their work. This situation again shows why actual application use (in the security context of a user and not as an administrator) is a critical step in the package development and deployment process. When a hard-coded working or data directory is required by an application, the decision to allow access to the directory may be one forced on you as a deployment requirement.

 We will discuss methods for modifying access to files and directories later in this chapter.

### **First Launch**

Although you might not know it until you see it fail, some applications perform actions that are restricted to users when the applications are launched for the first time. Some applications attempt to write data to the HKEY\_LOCAL\_MACHINE area of the registry. Others attempt to register DLL files when first launched or when their functionality is first needed. This should be performed as part of the installation process, but might be easily overlooked. Ensure that you log on and perform the initial execution of an application as a user immediately following deployment to determine whether this issue is one you will have to deal with.

## Complex Deployments

Although restricting the environment in which users operate may mean fewer Help desk calls as a result of users' own actions, your own job of testing and deploying software packages becomes far more difficult as a result of a locked down environment:

- Restriction of actions automated for users—Out of the box, the logon script is executed in the security context of the user logging onto the computer. Although you might want to automate printer installation, software configurations, or other restricted actions, such actions may be just that—restricted. Microsoft and third-party utilities and command-line tools exist to trick or even replace this functionality; most environments are limited in their ability to perform actions during user logon as a result of the fact that systems must operate in the security context of the user.
- Bad package or bad application? The failure of an application to run may be the result of a bad deployment package or the application's inability to operate in a locked down environment. The additional step of installing the application and operating it as a user with regular user access to the computer thus becomes a necessity. I have often seen desktop administrators spend hours trying to determine why their script or repackaged installation is failing to operate correctly only to find that even when installed manually, the same problem occurs.

## Political Considerations


Many companies have gone down the locked-down path and found that it decreases productivity, impacts morale, and causes increased difficulties in desktop administration. The decision to lock down your environment (and to what extent) must be measured against your corporate culture and the sensitivity of the systems you are trying to protect. Simply approaching desktop administration from a technical perspective will often result in backlash when the cultural implications are not also taken into account.

## Modifying File and Registry Access and User Rights

With a read-only registry and file system, you may exercise the strictest level of security. However, doing so will most certainly result in application and system failures aplenty. Still, the most methodical and thorough approach to the limitation of file and registry access is to lock everything away from the user, then open only what is deemed necessary on a case-by-case basis. As situations that require relaxed security of specific folders and registry keys increase over time, your once locked down system could become a very open one. It is therefore important that the additional engineering and testing time be taken to identify, document, and adequately justify each security modification determined to be necessary. In this section, we will discuss some of the tools available for modifying registry security, file security, and user rights.

## Registry Security

The registry holds settings for both the user (HKCU) and the computer (HKLM). These computer settings affect everyone that utilizes the system and are typically restricted to manipulation by those with normal “user” access to the system. The installation of most all software requires keys and values to be created in the HKLM hive of the registry. Thus, software installation can be fairly easily restricted simply by ensuring that users are not members of groups that grant them access (such as the Administrators or Power Users groups).

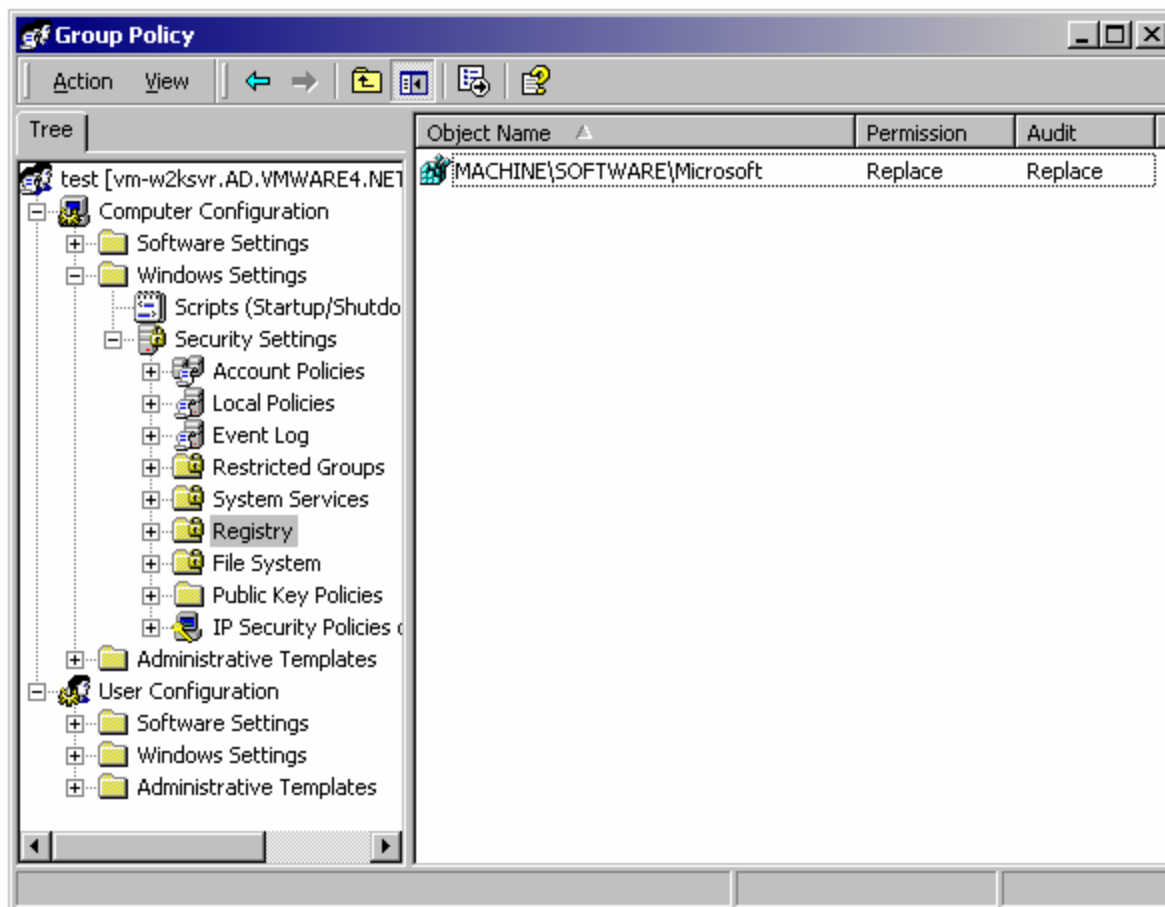
 In Win2K and later, only Administrators and Backup Operators have default network access to the registry. To restrict network access to the registry, create the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg key in the registry, and create a value named Registry Server with a type of REG\_SZ. The Security permissions set on this key define which users or groups can connect to the system for remote registry access. For more details, see the Microsoft article “How to Restrict Access to the Registry from a Remote Computer.”

Because some applications insist on writing to the HKLM area of the registry, you might need to modify permission to allow users write access to certain keys. In other cases, you might not want users to have the ability to make changes to keys that contain certain values. There are several ways to go about modifying registry security; we will cover some of these tools in the following sections.

## Group Policy


In an AD environment in which client systems are running Win2K or later, the preferred way to go about enforcing access control list (ACL) changes to either the registry or the file system is to use Group Policy. You can use the following steps to create a Group Policy Object (GPO) that will modify the permissions of a registry subkey:

1. In a new or existing GPO, navigate to the Windows Settings/Security Settings/Registry folder under Computer Configuration in the tree view on the right (see Figure 5.2).
2. Right-click the Registry folder (or after selecting this folder, right-click in the pane at the right of the display), and choose Add Key.
3. A browse dialog box will appear entitled Select Registry Key. Browse to the key you want to modify or enter the key manually, and click OK to continue.
4. A standard security dialog box will appear in which you can add groups or individuals and choose their desired level of access. Click OK when your desired modifications are complete.
5. A dialog box will appear that lets you choose whether you would like to propagate (edit) the permissions to all subfolders and files or you would prefer to entirely replace the existing permissions. You may also choose not to affect the key changes whatsoever. Click OK to confirm your choice.



**Figure 5.2: GPO with registry security modification.**

Once a GPO such as this has been created, you can link it to any group of computers or organizational unit (OU) containing computers within AD. Many organizations choose to implement a single GPO that contains all ACL changes in their environment. However, where a GPO exists for a specific software distribution, it is common to include the ACL change in the same GPO as the software package. However you choose to implement ACL changes via Group Policy, aim to minimize the number of GPOs required to avoid delays during the startup process.

 You can use Group Policy to manage only Win2K and later clients in an AD environment. Even with AD services installed on earlier versions of Windows, Group Policy is not an option. You can enforce settings on these earlier versions using System Policy, but System Policy can be used only to enforce settings and not to manipulate registry or file security. For these systems, an alternative means of accomplishing this task must be utilized (typically using a command-line utility such as RegINI.)

## RegINI


Available in NT and later resource kits, RegINI provides a means of manipulating registry values and, more importantly, security settings from the command line. The utility specifies an external file that acts as a script for setting and modifying registry entries, and optionally, their security. With its long list of security options and odd formatting, it is not the friendliest of utilities and can prove difficult to work with. Table 5.1 shows many of the permission identifiers that you can use for setting security with this tool.

Permission Identifier	Definition
1	Administrators Full Access
2	Administrators Read Access
3	Administrators Read and Write Access
4	Administrators Read, Write and Delete Access
5	Creator Full Access
6	Creator Read and Write Access
7	World Full Access
8	World Read Access
9	World Read and Write Access
10	World Read, Write and Delete Access
11	Power Users Full Access
12	Power Users Read and Write Access
13	Power Users Read, Write and Delete Access
14	System Operators Full Access
15	System Operators Read and Write Access
16	System Operators Read, Write and Delete Access
17	System Full Access
18	System Read and Write Access
19	System Read Access
20	Administrators Read, Write and Execute Access
21	Interactive User Full Access
22	Interactive User Read and Write Access
23	Interactive User Read, Write and Delete Access

**Table 5.1: RegINI permission identifiers.**

The following RegINI script file will change the permissions of the RunOnce key to allow everyone Full Access:

```
\Registry\Machine
    SOFTWARE
        Microsoft
            Windows
                CurrentVersion
                    RunOnce [7]
```

 Because security settings for a key affect its subkeys as well, you must have permission to change security information for the key and all its subkeys in order to change security information for the key.

## RegDmp

RegDmp is a Windows resource kit utility that works in conjunction with RegINI. It dumps the contents of the registry to an output file in a RegINI-compatible format. Using RegDmp, you can create RegINI input scripts based on actual registry values. You can then modify the contents of RegDmp output to make any modifications you need to the registry.

## SecAdd

SecAdd is a simple command-line tool that allows registry security modification from the command line. It is much easier to use than RegINI, but is more limited in its functionality. You can use the tool to remove the Everyone group from a specified registry key in the HKEY\_LOCAL\_MACHINE hive or to add read access to a specific user for a specified registry key.

## File Security

There are times when you might want to restrict a user's ability to save files to a certain location or to allow access to a certain file or folder in order for an application to operate. When locking down a system, only the files and folders that are required to be modified by users provide such access.

As we have discussed, with everything locked away from the users, there are likely to be situations in which you need to relax certain permissions in order for applications to operate. There are several tools available for managing file security to help you in this task. In this section, we will discuss some of the methods and tools available for modifying file and folder permissions.

## Group Policy

Using the same procedure specified earlier in this section for modifying registry security, you can use Group Policy to modify file security. Once again, this capability is restricted to AD environments in which client OSs are running Win2K or later.



## CACLS

The native CACLS command allows ACL modification from the command line. CACLS supports the following command-line switches:

- /T—Changes ACLs of specified files in the current directory and all subdirectories.
- /E—Edits the ACL instead of replacing it.
- /C—Continues when an access denied error is encountered.
- /G user:perm—Grants specified users access rights; perm can be R (read), W (write), C (change), or F (full control).
- /R user—Revokes specified user's access rights (only valid with /E).
- /P user:perm—Replaces the specified user's access rights; perm can be R (read), W (write), C (change), or F (full control).
- /D user—Denies the specified user access.

You can use wildcards to specify more than one file in a command. You may also specify more than one user in a command.

## XCACLS

The XCACLS tool provides further support for modifying ACLs from the command line. In addition to the switches provided by CACLS, XACLS also supports:

- /X—The same as /E except /X affects only the ACL, which the specified users own.
- /G user:perm;spec—Grants specified users access rights as CACLS does, but provides more options including the ability to modify the ACL for a directory; perm can be R (read), C (change), F (full control), P (change permissions), O (take ownership), X (execute—special access), E (read—special access), W (write—special access), and D (delete—special access.); spec has the same options as perm and will only be applied to a directory.
- /P user:perm;spec—Replaces specified user access rights; it accepts the same parameters as the /G switch.
- /Y—Replaces user rights without verification.

XCACLS is not a native Windows command, but you can download it at no cost from <http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/xcacls-o.asp>.

## SuperCACLS

TrustedSystems.com's SuperCACLS is a third-party tool for command-line manipulation of ACL settings. It contains a suite of tools including PRACL (for printing ACLs in a simple format that you can also use as a backup and restore feature), REACL (for replacing ACLs with new ones), MODACL (for modifying, removing, or adding individual ACL entries, leaving other entries unchanged), and TAKEOWN (for taking ownership of items and optionally granting you full control).

 To learn more about SuperCACLS at <http://www.trustedsystems.com/scacsl.htm>.

## User Rights

User rights dictate which actions a user may perform on an NT and later system. There are several rights restricted by NT and later systems that you can use to limit what a user can do without elevated access to the system. Rights are normally assigned at the group level (as opposed to individual users) and can be assigned from a GUI or command-line interface with various tools made available by Microsoft and other third-party vendors.

From within NT, rights are set using the User Manager for Domains (at the domain level) and User Manager (at the local machine level) tools for defining which groups can perform actions that are restricted by the available user rights. In Win2K and later, there are additional rights that you can specify by using a Group Policy Object (GPO), which may be assigned to an OU or even to the entire domain. Finally, there are tools provided to allow for the command-line granting and revoking of user rights.

## Group Policy

You can specify user rights within any GPO or using the Domain Security Policy snap-in that modifies the Default Domain Policy, which is a GPO assigned at the domain level. It is customary to place domain-wide security settings in this single policy, including the assignment of user rights.

## NT User Manager

In NT, user rights are assigned using the User Manager and User Manager for Domains applets. To access user rights for a domain, launch User Manager for Domains. From the toolbar, click Policies, and choose User Rights. From the drop-down box, choose the right you want to grant or restrict (see Figure 5.3).

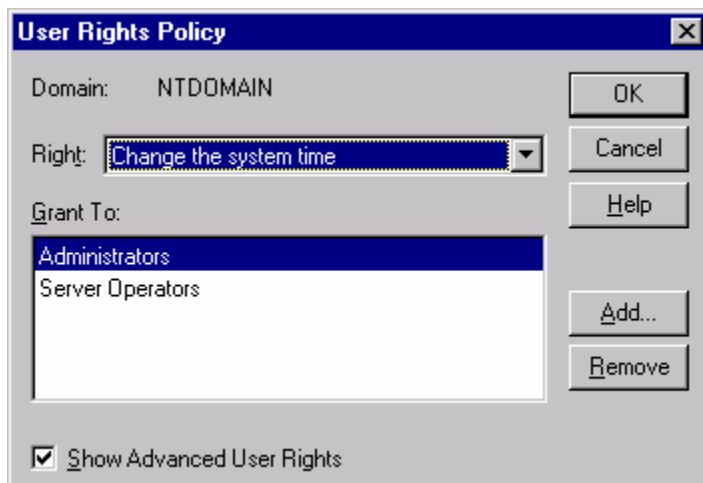



Figure 5.3: User rights manipulation in NT.

## NTRights

You can use the NTRights utility to deny or grant user rights to users and groups from the command line. Table 5.2 defines these rights.

Right	Definition
SeAssignPrimaryTokenPrivilege	Replace a process-level token
SeAuditPrivilege	Generate security audits
SeBackupPrivilege	Back up files and directories
SeBatchLogonRight	Log on as a batch job
SeChangeNotifyPrivilege	Bypass traverse checking
SeCreatePagefilePrivilege	Create a pagefile
SeCreatePermanentPrivilege	Create permanent shared objects
SeCreateTokenPrivilege	Create a token object
SeDebugPrivilege	Debug programs
SeIncreaseBasePriorityPrivilege	Increase scheduling priority
SeIncreaseQuotaPrivilege	Increase quotas
SeInteractiveLogonRight	Log on locally
SeLoadDriverPrivilege	Load and unload device drivers
SeLockMemoryPrivilege	Lock pages in memory
SeMachineAccountPrivilege	Add workstations to domain
SeNetworkLogonRight	Access this computer from the network
SeProfileSingleProcessPrivilege	Profile single process
SeRemoteShutdownPrivilege	Force shutdown from a remote system
SeRestorePrivilege	Restore files and directories
SeSecurityPrivilege	Manage auditing and security log
SeServiceLogonRight	Log on as a service
SeShutdownPrivilege	Shut down the system
SeSystemEnvironmentPrivilege	Modify firmware environment values
SeSystemProfilePrivilege	Profile system performance
SeSystemtimePrivilege	Change the system time
SeTakeOwnershipPrivilege	Take ownership of files or other objects
SeTcbPrivilege	Act as part of the OS
SeUnsolicitedInputPrivilege	Read unsolicited input from a terminal device

**Table 5.2: NTRights command-line rights.**

 The NTRights.exe utility is included in the NT Server 4.0 Resource Kit, Supplement 3.

## Changing Security Context

Although an administrative or service account may have desired rights and ACL accesses, you might not want to provide them to users. To make use of such access and rights for a specific task, you may choose to temporarily change to a user context that does.

Changing the security context of a user to that of one with greater access can be a security risk. Some tools require that a name and password be provided in plain text, which you will need to store in your script or batch file in order to automate such a task. Win2K introduces the RunAs utility that allows you to execute a process using alternative security credentials by specifying a name and password. RunAs does not accept a password as a parameter, which eliminates silent automation of this utility. There are, however, other tools available to help you accomplish the same results, as we will discuss.


## The Switch User Utility (SU.EXE)

Earlier versions of SU required that the user have several rights that are not standard for regular users, including *Act as part of the operating system*, *Increase Quotas*, *Replace a process level token*, and *Restore files and directories*. In addition to having to supply a username and password in clear text, this utility was often considered to be an undesirable option. The current release utilizes a client-side service that eliminates the need for additional rights by users.

You can install the client-side service using the following command:

```
suss.exe -install
```


There are several optional command-line parameters that you can specify to dictate the user name, user account domain, and, of course, the command to be executed.

 The SU utility is available in NT and later resource kits. For more information about the SU utility, see SU.TXT included with the SU utility in the Windows resource kit.

## TqcRunas

Quimeras Software's TqcRunas is a third-party utility that accepts passwords directly in the command line. You can use this utility by creating executable modules or by using the scriptable COM objects provided by the TqcRunas.dll.

 To learn more about TqcRunas, visit <http://www.quimeras.com/TqcRunAs/tqcrunas.htm>.

 In Win2K, Microsoft introduced the RunAs command, which allows a specific command to run in a specified user context by providing the name and password of the account to be used. Unfortunately, the command was specifically designed for manual use and not to be used in a script; the name and password cannot be passed as parameters.


## Controlling Removable Media and Restricting Device Access

When Internet access is limited or unavailable, managing the security of peripheral devices can put up an effective roadblock against the introduction of unauthorized files. You can greatly minimize the introduction of viruses and unauthorized software by preventing their introduction to the network.


Restricting access to floppy and CD-ROM drives is a common practice to help prevent both the introduction and removal of data and software to and from the network. Depending upon how serious you are about this restriction, you may limit access using software controls or even go so far as removing the device entirely.

Windows does offer policies that control access to floppies and CD-ROM drives over the network, but it does not yet provide a built-in ability to restrict access to removable media by the locally logged on user. However, there are resource kit and third-party utilities available to provide restricted access.

- Floplock—Floplock restricts access to floppy drives, allowing only those that are members of the Power Users or Administrators groups to utilize the drive. It is available in both the NT and Win2K resource kits.

 To learn more about the Floplock utility, see the Microsoft article “How to Restrict Floppy Disk Drive Access Using Floplock Service.”

 Floplock is also available as part of Microsoft’s Zero Administration Kit (ZAK)  
<http://www.microsoft.com/networkstation/downloads/Recommended/Featured/NTZAK.asp>.

 Full source code for Floplock is available on the Microsoft Win32 Software Development Kit (SDK) compact disk, in the \q\_a\sd\_floppy directory.


- DeviceLock—SmartLine’s DeviceLock provides control over which users can access specified devices (floppies, serial and parallel ports, magnetic and optical disks, CD-ROMs, USB drives, zip drives, and so on) on a local computer. To learn more about DeviceLock, visit <http://www.protect-me.com/dl/>.

Some manufacturers (Dell being the first major one) have already begun the move to cease shipping computers with floppy drives. However, CD-ROM burners are very common and provide a similar risk in the removal of software from a network.

### Disable PnP and Other Devices

With floppies and CD-ROMs removed or restricted, do not overlook Windows PnP support. If a user sticks a USB memory device into an available USB port, the native support for such a device may even eliminate your ability to simply restrict driver installation.

Devices such as the mouse and keyboard are set to start at startup by default; however, you can edit the registry to modify this behavior. You can set the floppy and CD-ROM not to start in Windows by setting the Start values to 4 in both the Ftdisk and Cdrom keys (under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services). With these devices set to not start, the floppy and CD-ROM drives will not appear to the user when in Windows (before Windows loads, they are still accessible).

 Scripting will be covered with more detail in Chapter 7

## The Load and unload device drivers Right

The *Load and unload device drivers* right (see Figure 5.4) allows users to install and uninstall PnP device drivers. This right does not affect the ability to install drivers that are not PnP—those may only be installed by Administrators.

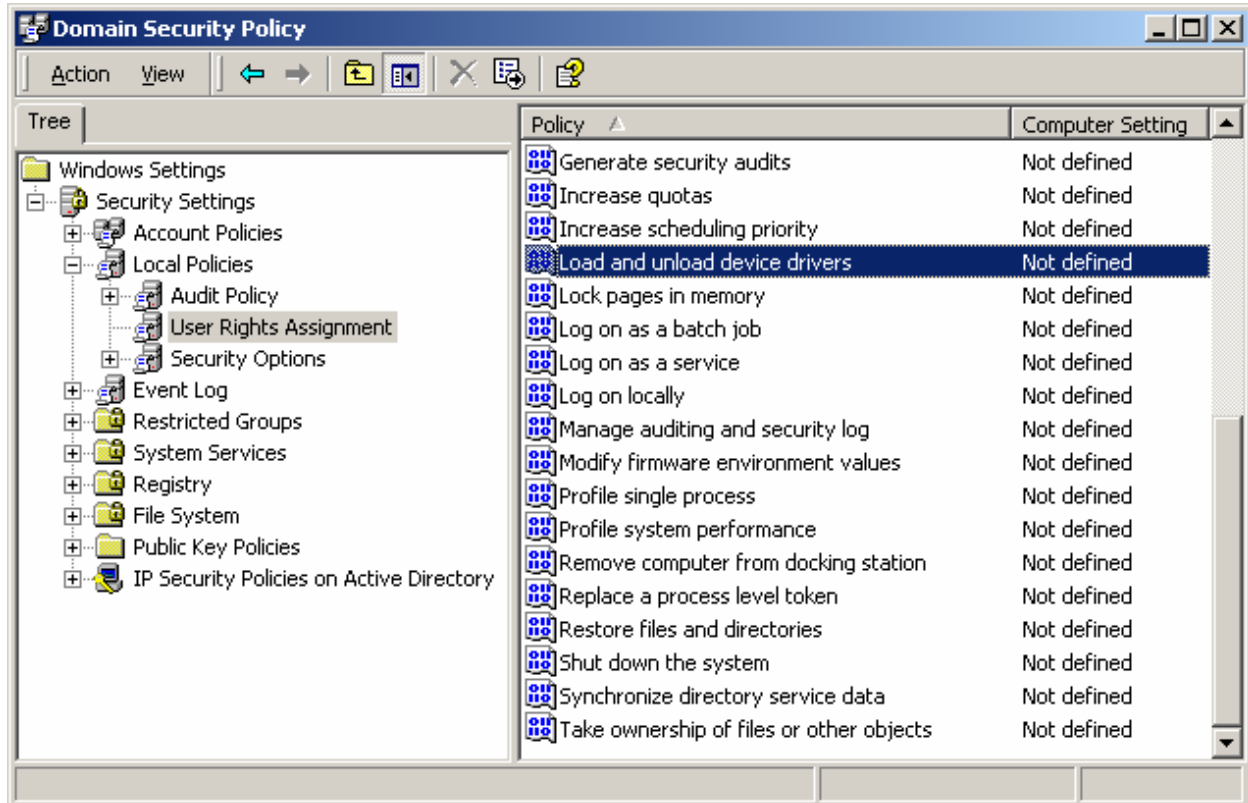


Figure 5.4: User right for loading and unloading drivers.

Many PnP devices do not require administrative privileges to be installed.

## SecureNT

SecureWave SecureNT provides the ability to control end-user access to I/O devices such as the floppy drive, memory sticks, PDAs, USB external storage, CD-ROM, serial and parallel ports, as well as many other PnP devices.

To learn more about SecureNT, visit <http://www.securewave.com/products/securent>.

## General Security Recommendations

Certain security settings will be more or less important to one organization than another. However, there are several security practices that make sense for all environments, as we'll explore in this section.

### Rename Local Administrator Account

By renaming the local administrator account, you make it twice as hard for unauthorized individuals to utilize the account. With a user name and password being the key to full system access, having an administrator account named Administrator provides unauthorized users half of what they need to gain access.

### Enforce Complex Passwords

NT account policies provide the ability to enforce passwords of a certain length, to enforce how often they must be changed, and to limit reuse of passwords through its User Manager tool (see Figure 5.5).

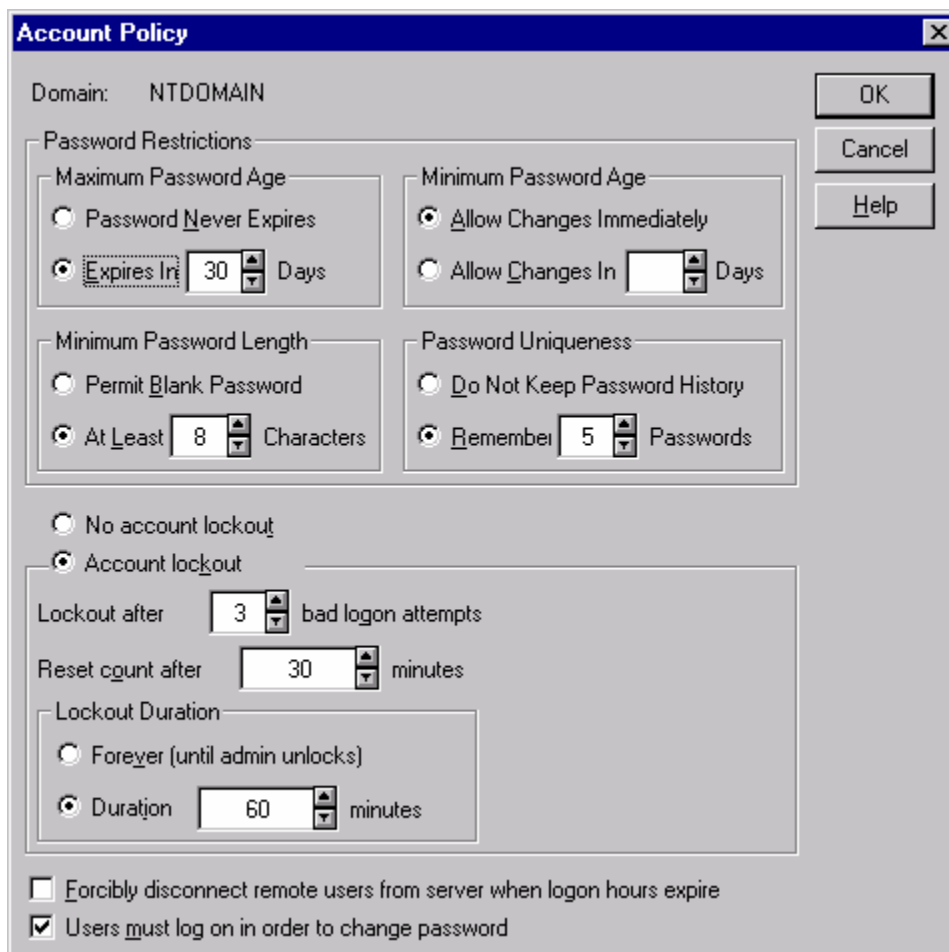


Figure 5.5: NT Account Policy dialog box.

Further, you can enforce complex passwords that must contain at least three of four character types: upper case, lower case, numbers, and special characters (symbols). In NT SP2, you can configure this requirement by performing the following steps:

1. Copy PASSFILT.DLL from SP2 to %WINDIR%\SYSTEM32.
2. Launch a registry editor, and create (or edit) the HKLM\SYSTEM\CurrentControlSet\Control\Lsa key.
3. Add a REG\_MULTI\_SZ value called Notification Packages with a value of PASSFILT (if the value FPNWCLNT already exists, then edit the value, and add PASSFILT under FPNWCLNT).
4. Restart the server.

For Win2K and later servers, this information may be set within a GPO, typically the Domain Security Policy GPO, which Figure 5.6 shows.

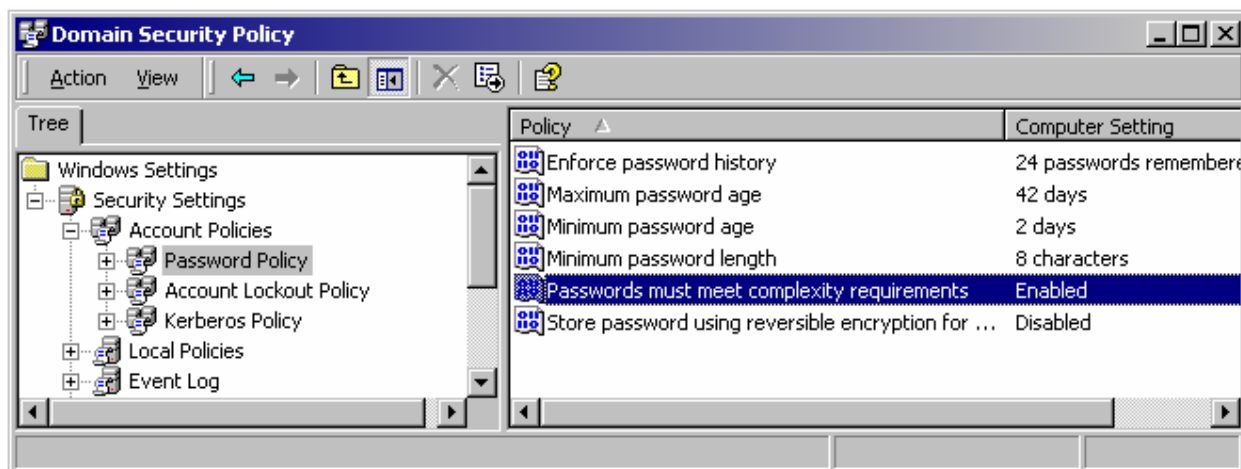


Figure 5.6: Domain Security Policy's password policy settings.

### Disable Guest Account

On Win2K and later, the guest account is disabled by default. However, before rolling an image out across your network, it is wise to give this setting a quick check to ensure that the Guest account is disabled. With the guest account enabled, users may utilize the guest account to access resources without providing credentials of their own.

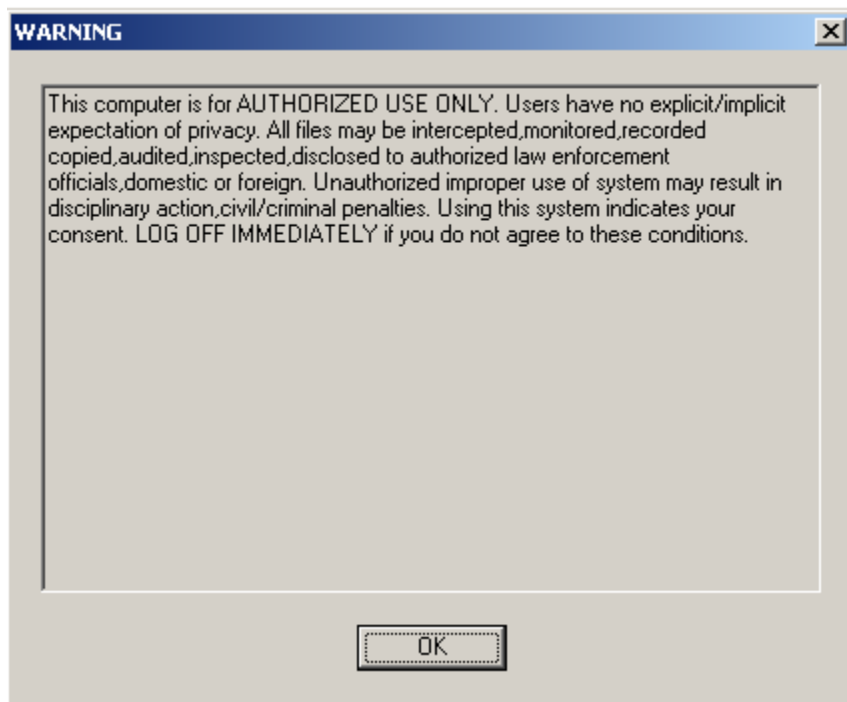
### Replace the Everyone Group with Authenticated Users on File Shares

Authenticated Users was added with the release of NT SP3 and is included by default within Win2K. The Everyone group includes even unauthenticated users, whereas the Authenticated Users group includes only users who have supplied proper credentials. Wherever possible, remove permissions from the Everyone group and replace it with permissions for Authenticated Users.



### **Employ Logon Warning Messages**


Security banners are presented when Ctrl+Alt+Delete is pressed, before the logon box is presented for entering a user name and password. It is customary to make use of this feature in order to provide a legal warning or notice of how the system may be used.



*Figure 5.7: Example logon security banner.*

### **Hide Last Logged On User Name**

Without a policy in place to prevent it, the name of the last user who logged onto the computer is already typed into the Windows logon dialog box and only the password need be entered. Although this configuration is more convenient, it gives someone attempting to break into the system half of what he or she needs to gain access. You can disable this setting through the registry or using NT System Policy or Win2K Group Policy.

 For more information about this setting, see the Microsoft article "HOW TO: Prevent the Last Logged-On User Name from Being Displayed in Windows 2000."

### **Password Protect the Screensaver**

By enforcing a screensaver timeout period and specifying that the system should lock when the screensaver activates, you can minimize the possibility of someone sitting down at a machine and performing actions with another user's credentials. You can configure this setting through either System Policy or Group Policy, depending upon your environment.

## Enable Auditing

The most basic form of intrusion detection for NT and later is to enable auditing. Doing so will alert you to changes in account policies, attempted password hacks, unauthorized file access, and other configurable items. Consider auditing the events that Table 5.3 shows.

Event	Setting
Account logon events	Success, failure
Account management	Success, failure
Logon events	Success, failure
Object access	Success
Policy change	Success, failure
Privilege use	Failure
System events	Success, failure

**Table 5.3: Suggested auditing configuration settings.**

## Use RunAs

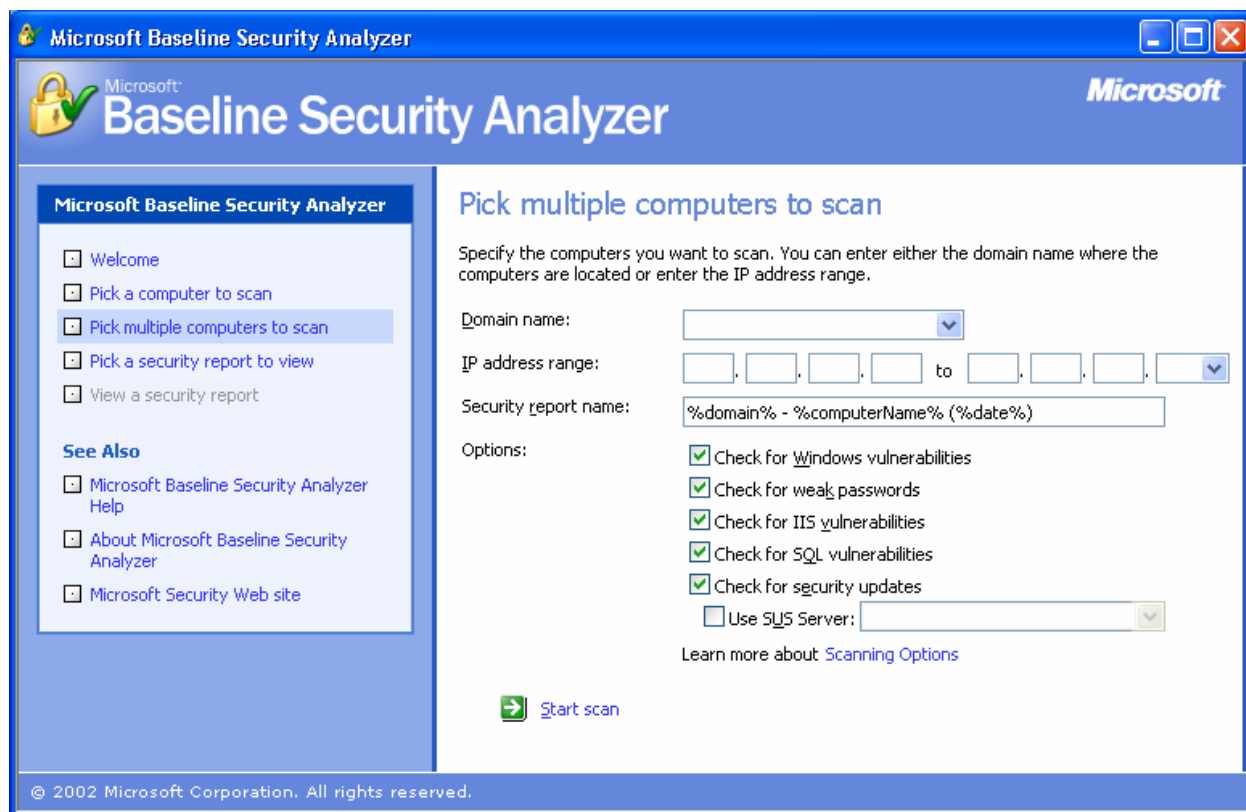
Using the Win2K and later RunAs command will allow you to perform the functions that require administrative access while logged on as a user with normal access. One reason to avoid being logged on as an administrator unnecessarily is that any viruses or malicious code you should encounter will run in the security context in which you are logged on. With administrative permissions, such a situation has the potential to be far more damaging not only to your system but to others on the network.

## Examining Your Security

Once you've implemented your desired security settings on your systems, it's time to check whether you missed anything. After systems have been in use for a few months, do they still comply with your desired settings? You've implemented different security policies to several OUs via Group Policy, do they conflict? Always perform periodic checks and be aware of the tools you can use to troubleshoot conflicts. In this section, we will discuss some of the tools available to help you do just that.

### Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer checks computers running NT 4.0, Win2K, and Windows XP for common security issues. The tool provides recommendations and is useful for identifying misconfigurations—it focuses on items that are appropriately set by default. IN addition, it lets you scan remote systems (provided you have access); thus, in a large environment in which systems are not well managed, this tool can be very helpful in identifying problems you might have otherwise assumed were not an issue for your network. It provides a HTML view as well as links to what it scanned and how to correct any problems (see Figure 5.8).



**Figure 5.8:** The Microsoft Baseline Security Analyzer.

The tool scans and reports on several security-related configuration settings for the Windows OS as well as some specific Microsoft applications such as Outlook and Office. The items processed as part of a scan of Windows include:

- Checking for missing security updates and service packs
- Checking for account password expirations
- Checking for which file system is in use for local hard drives
- Checking to see whether the autologon feature is enabled
- Checking to ensure that the guest account is not enabled
- Checking the RestrictAnonymous registry key settings (dictates access for anonymous users)
- Checking the number of local Administrator accounts (should be only one or two)
- Checking for blank or simple local user account passwords
- Checking to ensure that there no unnecessary services are running
- Listing the shares present on the local computer
- Checking to see whether auditing is enabled



The Microsoft Baseline Security Analyzer is available for download at <http://www.microsoft.com/technet/security/tools/tools/MBSAHome.ASP>.

### **Security Configuration and Analysis**

You can use the Security Configuration and Analysis Microsoft Management Console (MMC) snap-in to compare (or apply) a system with a security template:

1. Select Run from the Start menu, and type  
MMC  
into the Run text box, then click OK.
2. Select Add/Remove Snap-in from the Console menu on the toolbar, then select Security Configuration and Analysis, and click Add.
3. Click Close, then click OK.
4. Right-click the Security and Configuration Analysis node, and select Open Database. Here you may type in any name (the security database is just temporary storage for this program). You may also make a copy of the Secedit.sdb file from the Winnt\Security\Database folder from a domain server and specify this file to compare local settings with that of Group Policy settings.
5. Choose a template to import. You can also make your own template using the Security Templates MMC snap-in. The template is a database of recommended security settings. The following are some of the predefined templates that are available:
  - basicdc.inf contains basic security settings for an AD domain controller
  - basicsv.inf contains basic security settings for a Win2K server
  - basicwk.inf contains basic security settings for a Win2K Professional machine
  - compatws.inf contains low security settings for a Win2K Pro machine in a mixed mode domain (NT compatible)
  - hisecdc.inf contains high security settings for an AD domain controller
  - hisecwk contains high security for a Win2K server

Choose the security template that is appropriate for your situation, and click Open.

6. Right-click the Security Analysis and Configuration node in the left pane, and select Analyze Computer Now from the resulting menu.

The computer's settings are compared with those that are recommended by the template, and when complete, you can navigate through all the items in the left pane. A red X will appear in the right pane for any settings that conflict with the selected template, as Figure 5.9 illustrates.



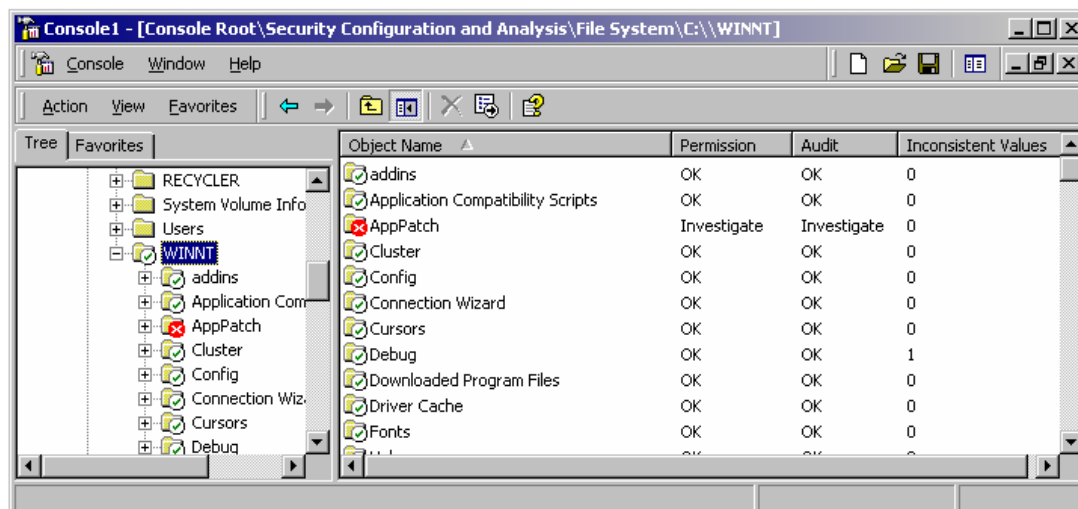




Figure 5.9: The security analysis results view.

 The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have both published Win2K security guidelines as well as security templates that are available online at [http://csrc.nist.gov/itsec/guidance\\_W2Kpro.html](http://csrc.nist.gov/itsec/guidance_W2Kpro.html) and <http://www.nsa.gov/snac/win2k/index.html>, respectively.

## SecEdit

SecEdit performs the same functions as the Security Configuration and Analysis snap-in, but does so from the command line. It configures and analyzes system security by comparing a system's current configuration with a specified security template. SecEdit supports several switches. You can use the following switches to analyze security:

- /db—Specifies the path and file name of a database that contains the stored configuration against which the analysis will be performed
- /cfg—Specifies the path and file name for the security template that will be imported into the database for analysis
- /log—Specifies the path and file name of the log file for the process
- /quiet—Suppresses screen and log output, but the results can be viewed with the Security Configuration and Analysis snap-in described earlier.

 You can use Secedit.exe with the /REFRESHPOLICY switch to impose Group Policy object settings upon a target workstation. To immediately enforce GPO settings located within the machine node of relevant GPOs, type

```
SECEDIT /REFRESHPOLICY MACHINE_POLICY /ENFORCE
```

To do the same for the user node of the relevant GPOs, type

```
SECEDIT /REFRESHPOLICY USER_POLICY /ENFORCE
```

For Windows XP and later, this functionality has been replaced with the GPUPDATE command.

## Event Log Management

Event logs are a good troubleshooting tool, and with auditing in place, there is often a requirement to maintain, back up, and archive log files for security reasons. You can configure and back up event logs in multiple ways, a few of which are explored in this section.

### Configuring Event Logs' Retention

Locally, or via policy, you can configure the Application, Security, and Systems logs independently. You can specify how large they may get and how long you would like to keep them (see Figure 5.10).

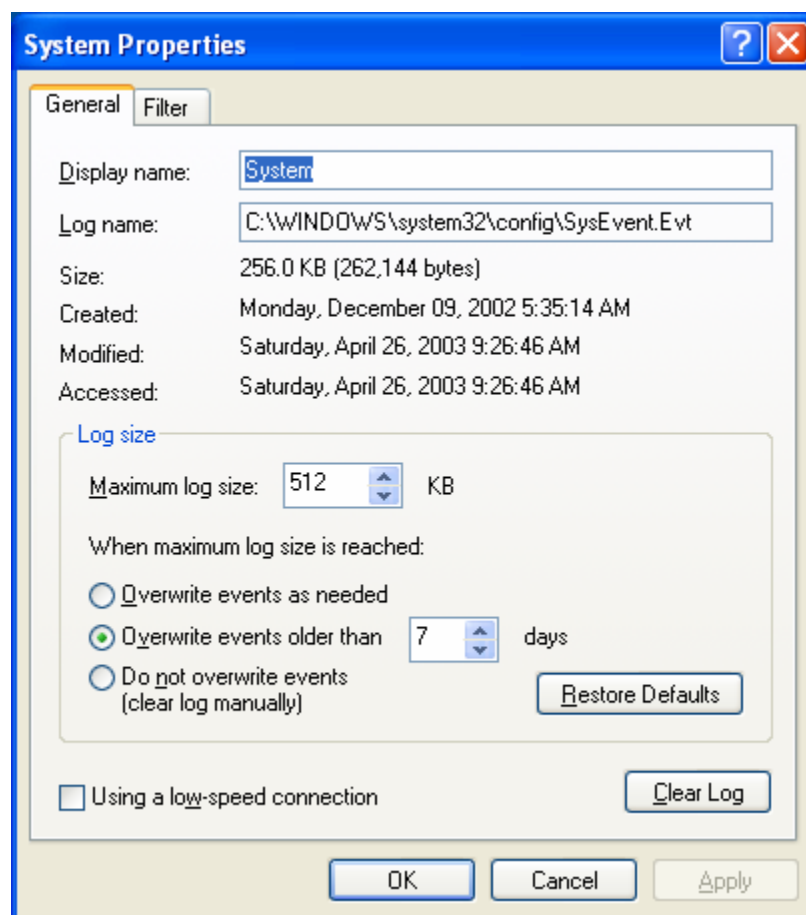


Figure 5.10: System event log default retention settings.

You can also configure event properties using Group Policy (see Figure 5.11) and assign those preferences to an entire domain or specific OU.

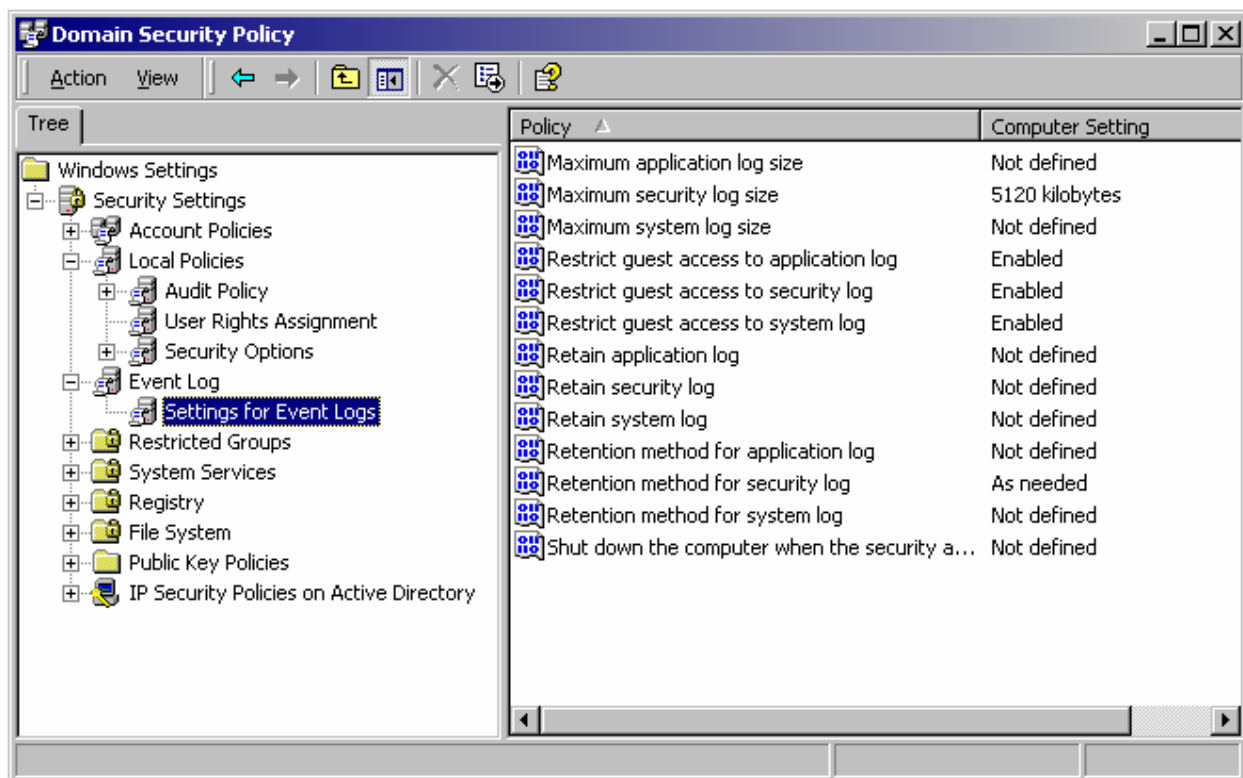


Figure 5.11: Domain security policy event log settings.

## Archiving Event Logs

An audit trail can contain information about changes that are made to computers on the network. If intruders gain Administrator rights and permissions, or if administrators abuse their rights and permissions, they can erase event logs' entries to conceal their actions. If you regularly back up and archive security log entries across your organization, even if entries are cleared, you have an increased chance of being able to trace the actions of intruders or administrators using your archived copies:

- **DumpEL**—Dump Event Log is a command-line tool that dumps an event log for a local or remote system into a tab-separated text file. You can also use this tool to filter for or filter out certain event types. Although you can export the data in a tab-delimited or comma-delimited format, the tool does not dump the files in the native .evt file format that the Event Viewer uses.

 DumpEL is available in the Win2K resource kit or online, at <http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp>.

- EventSave—This freeware utility saves event logs in their native .evt file format to a specified location. It creates one file for each month named year\_month\_computer\_xxx.evt, where xxx is the name of the log (Application, Security, or System).

 For more information about EventSave, visit [http://www.heysoft.de/Frames/f\\_sw\\_es\\_en.htm](http://www.heysoft.de/Frames/f_sw_es_en.htm).

More robust solutions exist that include event log collection and reporting, such as Microsoft Operations Manager (MOM) those from NetIQ. Such systems can provide a consolidated view of an entire organization's event logs.

## Summary

In this chapter, we have explored how to generate a security policy for your environment and the benefits and drawbacks of implementing a locked down environment. We also discussed some general security recommendations and methods that you can use to examine your own security configuration. In the next chapter, we will discuss desktop support, exploring methods and tools, including remote control.