

UNCLASSIFIED

Report Number: C4-052R-00

Guide to Securing Microsoft Windows 2000[®] Group Policy: Security Configuration Tool Set

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

Author:
Julie M. Haney



Updated: May 17, 2001
Version 1.0

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

410-854-6015
SecureW2K@dewnet.ncsc.mil

UNCLASSIFIED

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Disclaimer

SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL THE NATIONAL SECURITY AGENCY OR ANY AGENT OR REPRESENTATIVE THEREOF 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 UNDER ANY THEORY OF LIABILITY, ARISING IN ANY WAY OUT OF THE USE OF OR INABILITY TO MAKE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Disclaimer

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

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, and 3.0, 4.0, and 4.1.

The author acknowledges Michael Samsel for his development of the Enhanced Password DLL included with this guide.

The author would also like to thank Paul Bartock, Neal Ziring, Edward Wojciechowski, and Kim Downin, along with the many others involved in reviewing this document. Your comments and suggestions were invaluable.

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

Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

Disclaimer iii

Acknowledgements v

Trademark Information vi

Table of Contents vii

Table of Figures ix

Table of Tables x

Chapter 1 Important Information on Using this Guide 11

Assumptions 11

Warnings to Review Before Using this Guide 11

Conventions and Commonly Used Terms 12

About the Guide to Securing Microsoft Windows 2000: Security Configuration Tool Set 13

Comments 14

Chapter 2 Introduction to the Security Configuration Tool Set 15

Security Configuration Functionality 16

Security Templates 16

 Default Security Templates 18

 Microsoft-provided Templates 18

 NSA Security Templates 18

Checklist for Applying the Recommendations in this Guide 19

Undoing Security Changes 20

Chapter 3 Modifying Account Policy Settings with Security Templates 21

Password Policy 21

Account Lockout Policy 25

Kerberos Policy 25

Chapter 4 Modifying Local Policy Settings with Security Templates 27

Auditing Policy 27

User Rights Assignment 29

Security Options 35

Adding an Entry to Security Options 50

Chapter 5 Modifying Event Log Settings with Security Templates 53

Event Log Settings 53

Managing the Event Logs 54

Chapter 6 Managing Restricted Groups with Security Templates.....	57
<i>Modifying Restricted Groups via the Security Templates Snap-in.....</i>	<i>57</i>
Chapter 7 Managing System Services with Security Templates	59
<i>Modifying System Services via the Security Templates Snap-in.....</i>	<i>59</i>
<i>System Services Security.....</i>	<i>60</i>
Chapter 8 Modifying Registry Security Settings with Security Templates.....	63
<i>Inheritance model.....</i>	<i>63</i>
<i>Registry permissions.....</i>	<i>63</i>
<i>Modifying Registry settings via the Security Templates snap-in.....</i>	<i>65</i>
<i>Recommended Registry Key Permissions.....</i>	<i>67</i>
Chapter 9 Modifying File System Security Settings with Security Templates	73
<i>File and folder permissions</i>	<i>73</i>
<i>Modifying File System settings via the Security Template snap-in.....</i>	<i>76</i>
<i>Recommended File and Folder Permissions</i>	<i>78</i>
Chapter 10 Security Configuration and Analysis	87
<i>Loading the Security Configuration and Analysis snap-in into the MMC.....</i>	<i>87</i>
<i>Security Configuration Databases.....</i>	<i>88</i>
<i>Secedit Command Line Options</i>	<i>89</i>
<i>Performing a Security Analysis</i>	<i>90</i>
<i>Configuring a System.....</i>	<i>92</i>
Appendix A Example Logon Banner.....	95
Appendix B References.....	96

Table of Figures

Figure 1 Security Templates snap-in17
Figure 2 Password Policy Recommended Settings.....24
Figure 3 Recommended User Rights29
Figure 4 System Services60
Figure 5 Advanced Registry Permissions Dialog Box66
Figure 6 File/Folder Permission Inheritance Options79
Figure 7 Configuration File Selection.....89
Figure 8 Results of a Security Analysis92

Table of Tables

Table 1 Default Security Configuration Files	18
Table 2 Enhanced Security Configuration Files.....	19
Table 3 Password Policy Options	23
Table 4 Account Lockout Options	25
Table 5 Kerberos Policy Options	26
Table 6 Audit Policy Options.....	28
Table 7 User Rights Options.....	35
Table 8 Security Options.....	50
Table 9 Domain-wide Security Options	50
Table 10 Event Log Options	54
Table 11 Registry Permissions and Descriptions	64
Table 12 Registry Permission Options	64
Table 13 Recommended Registry Permissions.....	71
Table 14 File Permissions and Descriptions.....	74
Table 15 Folder Permissions Options.....	75
Table 16 File Permissions Options	76
Table 17 Recommended File Permissions	86
Table 18 Secedit Command Line Parameters.....	90

Important Information on Using this Guide

The purpose of this document is to inform the reader about the Windows 2000 Security Configuration Tool Set's capabilities and recommended security settings that can be configured via the tool set. This document represents only a portion of Group Policy security-related issues. **Additional security information on Group Policy Objects (GPOs) is addressed in the *Guide to Securing Microsoft Windows 2000 Group Policy*, which should be read prior to reading this document.**

Included with this document are four security templates: W2K DC.inf, W2K Workstation.inf, W2K Server.inf, and W2K Domain Policy.inf. The purpose and use of these templates will be discussed later in this document.

This document is intended for Windows 2000 network administrators, but should be read by anyone involved or interested in Windows 2000 or network security.

Assumptions

The following essential assumptions have been made to limit the scope of this document:

- ❑ The network consists only of machines running Microsoft Windows 2000 clean-installed machines (i.e., not upgraded).
- ❑ 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://windowsupdate.microsoft.com> or search for security hotfixes by service pack at the Technet Security Bulletin Search <http://www.microsoft.com/technet/security/current.asp>.
- ❑ All network machines are Intel-based architecture.
- ❑ Applications are Windows 2000 compatible.
- ❑ Users of this guide have a working knowledge of Windows 2000 installation and basic system administration skills.

Warnings to Review Before Using this Guide

The user should read and agree with the following warnings/caveats prior to configuring a network with this guide's recommendations:

- ❑ **Do not attempt to install 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 while using products such as Microsoft Exchange, IIS, and SMS.

- ❑ The security changes described in this document only apply to **Microsoft Windows 2000** systems and should not be applied to any other Windows 2000 or Windows NT versions or operating systems.
- ❑ A Windows 2000 system can be severely impaired or disabled with incorrect changes or accidental deletions when using programs (examples: Security Configuration Tool Set, `Regedt32.exe`, and `Regedit.exe`) to change the system configuration. Therefore, it is extremely important to test all settings recommended in this guide before installing them on an operational network.
- ❑ Currently, no Undo function exists for deletions made within the Windows 2000 registry. The registry editor (`Regedt32.exe` or `Regedit.exe`) prompts the user to confirm the deletions if **Confirm On Delete** is selected from the options menu. When a registry key is being deleted, the message does not include the name of the key being deleting. Check your selection carefully before proceeding with any deletion.
- ❑ Care should be taken when applying this document's recommended security settings on Exchange 2000 servers. There will be occasional notes/warnings when settings could affect the operation of Exchange servers, but it is highly recommended that the upcoming NSA Exchange 2000 security guide be reviewed prior to applying the provided recommendations.

Conventions and Commonly Used Terms

Users and Authenticated Users

For permissions on Windows 2000 workstations and member servers, Microsoft now makes wide use of the Users group. The Users group by default contains the Authenticated Users group and INTERACTIVE user (along with Domain Users for a domain machine). Membership in Users can be controlled by administrators, which is Microsoft's reasoning for using this group in access control lists. Looking at the default security templates for workstations and member servers (see the next chapter for information on these templates), the Users group is used in file and registry permissions as well as user rights assignment.

However, Microsoft uses the built-in Authenticated Users group to assign permissions on domain controllers. Out-of-the-box domain controller security templates replace Users with Authenticated Users.

This guide has chosen to follow Microsoft's convention. No security should be lost if you choose to replace the Users group with the Authenticated Users group on workstations and member servers.

System Variables

The following system variables are referenced throughout this document:

- **%SystemDrive%** - The drive letter on which Windows 2000 is installed. This is usually C:\.
- **%SystemRoot%** - The folder containing the Windows 2000 operating system files. This is usually %SystemDrive%\winnt.
- **%SystemDirectory%** - %SystemRoot%\system32

- **%ProgramFiles%** - Folder in which most applications are installed. This is usually %SystemDrive%\Program Files.

About the Guide to Securing Microsoft Windows 2000: Security Configuration Tool Set

This document consists of the following chapters:

Chapter 1, “Important Information on Using this Guide,” (this chapter) provides important assumptions and warnings to be read prior to using the guide.

Chapter 2, “Introduction to the Security Configuration Tool Set,” provides an overview of the Security Configuration Tool Set and its capabilities and describes how to use the Security Templates Microsoft Management Console (MMC) snap-in to implement, edit, and create new security configuration files. This chapter also introduces the security configuration files included with this document and details a checklist for configuring a network using the provided settings.

Chapter 3, “Modifying Account Policy Settings with Security Templates,” explains how to set domain wide account policies using the Security Templates snap-in. The section also covers Password Policy, Account Lockout, and Kerberos Policy.

Chapter 4, “Modifying Local Policy Settings with Security Templates,” illustrates how to use the Security Templates snap-in to implement and modify Local Policy settings. Specifically this section describes suggested policies for Auditing, User Rights, and Security Attributes.

Chapter 5, “Modifying Event Log Settings with Security Templates,” explains how to capture, view, and store the critical events that have occurred on the network by modify the Event Log Settings. Also included in this section is management of Event Logs.

Chapter 6, “Managing Restricted Groups with Security Templates,” discusses how to manage the membership of sensitive groups using the Restricted Groups option.

Chapter 7, “Managing System Services with Security Templates,” illustrates how to manage System Service settings such as Startup Modes and Access Control Lists using the Security Templates snap-in. This section also describes how settings are established that can control which users and/or groups can read and execute, write to, delete, start, pause, or stop a service.

Chapter 8, “Modifying Registry Security Services with Security Templates,” discusses how to configure access control lists for Registry Keys. Also discussed is how to implement adequate security in a Windows 2000 environment, by modifying registry keys and their associated permissions must be changed.

Chapter 9, “Modifying File System Security Settings with Security Templates,” steps the reader through the actions required to modify file and folder permissions using the Security Templates snap-in. Additionally, this section outlines recommended file and folder permission settings.

Chapter 10, “Security Configuration and Analysis,” explains how to perform security analysis and configuration via the Security Configuration and Analysis snap-in or the command line program, once the appropriate configuration file(s) have been modified.

Comments

As this document is a work in progress, comments, suggestions, questions, and bug reports are welcomed and encouraged. Send an email to W2KComments@dewnet.ncsc.mil describing the issue in detail. In order to allow ample time to research problems, email is preferred to phone calls.

Introduction to the Security Configuration Tool Set

Windows 2000 includes support for the Security Configuration Tool Set. The tool set allows system administrators to consolidate many security-related system settings into a single configuration file (called a template or `inf` file in this guide because of the file extension `.inf`). It is possible to layer security configuration files to adjust for different software applications and security settings. These security settings may then be applied to any number of Windows 2000 machines either as part of a Group Policy Object (GPO) or through local computer configuration.

The Security Configuration Tool Set allows analysis and configuration of the following security areas:

- **Account Policies** - includes Password Policy, Account Lockout Policy, and Kerberos Policy
- **Local Policies** – includes Audit Policy, User Rights Assignment, and Security Options
- **Event Log** – includes settings for the event logs
- **Restricted Groups** – includes membership settings for sensitive groups
- **System Services** – includes configurations for system services such as network transport
- **Registry** – includes registry key Discretionary Access Control List (DACL) settings (i.e., registry key permissions)
- **File System** – includes NTFS file and folder DACLs (i.e., file and folder permissions)

Chapters 3 – 9 describe recommended settings and how to customize the templates, and Chapter 10 describes how to conduct a security analysis and configuration.

For more detailed information on the Security Configuration Tool Set, refer to the *Step by Step Guide to Using the Security Configuration Toolset* <http://www.microsoft.com/windows2000/techinfo/planning/security/secconfsteps.asp>.

Security Configuration Functionality

The Security Configuration Tool Set supports both a graphical user interface (GUI) and a command line tool.

The Security Configuration GUI

The graphical user interface is provided via the Microsoft Management Console (MMC). The MMC is a container for administrative tools and is used extensively in Windows 2000. Tools are imported into the MMC via “snap-ins.”

In actuality, the Security Configuration Tool Set consists of two MMC snap-ins: Security Templates and Security Configuration and Analysis. Both snap-ins will be discussed in greater detail in this chapter and Chapter 10, respectively.

The security configuration GUI allows an administrator to:

- Create and/or edit security configuration files
- Perform a security analysis
- Graphically review the analysis results
- Apply a security configuration to a system

The GUI provides different colors, fonts, and icons to highlight the differences between the baseline information and the actual system settings. When an analysis or configuration is performed, all security areas within a security template are included in the analysis.

The Security Configuration Command Line Tool

The security configuration command line tool (`secedit.exe`) is all that is needed to:

- Perform a security analysis
- Apply a security configuration to a Windows 2000 system

The command line option allows for analysis of individual security areas versus the entire configuration file. Also, analysis results can be redirected to a file for review at a later time. The command line tool is also useful for applying predefined configuration files to many systems using distributed systems management tools.

Security Templates

Security templates are files that contain a set of security configurations. Templates provide an easy way to standardize security across a platform or domain. They may be applied to Windows 2000 computers either by being imported into a Group Policy Object, or by being directly applied to the local computer policy.

This section provides a general overview of the Security Templates snap-in and discusses the security configuration files included with the tool.

Loading the Security Templates Snap-in into the MMC

The Security Templates snap-in must be loaded into the Microsoft Management Console (MMC). The MMC is loaded by default on Windows 2000 systems. To load the Security Templates snap-in:

- ❑ Run the Microsoft Management Console (`mmc.exe`)
- ❑ Select **Console** → **Add/Remove Snap-in**
- ❑ Click **Add**
- ❑ Select **Security Templates**
- ❑ Click **Add**
- ❑ Click **Close**
- ❑ Click **OK**

Figure 1 shows the Security Templates snap-in loaded into the MMC.

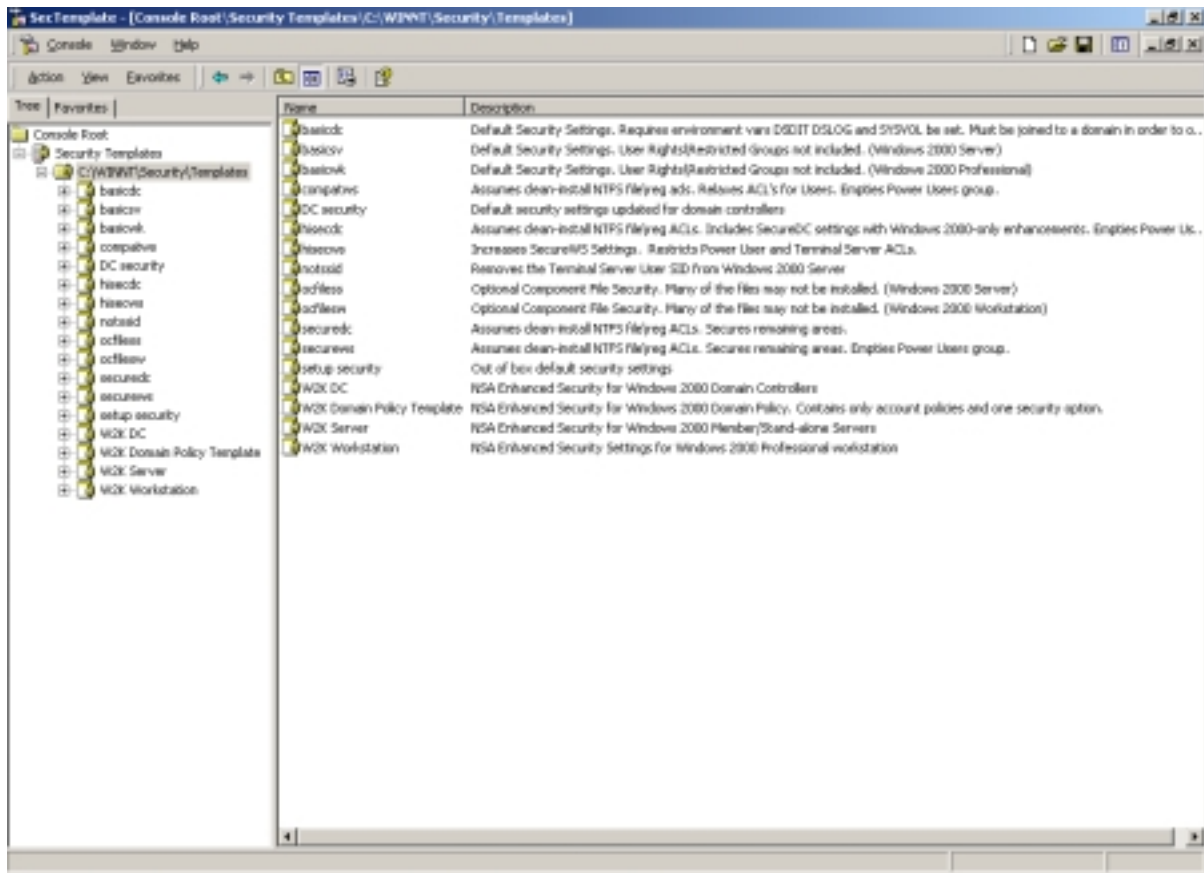


Figure 1 Security Templates snap-in

To avoid having to reload the snap-in every time the MMC is exited and reopened, save the current console settings by performing the following:

- ❑ In the **Console** menu, select **Save**. By default, the file will be saved in the Administrative Tools menu of the currently logged-on user.

- ❑ Enter the file name under which the current console settings will be saved
- ❑ Click **Save**

From then on, the console can be accessed from **Start → Program Files → Administrative Tools**.

Security Configuration Files

This section describes the default and NSA security templates available for the Security Templates snap-in.

Default Security Templates

There are several security template files that contain the default security settings applied to a clean-install (non-upgraded) Windows 2000 machine. These files reside in the %SystemRoot%\inf folder. **Table 1** shows a list of the default security templates.

The default security templates are especially useful when wanting to return the system to its original state or when converting from a FAT or FAT32 file system to NTFS. When a conversion is made, the default settings on the file system default to the “Everyone” group having full control over all files and folders. To obtain the file system security settings that would have been present if NTFS had been the original file system, apply the File System portion of the appropriate default security template. See Chapter 10 for more information on running `secedit.exe` and specifying that only the file system be configured.

File Name	Platform
Defltdc.inf	Windows 2000 Server/Advanced Server Domain Controller
Defltsv.inf	Windows 2000 Server/Advanced Server
Deflwtk.inf	Windows 2000 Professional

Table 1 Default Security Configuration Files

The template actually applied to a machine out-of-the-box is stored in %SystemRoot%\security\templates as `setup security.inf`. Domain controllers will, in addition, be configured with the settings in a template called `DC security.inf`.

Microsoft-provided Templates

Within the Security Templates snap-in, Microsoft provides several templates addressing varying levels of security. Among these are `basicwk.inf`, `basicdc.inf`, `basicsv.inf`, `securedc.inf`, `securews.inf`, `hisecdc.inf`, and `hisecws.inf`. Since this guide’s recommended security settings are addressed in the NSA-provided templates (see section below), the details of the Microsoft templates will not be discussed here.

NSA Security Templates

This document also includes a set of security configuration files that comply with the recommendations found in this manual. Refer to **Table 2** below in order to choose the file(s) appropriate for your system(s).

File Name	Platform	Description
W2K DC.inf	Windows 2000 Server/Advanced Server Domain Controller	Enhanced security settings for Windows 2000 domain controllers
W2K Workstation.inf	Windows 2000 Professional	Enhanced security settings for Windows 2000 workstations
W2K Server.inf	Windows 2000 Server/Advanced Server	Enhanced security settings for Windows 2000 member or standalone servers
W2K Domain Policy	Windows 2000 domain	Enhanced account policy settings to be applied in a domain-level Group Policy Object

Table 2 Enhanced Security Configuration Files

Checklist for Applying the Recommendations in this Guide

This section provides a general checklist of steps to be performed when customizing the security templates included in this document.

- ❑ Review and understand the warnings in Chapter 1. **It is NOT recommended that the NSA-provided templates be applied blindly without thoroughly reviewing the settings in Chapters 3-9.**
- ❑ Backup your system, especially if it is a server or domain controller. Backups are the only sure-fire way to restore your system if security configurations break something.
- ❑ Copy the appropriate configuration files included on the companion CD to the template directory (%Systemroot%\Security\Templates). Review **Table 2** to determine the necessary template file(s).
- ❑ It is suggested that you make copies of the template files under different names if you plan to perform modifications to the recommended settings. You can do this prior to opening the files in the MMC, or by performing a **Save As** after making modifications to the templates (see the above section on **Editing Security Configuration Files**).
- ❑ Several new security options have been added to the NSA templates. To make these options available, copy the NSA `sceregl.inf` file from the companion CD into the %SystemRoot%\inf folder. You should rename the original copy of `sceregl.inf` prior to copying the NSA-provided file in case you need to revert back to original configurations.
- ❑ To register the new security options, from the command prompt run `regsvr32 scecli.dll`. The end of Chapter 4 discusses how other security options can be added to the templates.
- ❑ Review the recommended security settings in Chapters 3 – 9. Via the Security Templates MMC snap-in, modify the template files according to your network's needs. **Pay close attention to any notes or warnings associated with the settings.** To modify the templates:

- ❑ Within the MMC, double-click on the **Security Templates** node in the left pane
- ❑ Double-click the default configuration file directory (%Systemroot%\Security\Templates). A list of available configuration files is revealed.



NOTE: Template files from other directories may be loaded by right-clicking on Security Templates and choosing the New Template Search Path option.

- ❑ Double-click on a specific configuration file
- ❑ Double-click on a specific security area
- ❑ Double click on a security object in the right pane
- ❑ Customize the security setting for your environment
- ❑ To save the customized configuration file under a new file name (to avoid writing over the provided templates), right-click on the file in the left pane and select **Save As**, specifying a new name for the modified template
- ❑ Several security settings are recommended, but not defined in the templates because they are environment specific. You will have to decide on the values for the configurations. Among these settings are the following security options presented in Chapter 4:
 - Message text for users attempting to log on
 - Message title for users attempting to log on
 - Rename Administrator account
 - Rename Guest account
- ❑ Once the templates have been customized to your network environment and saved, apply the templates. If the template will be applied locally, see Chapter 10 for information on configuration options via the Security Configuration and Analysis snap-in or the `secedit.exe` command line tool. If the template will be imported into a Group Policy Object, please refer to the *Guide to Securing Microsoft Windows 2000 Group Policy*.

Undoing Security Changes

If problems arise after applying the security templates to a system, troubleshooting may be difficult if many settings were applied at once. First and foremost, try the settings out in a test environment before applying to an operational network. Also try configuring one section of the templates at a time via the command line `secedit.exe` tool (described later) or by isolating specific sections in a separate inf file. This method will allow you to apply one part of the templates (e.g. Account Policy or File System) and then test the system for problems before moving onto the next section.

The only sure-fire way to restore a system to its original configuration is via a backup. The `setup security.inf` file (mentioned earlier in this chapter) can be used to reset most settings to their default (out-of-the-box) values. However, any settings specified as “Not Defined” in the default template will not change the values configured by the NSA templates.

Modifying Account Policy Settings with Security Templates

A key component of controlling the security in a Windows 2000 domain is the proper setting of account policies. Depending on the type of system (e.g. domain controller, workstation, member server), account policy configuration will impact the network differently. **In Windows 2000 domains, account policy is set and enforced in the domain's Group Policy. Attempts to configure domain account policies in other GPOs are ignored. Configuring account policies directly on workstations and member servers only impacts the local password or lockout policy on the machine.** To ensure a consistent password and lockout policy throughout the entire domain for both local and domain logons, the same policy should be set on the domain controllers (via the domain GPO), member servers and workstations. See the *Guide to Securing Microsoft Windows 2000 Group Policy* for more information on importing security templates into the appropriate containers.

To view account policy settings of a security template double-click the following in the MMC:

- ❑ Security Templates
- ❑ Default configuration file directory (%SystemRoot%\Security\Templates)
- ❑ Specific configuration file
- ❑ Account Policies



NOTE: After making any modifications to the configuration files make sure the changes are saved, and then test the changes before installing them on an operational network.

Password Policy

Before making modifications to the **Account Policy** dialog box, review your organization's written password security policy. The settings made in the **Account Policy** dialog box should comply with the written password policy. Users should read and sign statements acknowledging compliance with the organizational computer policy.

Recommendations for a password policy include:


- ❑ Users should never write down passwords
- ❑ Passwords should be difficult to guess and include uppercase, lowercase, special (e.g., punctuation and extended character set), and numeric characters

- ❑ Users should not transmit clear-text passwords using any form of electronic communications.

To modify the password policy settings via the Security Templates snap-in, double-click the following path:

Account Policies → **Password Policy** → specific option to view or edit current settings

Table 3 lists the recommended password policy settings and **Figure 2** shows the password policy as it appears in the MMC.

Password Policy Options	Recommended Settings
<p><u>Enforce password history</u> Prevents users from toggling among their favorite passwords and reduces the chance that a hacker/password cracker will discover passwords. If this option is set to 0, users can revert immediately back to a password that they previously used. Allowable values range from 0 (do not keep password history) to 24 passwords remembered.</p>	24 Passwords
<p><u>Maximum Password Age</u> The period of time that a user is allowed to have a password before being required to change it. Allowable values include 0 (password never expires) or between 1 and 999 days. The maximum password age may be set to less than 90 days in more secure environments.</p>	90 days
<p><u>Minimum Password Age</u> The minimum password age setting specifies how long a user must wait after changing a password before changing it again. By default, users can change their passwords at any time. Therefore, a user could change their password, then immediately change it back to what it was before. Allowable values are 0 (password can be changed immediately) or between 1 and 998 days.</p>	1 Day
<p><u>Minimum Password Length</u> Blank passwords and shorter-length passwords are easily guessed by password cracking tools. To lessen the chances of a password being cracked, passwords should be longer in length. Allowable values for this option are 0 (no password required) or between 1 and 14 characters.</p> <p> NOTE: In actuality, Windows 2000 supports passwords up to 127 characters long. However, the security templates interface will not allow setting of minimum password length to be greater than 14. Also, if a network contains Windows 9x computers, the maximum password length cannot exceed 14 characters.</p> <p>NOTE: It is recommended that privileged users (such as administrators) have passwords longer than 12 characters if possible.</p>	12 Characters


Password Policy Options	Recommended Settings
<p><u>Passwords must meet complexity requirements</u> Enforces strong password requirements for all users by use of a dynamic link library called <code>passfilt.dll</code>. Stronger passwords provide some measure of defense against password guessing and dictionary attacks launched by outside intruders. Passwords must contain characters from 3 of 4 classes: upper case letters, lower case letters, numbers, and special characters (e.g., punctuation marks). Also, passwords cannot be the same as the user's logon name.</p> <p>Complexity requirements will take effect the next time a user changes his password. Already-existing passwords will not be affected.</p> <p> NOTE: NSA provides an enhanced password complexity filter, ENPASFLT.DLL (provided on the companion CD), that can be used in place of the Microsoft-provided PASSFLT.DLL. This password filter enforces passwords of at least 8 characters in length containing all 4 classes of characters. Additionally, the use of the user logon name or full name as a password is not permitted. See the ENPASFLT documentation for installation procedures. If using ENPASFLT instead of PASSFLT, this template option should be set to Disabled to avoid conflicts between the two DLLs.</p>	<p>Enabled</p>
<p><u>Store password using reversible encryption for all users in the domain</u> Determines whether user passwords will be stored using a two-way hash. This option exists to provide password information to certain applications. However, storing passwords with reversible encryption is similar to storing clear-text passwords and should NOT be permitted.</p>	<p>Disabled</p>

Table 3 Password Policy Options

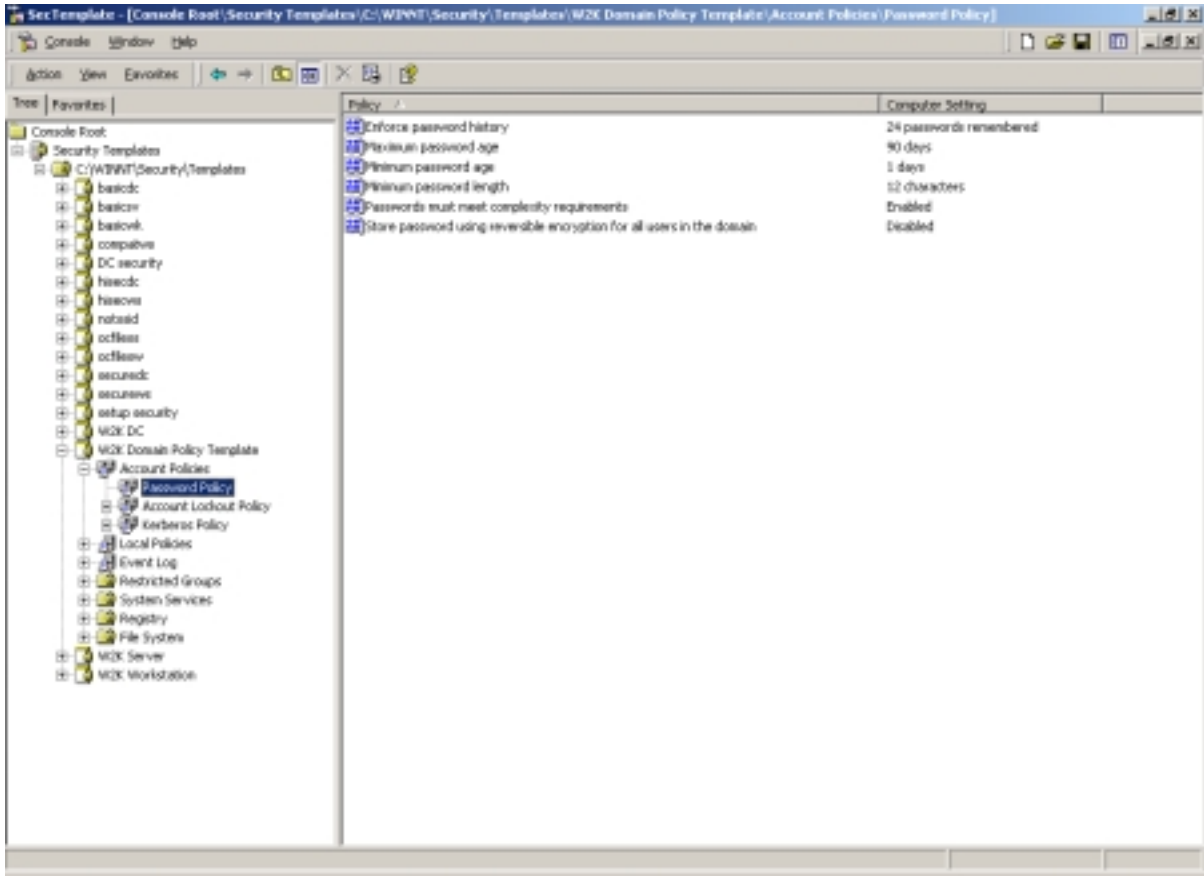


Figure 2 Password Policy Recommended Settings

Account Lockout Policy

Account lockout is recommended after three invalid logon attempts. This setting will slow down a dictionary attack in which thousands of well-known passwords are tried. If the account is locked out after each invalid attempt to logon, the hacker must wait until the account is enabled again. If an account is locked out, the administrator can reset it using **Active Directory Users and Computers** for domain accounts or **Computer Management** for local accounts instead of waiting the allotted lockout duration.

To modify the account lockout policy settings via the Security Templates snap-in, double-click the following path:

Account Policies → **Account Lockout Policy** → specific option to view or edit settings

Table 4 lists the recommended account lockout policy settings.



Account Lockout Policy Options	Recommended Settings
<p><u>Account lockout duration</u> Sets the number of minutes an account will be locked out. Allowable values are 0 (account is lockout out until administrator unlocks it) or between 1 and 99999 minutes.</p> <p> WARNING: Setting this value to 0 (until administrator unlocks) may allow a potential denial of service attack. It is important to note that the built-in Administrator account cannot be locked out.</p>	15 minutes
<p><u>Account lockout threshold</u> Prevents brute-force password cracking/guessing attacks on the system. This option specifies the number of invalid logon attempts that can be made before an account is locked out. Allowable values range from 0 (account will not lockout) to 999 attempts.</p> <p> NOTE: Failed logons on machines that have been locked via CTRL-ALT-DEL or a password-protected screen saver do not count as failed attempts.</p>	3 Invalid logon attempts
<p><u>Reset account lockout counter after</u> Sets the number of minutes until the invalid logon count is reset. Allowable values range from 1 to 99999 minutes.</p>	15 minutes

Table 4 Account Lockout Options

Kerberos Policy

Kerberos is the default authentication method used in Windows 2000 Active Directory. Since Active Directory is necessary for Kerberos authentication, the Kerberos policy only has significance for the Windows 2000 domain Group Policy Object. Therefore, for the standalone workstation and server configurations that this document addresses, the Kerberos policies will not be defined.

To modify Kerberos settings via the Security Templates snap-in, double-click the following path:

Account Policies → Kerberos Policy → specific option to view or edit settings

Table 5 lists the Kerberos Policy options that should be applied at the **domain group policy level (in the provided Domain Policy.inf template)**.


Kerberos Policy Options	Recommended Settings
<p><u>Enforce user logon restrictions</u> Forces the Key Distribution Center (KDC) to check if a user requesting a service ticket has either the “Log on locally” (for local machine service access) or “Access this computer from the network” user right on the machine running the requested service. If the user does not have the appropriate user right, a service ticket will not be issued. Enabling this option provides increased security, but may slow network access to servers.</p>	Enabled
<p><u>Maximum lifetime for service ticket</u> Determines the number of minutes a Kerberos service ticket is valid. Values must be between 10 minutes and the setting for “Maximum lifetime for user ticket.” This value is set to 600 minutes in the default domain GPO.</p> <p> NOTE: Expired service tickets are only renewed when making a new connection to a server. If a ticket expires during an established session, the session is not interrupted.</p>	600 minutes
<p><u>Maximum lifetime for user ticket</u> Determines the number of hours a Kerberos ticket-granting ticket (TGT) is valid. Upon expiration of the TGT, a new one must be obtained or the old one renewed. This value is set to 10 hours in the default domain GPO.</p>	10 hours
<p><u>Maximum lifetime for user ticket removal</u> Sets the maximum number of days that a user's TGT can be renewed. This value is set to 7 days in the default domain GPO.</p>	7 days
<p><u>Maximum tolerance for computer clock synchronization</u> Sets the maximum number of minutes by which the KDC and client machine's clocks can differ. Kerberos makes use of time stamps to determine authenticity of requests and aid in preventing replay attacks. Therefore, it is important that KDC and client clocks remain synchronized as closely as possible. This value is set to 5 minutes in the default domain GPO.</p>	5 minutes

Table 5 Kerberos Policy Options

Modifying Local Policy Settings with Security Templates

The Local Policies section in the Security Templates snap-in includes Audit Policy, User Rights Assignment, and Security Options. To view local policy settings of a security template, double-click the following in the MMC:

- ❑ Security Templates
- ❑ Default configuration file directory (%SystemRoot%\Security\Templates)
- ❑ Specific configuration file
- ❑ Local Policies



NOTE: After making any modifications to the configuration files make sure the changes are saved and then test the changes before installing them on an operational network.

Auditing Policy

Auditing is critical to maintaining the security of the domain. On Windows 2000 systems, auditing is not enabled by default. Each Windows 2000 system includes auditing capabilities that collect information about individual system usage. The logs collect information on applications, system, and security events. Each event that is audited in an audit policy is written to the security event log, which can be viewed with the Event Viewer.



WARNING: Auditing can consume a large amount of processor time and disk space. It is highly recommended that administrators check, save, and clear audit logs daily/weekly to reduce the chances of system degradation or save audit logs to a separate machine. It is also recommended that logs be kept on a separate partition.

To modify the audit policy settings via the Security Templates snap-in, double-click the following path:

Local Policies → **Audit Policy** → specific option to view or edit

Table 6 lists recommended Audit Policy Settings for domain controllers, member servers, and workstations.



NOTE: Auditing is important on all domain machines, workstations and servers alike. However, if operational constraints do not make auditing on all machines possible, at a minimum, auditing should be enabled on all servers.



Audit Policy Options	Recommended Settings
<p><u>Audit account logon events</u> Tracks user logon events on other computers in which the local computer was used to authenticate the account.</p>	Success, Failure
<p><u>Audit account management</u> Tracks changes to the Security Account database (i.e., when accounts are created, changed, or deleted).</p>	Success, Failure
<p><u>Audit directory service access</u> Audits users' access to Active Directory objects that have their system access control list (SACL) defined. This option is similar to Audit Object Access except that it only applies to Active Directory objects and not files and registry objects. Since this option only applies to Active Directory, it has no meaning on workstations and member servers.</p>	No auditing (workstations and member servers) Failure (domain controllers)
<p><u>Audit logon events</u> Tracks users who have logged on or off, or made a network connection. Also records the type of logon requested (interactive, network, or service). This option differs from "Audit Account Logon Events" in that it records where the logon occurred versus where the logged-on account lives. Track failures to record possible unauthorized attempts to break into the system.</p> <p> NOTE: The auditing of successful and failed logon events generates a large amount of data. Network, service, and user logons are all recorded. Auditing of success events is important for tracking users logged on during potential attacks. However, if log space is at a premium, at a minimum, failure of logon events should be recorded.</p>	Success, Failure
<p><u>Audit object access</u> Tracks unsuccessful attempts to access objects (e.g., directories, files, printers). Individual object auditing is not automatic and must be enabled in the object's properties.</p>	Failure
<p><u>Audit policy change</u> Tracks changes in security policy, such as assignment of privileges or changes in the audit policy.</p>	Success, Failure
<p><u>Audit privilege use</u> Tracks unsuccessful attempts to use privileges. Privileges indicate rights assigned to Administrators or other power users. Tracks all user rights except Bypass Traverse Checking, Debug Programs, Create a Token Object, Replace Process Level Token, Generate Security Audits, Back Up Files and Directories, and Restore Files and Directories.</p> <p> NOTE: The Audit use of all user rights including Backup and Restore setting under Security Options will audit those user rights excluded here.</p>	Failure
<p><u>Audit process tracking</u> Detailed tracking information for events such as program activation and exits. This option is useful to record specific events in detail if your system is believed to be under attack.</p>	No Auditing
<p><u>Audit system events</u> Tracks events that affect the entire system or the Audit log. Records events such as restart or shutdown.</p>	Success, Failure

Table 6 Audit Policy Options

User Rights Assignment

User rights are allowable actions that can be assigned to users or groups to supplement built-in abilities. Careful allocation of user rights can significantly strengthen the security of a Windows 2000 system. The recommended user rights are listed and described in **Figure 3** and **Table 7**. Advanced user rights are assigned to Administrators or other trusted users who are allowed to run administrative utilities, install service packs, create printers, and install device drivers. If resources are available, it is recommended assigning these duties to several trusted users. Administrators are not explicitly listed for rights they implicitly have.



NOTE: Based on network policies, some users/groups may need to be added or deleted from the recommended user rights

To modify the user rights settings via the Security Templates snap-in, double-click the following path:

- ❑ **Local Policies** → **User Rights Assignment**
- ❑ Right-click on the desired Attribute in the right frame
- ❑ **Select Security**
- ❑ To add a user or group, **Add** → **Select user or group** → **Add** → **OK** → **OK**
- ❑ To remove a user or group, select user or group → **Remove** → **OK**

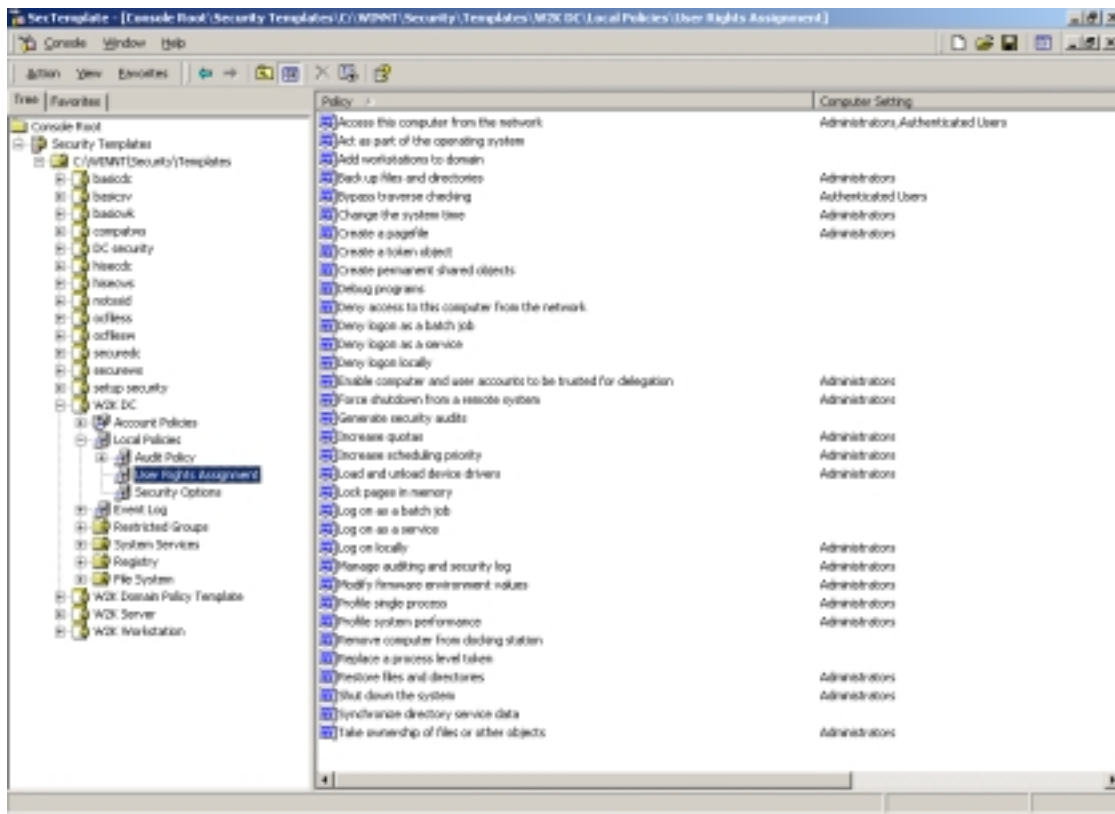
















Figure 3 Recommended User Rights

User Rights	Windows 2000 Workstations	Windows 2000 Domain Controllers and Member Servers
<p><u>Access this computer from network</u> Allows a user to connect over the network to the computer.</p>  <p>NOTE: If the system is an IIS 5.0 server, whenever the IIS 5.0 service is stopped and restarted, or the machine is rebooted, the IUSR_<machine_name> and IWAM_<machine_name> will automatically be assigned this right (although it is not necessary). If the security template is applied via Group Policy, these accounts will be removed from this right when the policy is refreshed. See NSA's "Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0" for information on a workaround for this issue.</p>	Administrators Users	Administrators Authenticated Users (DCs only) Users (Member Servers only)
<p><u>Act as part of the operating system</u> Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.</p>	(No one)	(No one)
<p><u>Add workstations to domain</u> Allows a user to add workstations to a particular domain. This right is meaningful only on domain controllers. The Administrators and Account Operators groups have the ability to add workstations to a domain and do not have to be explicitly given this right.</p>  <p>NOTE: By default, Authenticated Users are given this right on Domain Controllers. Allowing users to add their own machines to a domain could pose security risks. Therefore, it is recommended that the Authenticated Users group not be granted this right.</p>	(No one)	(No one)
<p><u>Back up files and directories</u> Allows a user to back up files and directories. This right supersedes file and directory permissions.</p>  <p>NOTE: If the network makes use of the Backup Operators or similar group, also assign this right to that group.</p>	Administrators	Administrators
<p><u>Bypass traverse checking</u> Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories.</p>	Users	Authenticated Users (DCs only) Users (Member Servers only)

User Rights	Windows 2000 Workstations	Windows 2000 Domain Controllers and Member Servers
<p><u>Change the system time</u> Allows a user to set the time for the internal clock of the computer.</p>	Administrators	Administrators
<p><u>Create a pagefile</u> Allows a user to create new pagefiles for virtual memory swapping and change the size of a pagefile.</p>	Administrators	Administrators
<p><u>Create a token object</u> Allows a process to create access tokens that can be used to access local resources. Only the Local Security Authority should be allowed to create this object.</p>	(No one)	(No one)
<p><u>Create permanent shared objects</u> Allows a user to create special permanent directory objects, such as \\Device, that are used within the Windows 2000 object manager.</p>	(No one)	(No one)
<p><u>Debug programs</u> Allows a user to debug various low-level objects such as threads.</p> <p> NOTE: Software developers working on the system may need this right. Assign the right to developer users/groups only when necessary.</p>	(No one)	(No one)
<p><u>Deny access to this computer from the network</u> Prevents specific users and/or groups from accessing the computer via the network. This setting supercedes the "Access this computer from the network" setting if an account is subject to both policies.</p>	(No one)	(No one)
<p><u>Deny logon as a batch job</u> Prevents specific users and/or groups from logging on as a batch job. This setting supercedes the "Logon as a batch job" setting if an account is subject to both policies.</p>	(No one)	(No one)
<p><u>Deny logon as a service</u> Prevents specific service accounts from registering a process as a service. This setting supercedes the "Log on as a service" setting if an account is subject to both policies.</p>	(No one)	(No one)
<p><u>Deny logon locally</u> Prevents specific users and/or groups from logging on directly at the computer. This setting supercedes the "Log on locally" setting if an account is subject to both policies.</p>	(No one)	(No one)
<p><u>Enable computer and user accounts to be trusted for delegation</u> Allows a user to set the "Trusted for Delegation" setting on a user or computer object. The user granted this right must have write access to the account control flags on the computer or user object.</p>	(No one)	Administrators (domain controllers) (No one) (member servers)

User Rights	Windows 2000 Workstations	Windows 2000 Domain Controllers and Member Servers
<u>Force shutdown from a remote system</u> Allows a user to shutdown a Windows 2000 system remotely over a network.	Administrators	Administrators
<u>Generate security audits</u> Allows a process to generate security audit log entries.	(No one)	(No one)
<u>Increase quotas</u> Allows a user to increase the processor quota assigned to a process.	Administrators	Administrators
<u>Increase scheduling priority</u> Allows a user to boost the execution priority of a process. This can be performed via the Task Manager user interface.	Administrators	Administrators
<u>Load and unload device drivers</u> Allows a user to install and remove device drivers. This right is necessary for Plug and Play device driver installation.	Administrators	Administrators
<u>Lock pages in memory</u> Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys.  NOTE: This right is obsolete in this version of Windows 2000.	(No one)	(No one)
<u>Log on as a batch job</u> Allows a user to log on by means of a batch-queue facility. In Windows 2000, the Task Scheduler automatically grants this right as necessary.  NOTE: If the system is an IIS 5.0 server, whenever the IIS 5.0 service is stopped and restarted, or the machine is rebooted, the IUSR_<machine_name> and IWAM_<machine_name> will automatically be assigned this right (although it is not necessary). If the security template is applied via Group Policy, these accounts will be removed from this right when the policy is refreshed. See NSA's "Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0" for information on a workaround for this issue.	(No one)	(No one)

User Rights	Windows 2000 Workstations	Windows 2000 Domain Controllers and Member Servers
<p>Log on as a service Allows a process to register with the system as a service.</p>  <p>NOTE: Some applications such as Microsoft Exchange require a service account, which should have this right. Review the users/groups assigned this right on the system PRIOR to applying the security templates in order to determine which assignments are necessary.</p>  <p>WARNING: The provided template files will remove all users/groups from this right unless you modify the setting.</p>	(No one)	(No one)
<p>Log on locally Allows a user to log on at a system's console. To allow a user to log on locally at a domain controller, this right must be enabled in the Domain Controller group policy object.</p>  <p>NOTE: If the system is an IIS 5.0 Server, the IUSR_<machine_name> and IWAM_<machine_name> accounts (or whatever account has been designated as the anonymous web user) must be assigned this right.</p>  <p>NOTE: If the network makes use of the Backup Operators or similar group, also assign this right to that group.</p>	Administrators Users	Administrators

User Rights	Windows 2000 Workstations	Windows 2000 Domain Controllers and Member Servers
<p><u>Manage auditing and security log</u> Allows a user to view and clear the security log and specify what types of object access (such as file access) are to be audited. Users with this right can enable auditing for a specific object by editing the auditing options in the security tab of the object's Properties dialog box. Members of the Administrators group always have the ability to view and clear the security log.</p> <p> NOTE: This right does not allow a user to enable file and object access auditing in general. Object auditing is enabled by setting the "Audit object access" item under Audit Policies.</p> <p> WARNING: If running Exchange 2000 on the network, the Exchange Enterprise Servers group must be assigned this user right on domain controllers.</p>	Administrators	Administrators
<p><u>Modify firmware environment variables</u> Allows a user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.</p>	Administrators	Administrators
<p><u>Profile single process</u> Allows a user to perform profiling (performance sampling) on a process.</p> <p> NOTE: Software developers working on the system may need this right. Assign the right to developer users/groups only when necessary.</p>	Administrators	Administrators
<p><u>Profile system performance</u> Allows a user to perform profiling (performance sampling) on the system.</p>	Administrators	Administrators
<p><u>Remove computer from docking station</u> Allows a user to undock a laptop from a docking station.</p>	Administrators Users	(No one)
<p><u>Replace a process-level token</u> Allows a user to modify a process's security access token. This is a powerful right used only by the system.</p>	(No one)	(No one)
<p><u>Restore files and directories</u> Allows a user to restore backed-up files and directories. This right supercedes file and directory permissions.</p> <p> NOTE: If the network makes use of the group to Restore backups, also assign this right to that group.</p>	Administrators	Administrators

User Rights	Windows 2000 Workstations	Windows 2000 Domain Controllers and Member Servers
Shut down the system Allows a user to shut down Windows 2000.	Administrators Users	Administrators
Synchronize directory service data This right has no effect in the initial release of Windows 2000.	(No one)	(No one)
Take ownership of files or other objects Allows a user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Administrators	Administrators



Table 7 User Rights Options

Security Options


The Security Templates Security Option section contains many security parameters that can be easily configured by adding or changing registry key values. **Table 8** lists the recommended settings. Customized security options added to the NSA templates are shaded.







WARNING: Use the Security Configuration Tool Set when configuring Security Options. Using the registry editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows 2000.



Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Additional restrictions for anonymous connections</u> Places restrictions on anonymous users. The options are:</p> <p>None. Rely on default permissions. Default permissions allow anonymous users to enumerate the names of domain accounts and network shares and have the same amount of access to resources as the “Everyone” group. The registry value for this option is 0.</p> <p>Do not allow enumeration of SAM accounts and shares. Replaces the “Everyone” group with “Authenticated Users” in resource security permissions. The registry value for this option is 1.</p> <p>No access without explicit anonymous permissions. Requires that “Anonymous” be given explicit permissions to access resources by removing the “Everyone” and “Network” groups from the anonymous user token. The registry value for this option is 2.</p> <p> WARNING: Setting the Restrict Anonymous key value = 2 could result in undesired effects when setting up trust relationships, authenticating in a mixed environment, or running certain services or applications. Please see KB Article Q246261 http://support.microsoft.com/support/kb/articles/Q246/2/61.asp for further information on setting this key. If setting the key = 2 is not feasible, it is recommended that the value be set to “Do not allow enumeration of SAM accounts and shares” (value = 1).</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous = 2</p>	<p>No access without explicit anonymous permissions</p>	<p>No access without explicit anonymous permissions</p>
<p><u>Allow Automatic Administrator Logon</u> Allows a system to automatically logon as administrator when the machine is started. By default, this setting is disabled.</p> <p> NOTE: If this option was at one time enabled, a DefaultPassword registry value may also exist in the same registry key. This value contains the administrator password in clear text and should be deleted.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon = 0</p>	<p>Disabled</p>	<p>Disabled</p>

Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Allow Server Operators to schedule tasks (domain controllers only)</u> Allows Server Operators to use the Schedule Service (AT command) to schedule a task to automatically run. By default, Administrators are able to schedule tasks. Options are:</p> <p>Disabled Only allow Administrators to schedule tasks</p> <p>Enabled Allow Administrators and Server Operators to schedule tasks</p> <p>HKLM\System\CurrentControlSet\Services\Schedule = 0</p>	Not defined	Disabled
<p><u>Allow system to be shut down without having to log on</u> On Windows 2000 Professional, a Shutdown button is available in the Logon dialog box. When this option is disabled, users must be able to log on to the system and have the "Shut down the system" user right in order to shutdown the computer. By default, this option is disabled on servers.</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon = 0</p>	Disabled	Disabled
<p><u>Allowed to eject removable NTFS media</u> By default, only Administrators are allowed to eject removable NTFS media. This setting allows for the following options:</p> <p>Administrators Administrators and Power Users Administrators and Interactive Users</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\winlogon\AllocateDASD = 0</p>	Administrators	Administrators
<p><u>Amount of idle time required before disconnecting session</u> Sets the amount of continuous idle time in a Server Message Block (SMB) session before a session is disconnected. If client activity resumes after a disconnect, the session is automatically reestablished. Allowable values are between 0 (Do not disconnect clients) and 99,999 minutes</p> <p>HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect = 15</p>	30 minutes	30 minutes


Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Audit the access of global system objects</u> When enabled, this option will assign a default SACL to system objects such as mutexes, events, semaphores, and DOS devices. In order for these system objects to be audited, Audit Object Access must be enabled under auditing.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\AuditBaseObjects = 1</p>	Enabled	Enabled
<p><u>Audit use of Backup and Restore privilege</u> Enables auditing of all user rights in conjunction with Audit Privilege Use auditing being enabled. If this option is disabled, the Backup and Restore rights will not be audited even if Audit Privilege Use is enabled.</p> <p> NOTE: Since there could be many Backup and Restore events generated during the course of system backups, this option may be disabled if there are concerns about the growth of the security log.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing = 1</p>	Enabled	Enabled
<p><u>Automatically log off users when logon time expires</u> Causes client SMB sessions to be forcibly disconnected when a user's logon hours expire. This setting affects all machines in a domain and should be set at the domain-level group policy.</p>	Not Defined	Not defined
<p><u>Automatically log off users when logon time expires (local)</u> Causes client SMB sessions to be forcibly disconnected when a user's logon hours expire. This policy affects the local machine on which it is applied.</p> <p>HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogoff = 1</p>	Enabled	Enabled
<p><u>Clear virtual memory pagefile when system shuts down</u> Wipes the system pagefile clean when Windows 2000 shuts down, ensuring that sensitive information that may be in the pagefile is not available to malicious users. When this option is enabled, it also causes the hibernation file (<i>hiberfil.sys</i>) to be cleared when hibernation is disabled on a laptop system.</p> <p>HKLM\CurrentControlSet\Control\SessionManager\MemoryManagement\ClearPageFileAtShutdown = 1</p>	Enabled	Enabled



Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Digitally sign client communication (always)</u> Forces an SMB client to always digitally sign SMB communications. Digital signatures provide mutual authentication during SMB exchanges, preventing “man-in-the-middle” and active message attacks.</p> <p> NOTE: To use SMB digital signing, this option must be enabled on both the SMB client and server.</p> <p>HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature = 0</p>	Disabled	Disabled
<p><u>Digitally sign client communication (when possible)</u> Enables an SMB client to perform digital packet signing when communicating with an SMB server that also supports packet signing. Digital signatures provide mutual authentication during SMB exchanges, preventing “man-in-the-middle” and active message attacks.</p> <p>HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature = 1</p>	Enabled	Enabled
<p><u>Digitally sign server communication (always)</u> Forces an SMB server to always digitally sign SMB communications. Digital signatures provide mutual authentication during SMB exchanges, preventing “man-in-the-middle” and active message attacks.</p> <p> NOTE: To use SMB digital signing, this option must be enabled on both the SMB client and server.</p> <p>HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\RequireSecuritySignature = 0</p>	Disabled	Disabled
<p><u>Digitally sign server communication (when possible)</u> Enables an SMB server to perform digital packet signing when communicating with an SMB client that also supports packet signing. Digital signatures provide mutual authentication during SMB exchanges, preventing “man-in-the-middle” and active message attacks.</p> <p>HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\EnableSecuritySignature = 1</p>	Enabled	Enabled






Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Disable CTRL+ALT+DEL requirement for logon</u> If this option is enabled, a user is not required to press CTRL+ALT+DEL to log on. CTRL+ALT+DEL establishes a trusted path to the operating system when entering a username/password pair; therefore, disabling it poses a security risk to the users' logon credentials. By default, this option is disabled on systems in a domain and enabled on stand-alone workstations.</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD = 0</p>	Disabled	Disabled
<p><u>Disable Media Autoplay</u> Autoplay reads from a drive as soon as it is inserted. By default, Windows 2000 autoruns any CDROM that is placed in the drive. This could allow executable content to be run without any access to the command prompt. Autoplay on floppy disks and network drives is disabled by default. The options for this setting are:</p> <p>CDROM drives Disables autorun on CDROMs. Registry value = 0x00000095</p> <p>All drives Disables autorun on all media. Registry value = 0x000000FF</p> <p> NOTE: This option can also be set in Group Policy via Computer Configuration\Administrative Templates\System\Disable Autoplay. Because it is considered a security-related item, it has been added to the security templates here.</p> <p> NOTE: CDROM autoplay/autorun can also be disabled by setting the registry value HKLM\System\CurrentControlSet\Services\Cdrom\Autorun = 0</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun = 0x000000FF</p>	All Drives	All Drives


Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Do not display last user name in logon screen</u> By default, Windows 2000 displays the name of the last user to log on the computer in the Logon dialog box. To prevent malicious users from gaining information about user names on the system, disallow display of the last logon. This is especially important if a generally accessible computer is being used for system administration.</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUsername= 1</p>	Enabled	Enabled
<p><u>LAN Manager authentication level</u> This parameter specifies the type of challenge/response authentication to be used for network logons with non-Windows 2000 Windows clients. LanManager authentication (LM) is the most insecure method, allowing encrypted passwords to be easily sniffed off the network and cracked. NT LanManager (NTLM) is somewhat more secure. NTLMv2 is a more robust version of NTLM and is available with Windows NT 4.0 Service Pack 4 and higher as well as Windows 95/98 with Directory Services Client. The following options are available:</p> <p>Send LM & NTLM responses - Registry value = 0.</p> <p>Send LM & NTLM – use NTLMv2 session security if negotiated - Registry value = 1.</p> <p>Send NTLM response only - Registry value = 2.</p> <p>Send NTLMv2 response only - Registry value = 3.</p> <p>Send NTLMv2 response only\refuse LM - Registry value = 4.</p> <p>Send NTLMv2 response only\refuse LM and NTLM - Registry value = 5.</p> <p> WARNING: Some Windows 2000 processes, such as Cluster Services, use NTLM to authenticate. Use of the recommended setting may cause these services to fail. For more information on NTLM and Cluster Services, see KB Article Q272129 http://support.microsoft.com/support/kb/articles/Q272/1/29.ASP</p> <p> WARNING: Setting this value higher than 2 on a Windows 2000 system could prevent some connectivity to systems that support only LM authentication (Windows 95®/98® and Windows for Workgroups®) or only NTLM (Windows NT 4.0 prior to</p>	Send NTLMv2 response only\refuse LM & NTLM	Send NTLMv2 response only\refuse LM & NTLM



Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p>Service Pack 4). The Active Directory Services client may be installed on Windows 9x machines to allow for NTLMv2 security.</p> <p>WARNING: If adding a Windows 2000 machine to a Windows NT 4.0 domain, this value may need to be set to 4 "Send NTLMv2 response only/refuse LM" or lower on the Windows NT 4.0 domain controller.</p> <p>WARNING: Access to an Exchange server via IMAP and POP may not work from either Outlook 2000 or Outlook Express if this setting = 5. Instead, set this option to "Send NTLMv2 response only/refuse LM," value = 4. Service Pack 2 fixes this problem.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel = 5</p>		



<p>Security Attribute</p>	<p>Recommended Security Setting For Workstations and Member Servers</p>	<p>Recommended Security Setting For Domain Controllers</p>
<p><u>Message text for users attempting to log on</u> It is recommended that systems display a warning message before logon, indicating the private nature of the system. Many organizations use this message box to display a warning message that notifies potential users that their use can be monitored and they can be held legally liable if they attempt to use the computer without proper authorization. The absence of such a notice could be construed as an invitation, without restriction, to enter and browse the system.</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText = "Text you want displayed"</p>	<p><Configure locally - see Appendix for sample></p>	<p><Configure locally - see Appendix for sample></p>
<p><u>Message title for users attempting to log on</u> In conjunction with the Logon Text, it is recommended that systems display a warning message title before logon, indicating the private nature of the system.</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption = "Text you want displayed on title bar"</p>	<p><Configure locally - see Appendix for sample></p>	<p><Configure locally - see Appendix for sample></p>
<p><u>Number of previous logons to cache (in case domain controller is not available)</u> The default Windows 2000 configuration caches the last 10 logon credentials for users who log on interactively to a system. This feature is provided for system availability reasons such as the user's machine being disconnected from the network or domain controllers not being available.</p> <p> WARNING: By setting this value to 0, users will NOT be able to log on to the domain unless connected to the network. This may have ramifications for mobile laptop users.</p> <p>WARNING: Not having cached logons may slow down the authentication process.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount = 0</p>	<p>0 logons</p>	<p>0 logons</p>
<p><u>Prevent system maintenance of computer account password</u> By default, computer account passwords are changed every seven days. Enabling this option prevents machines from requesting a weekly password change.</p> <p>HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange = 0</p>	<p>Disabled</p>	<p>Disabled</p>



Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Prevent users from installing printer drivers</u> Prevents members of the users group from adding printer drivers on the local machine.</p>  <p>NOTE: Users can still connect to Network Print shares to which they have permissions.</p>  <p>WARNING: After enabling this option, users will not be able to add printers that have not been previously installed.</p> <p>HKLM\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers = 1</p>	Enabled	Enabled
<p><u>Prompt user to change password before expiration</u> Sets how far in advance users are warned that their passwords will expire.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon>PasswordExpiryWarning = 14</p>	14 days	14 days
<p><u>Recovery Console: Allow automatic administrative logon</u> If this option is enabled, the Recovery Console will not prompt for an administrator password and will automatically log on to the system.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel = 0</p>	Disabled	Disabled
<p><u>Recovery Console: Allow floppy copy and access to all drives and folders</u> Enables the Recovery Console SET command, which allows setting of console environment variables such as AllowWildCards, AllowAllPaths, AllowRemovableMedia, and NoCopyPrompt.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand = 0</p>	Disabled	Disabled

Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Rename administrator account</u> The Administrator account is created by default when installing Windows 2000. Associating the Administrator SID with a different name may thwart a potential hacker who is targeting the built-in Administrator account. When choosing another name for this account, avoid obvious names such as “admin” or “root,” which reveal the use of the account. After renaming the account, it is recommended that the default account description be changed or deleted.</p> <p> NOTE: The provided templates do not define this setting due to the environment specificity of this option. However, renaming this account is a recommended setting.</p> <p> NOTE: Even after renaming the built-in domain administrator account, it will appear as Administrator in Active Directory Users and Computers. However, double-clicking on the account, and clicking the Account tab in the Properties window will show that the logon name has indeed been changed.</p> <p> WARNING: After configuring this option via Group Policy, event ID 1000 and 1202 may appear in the Application event log every five minutes. See KB article Q260715 http://support.microsoft.com/support/kb/articles/Q260/7/15.asp for more information.</p>	<Configure Locally>	<Configure Locally>
<p><u>Rename guest Account</u> The Guest account is created by default when installing Windows 2000, but is disabled. Associating the Guest SID with a different name may thwart a potential hacker who is targeting the built-in Guest account. After renaming the account, it is recommended that the default account description be changed or deleted.</p> <p> NOTE: The provided templates do not define this setting due to the environment specificity of this option. However, renaming this account is a recommended setting.</p> <p> NOTE: Even after renaming the built-in domain guest account, it will appear as Guest in Active Directory Users and Computers. However, double-clicking on the account, and</p>	<Configure Locally>	<Configure Locally>

Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p>clicking the Account tab in the Properties window will show that the logon name has indeed been changed.</p>		
<p><u>Restrict CD-ROM access to locally logged on user only</u> By default, Windows 2000 allows any program to access files on CD-ROM drives. In a highly secure, multi-user environment, it only allows interactive users to access these devices. When operating in this mode, the CD-ROM(s) are allocated to a user as part of the interactive logon process. These devices are automatically deallocated when the user logs off.</p> <p> WARNING: There exists a known bug when installing Office 2000 from a CD and having this option enabled. This error may appear as "Error 1311: Source file not found: E:\OFFICE1.CAB. Verify that the file exists and that you can access it." A similar error could occur with other software CD installations (e.g. Windows 2000 Resource Kit). Currently, the only solutions are as follows:</p> <ul style="list-style-type: none"> • Install the software from across the network <p style="text-align: center;">Or</p> • Copy the contents of the CD to the hard drive, then install <p style="text-align: center;">Or</p> • Temporarily disable this setting, install the software, then re-enable it. <p>For more information, refer to KB Article Q230895 http://support.microsoft.com/support/kb/articles/Q230/8/95.asp.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms = 1</p>	<p>Enabled</p>	<p>Enabled</p>
<p><u>Restrict floppy access to locally logged on user only</u> By default, Windows 2000 allows any program to access files on floppy drives. In a highly secure, multi-user environment, it only allows interactive users to access these devices. When operating in this mode, the floppy disks are allocated to a user as part of the interactive logon process. These devices are automatically deallocated when the user logs off.</p> <p>HKLM\Software\Microsoft\Windows NT\</p>	<p>Enabled</p>	<p>Enabled</p>

Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p>CurrentVersion\Winlogon\ AllocateFloppies = 1</p> <p><u>Secure channel: Digitally encrypt or sign secure channel data (always)</u> Forces a computer to always digitally encrypt or sign secure channel data. A secure channel is created between a system and its domain controller when the system boots. By default, communications sent via the secure channel are authenticated and sensitive information, such as passwords, is encrypted, but the channel is not integrity checked and not all information is encrypted. This option will encrypt or sign all data passing through the secure channel.</p> <p> NOTE: ALL domain controllers in ALL trusted domains must support digital encryption and signing if this option is enabled.</p> <p>HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignorSeal = 0</p>	<p>Disabled</p>	<p>Disabled</p>
<p><u>Secure channel: Digitally encrypt secure channel data (when possible)</u> Enables a computer to digitally encrypt secure channel data. See the explanation of secure channel communication in the previous option.</p> <p>If this option is enabled, all outgoing secure channel traffic should be encrypted.</p> <p>HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel = 1</p>	<p>Enabled</p>	<p>Enabled</p>
<p><u>Secure channel: Digitally sign secure channel data (when possible)</u> Enables a computer to digitally sign secure channel data. See the explanation of secure channel communication in the previous option.</p> <p>If this option is enabled, all outgoing secure channel traffic should be signed.</p> <p> NOTE: If Digitally encrypt secure channel data (when possible) is enabled, it will override any setting for this option and automatically enable it.</p> <p>HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel = 1</p>	<p>Enabled</p>	<p>Enabled</p>

Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Secure channel: Require strong (Windows 2000 or later) session key</u> Requires strong encryption keys for all outgoing secure channel communications.</p>  <p>NOTE: This option should be enabled only if ALL domain controllers in ALL trusted domains also support strong session keys.</p> <p>HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey = 0</p>	Disabled	Disabled
<p><u>Secure system partition (for RISC platforms only)</u> Restricts access of the RISC system partition (which is FAT) to administrators only when the operating system is running.</p>	Not defined	Not defined
<p><u>Send unencrypted password to connect to third-party SMB servers</u> Some non-Microsoft SMB servers only support unencrypted (plain text) password exchanges during authentication. Check with the vendor of the SMB server product to see if there is a way to support encrypted password authentication, or if there is a newer version of the product that adds this support.</p>  <p>WARNING: Enabling this will allow unencrypted (plain text) passwords to be sent across the network when authenticating to an SMB server that requests this option. This reduces the overall security of an environment and should only be done after careful consideration of the consequences of plain text passwords in your specific environment.</p> <p>HKLM\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword = 0</p>	Disabled	Disabled

Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
<p><u>Shut down system immediately if unable to log security audits</u> If events cannot be written to the security log, the system is halted immediately. If the system halts as a result of a full log, an administrator must log onto the system and clear the log.</p> <p> NOTE: Before clearing the security log, save the data to disk.</p> <p> WARNING: Enabling this option will disallow any connections to the system until the audit logs are cleared. Take caution when enabling this on critical systems. Also, enabling this option on a large number of workstations in the network may result in much overhead when the logs become full.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail = 1</p>	Enabled	Enabled
<p><u>Smart card removal behavior</u> Determines the action taken when a smart card for a logged-on user is removed from the smart card reader. Options are:</p> <p>No action</p> <p>Lock Workstation Users can remove their smart card, leave the area, then return to their same session at a later time.</p> <p>Force Logoff Users are automatically logged off when the card is removed.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption = 1</p>	Lock Workstation	Lock Workstation
<p><u>Strengthen default permissions of global system objects (e.g., Symbolic Links)</u> Strengthens the DACLs on the global list of shared system resources (such as DOS device names, mutexes, and semaphores) so that non-administrative users can read, but not modify shared objects they did not create.</p> <p>HKLM\Software\CurrentControlSet\Session Manager\ProtectionMode = 1</p>	Enabled	Enabled

Security Attribute	Recommended Security Setting For Workstations and Member Servers	Recommended Security Setting For Domain Controllers
Unsigned driver installation behavior Determines the action taken when a device driver that has not been certified for Windows 2000 attempts to load. Options are: Silently succeed Warn but allow installation Do not allow installation HKLM\Software\Microsoft\Driver Signing\Policy = 1	Warn but allow installation	Warn but allow installation
Unsigned non-driver installation behavior Determines the action taken when non-device driver software that has not been certified for Windows 2000 attempts to load. Options are: Silently succeed Warn but allow installation Do not allow installation HKLM\Software\Microsoft\Non-driver Signing\Policy = 1	Warn but allow installation	Warn but allow installation

Table 8 Security Options

Several settings should be configured at the domain-level group policy object. These are configured in the “W2K Domain Policy.inf” template and are shown in **Table 9**.

Security Attribute	Recommended Setting
Automatically log off users when logon time expires	Enabled
Rename Administrator account	<Configure Locally>
Rename Guest Account	<Configure Locally>

Table 9 Domain-wide Security Options

Adding an Entry to Security Options

In the Windows 2000 Security Configuration Tool Set, it is possible to add additional registry key settings to the Security Options portion of a template. To accomplish this, perform the following actions:

- ❑ Open the file %SystemRoot%\inf\sceregvl.inf (%SystemRoot% is usually C:\winnt) in Notepad, Wordpad, or another text editor
- ❑ Add a line in the form *regpath, type, displayname, displaytype* where
 - *regpath* – registry key value path, e.g.,
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects

- *type* – data type of the registry entry represented by a number. Possible values are REG_SZ (1), REG_EXPAND_SZ (2), REG_BINARY (3), REG_DWORD (4), REG_MULTISZ (7)
 - *displayname* – the name actually displayed in the security template, e.g., “Audit the access of global system objects”
 - *displaytype* – How the interface will display the registry value type. Possible values are Boolean (0), number (1), string (2), choices (3). If choices are specified, the choices should then be specified in the format *value1|display1,value2|display2,...*
- Re-register scecli.dll by executing `regsvr32 scecli.dll` at a command prompt

An example line in `sceregv1.inf` is:

```
MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ScRemoveOption,1,
%ScRemove%,3,0|%ScRemove0%,1|%ScRemove1%,2|%ScRemove2%
```

The strings listed above are defined in the [Strings] section of `sceregv1.inf`:

```
%ScRemove% = Smart card removal behavior
%ScRemove0% = No Action
%ScRemove1% = Lock Workstation
%ScRemove2% = Force Logoff
```

Deleting customized options

The deletion of customized security options is not as simple as removing the options from the `sceregv1.inf` file and re-registering the DLL. To ensure that options are permanently deleted from the templates, perform the following actions:

- Open `sceregv1.inf` in a text editor (e.g. Notepad)
- Delete the specific security option from the `sceregv1.inf` file under the [Register Registry Values] section
- Under the `sceregv1.inf` section labeled “delete these values from current system,” add the registry key to be removed from the templates. For example, taking the example used in the previous section, place `MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ScRemoveOption` under this section.
- Save and close `sceregv1.inf`
- At a command prompt, execute `regsvr32 scecli.dll`
- To confirm that the option has been deleted, open the Security Templates snap-in in the MMC and verify that the option no longer appears in the **Local Policies** → **Security Options** section of the template files
- To clean up, edit `sceregv1.inf` again, remove the entry added previously under “delete these values from current system,” save and close the file, then run `regsvr32 scecli.dll` again.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Modifying Event Log Settings with Security Templates

Windows 2000 event logs record system events as they occur. The Security, Application, and System event logs contain information generated by the specified audit settings. In addition to the audit settings enabled in the security templates, auditing of other system objects, such as specific files, registry keys, and printers, can be enabled.

To view event log settings of a security template double-click the following:

- ❑ **Security Templates**
- ❑ Default configuration file directory (%SystemRoot%\Security\Templates)
- ❑ Specific configuration file
- ❑ **Event Log**



NOTE: After making any modifications to the configuration files, make sure the changes are saved and then test the changes before installing them on an operational network.

Event Log Settings

Event log settings that can be configured with the security templates include maximum size, guest access, how long logs will be retained, and how the operating system handles logs at the maximum size.

To modify Event Log Settings via the Security Templates, double-click the following path:

Event Log → **Settings for Event Logs** → specific option to view or edit

Table 10 lists recommended Event Log settings for the Application, Security, and System logs.



Event Log Settings	Recommended Settings
<p><u>Maximum application log size</u> <u>Maximum security log size</u> <u>Maximum system log size</u></p> <p>If the event logs are too small, logs will fill up often and administrators must save and clear the event logs more frequently than required. Allowable values range from 64 KB to 4194240 KB.</p> <p>NOTE: This setting will allow the log file to equal the size of the available space on the hard disk or up to 4GB, whichever is smaller. This is to ensure that the system will not halt if the event log exceeds specified log space while there is additional space available on the hard drive.</p> 	4194240 KBytes
<p><u>Restrict guest access to application Log</u> <u>Restrict guest access to security Log</u> <u>Restrict guest access to system Log</u></p> <p>Default configuration allows guests and null logons the ability to view event logs (system and application logs). While the security log is protected from guest access by default, it is viewable by users who have the Manage Audit Logs user right. This option disallows guests and null logons from viewing any of the event logs.</p>	Enabled
<p><u>Retain application log</u> <u>Retain security log</u> <u>Retain system log</u></p> <p>These options control how long the event logs will be retained before they are overwritten. Allowable values are between 1 and 365 days. Since it is not recommended that any event logs be overwritten when they become full, this option should not be configured.</p>	Not defined
<p><u>Retention method for application Log</u> <u>Retention method for security Log</u> <u>Retention method for system Log</u></p> <p>How the operating system handles event logs that have reached their maximum size. The event logs can be overwritten after a certain number of days, overwritten when they become full, or have to be cleared manually. To ensure that no important data is lost, especially in the event of a security breach of the system, the event logs should not be overwritten.</p>	Manually
<p><u>Shut down the computer when the security audit log is full</u></p> <p>If events cannot be written to the security log, the system should be halted immediately. If the system halts as a result of a full log, an administrator must restart the system and clear the log.</p>  <p>WARNING: Enabling this option will disallow any connections to the system until the audit logs are cleared. Take caution when enabling this on critical systems. Also, enabling this option on a large number of workstations in the network may result in much overhead when the logs become full.</p>	Enabled

Table 10 Event Log Options

Managing the Event Logs

Security Options (discussed in Chapter 4) recommends enabling **Audit the access of global system objects** and **Audit use of all user rights including Backup and**

Restore. If these options are enabled, large amounts of audit data will be generated, requiring the logs to be cleared regularly.

Saving And Clearing the Audit Logs

To save and clear the logs:

- ❑ Select **Start** → **Programs** → **Administrative Tools** → **Event Viewer**
- ❑ Click on the log to be cleared in the right pane of the Event Viewer window
- ❑ Select **Clear All Events** from the **Action** menu
- ❑ Click **Yes** to save settings with unique file name
- ❑ Specify where the log will be saved and then click **Save**
- ❑ Click **Yes** to clear the log
- ❑ Repeat the above steps for each log

Resetting the Audit Log Settings After the System Halts

If the system halts as a result of a full log, an administrator must restart the system and clear the log.



NOTE: Before clearing the security log, save the data to disk.

After saving the log, use the registry editor (`regedt32.exe`) to modify the following registry key value:

Hive: **HKEY_LOCAL_MACHINE**
 Key: **\System\CurrentControlSet\Control\Lsa**
 Name: **CrashOnAuditFail**
 Type: **REG_DWORD**
 Value: **1**



NOTE: This value is set by the operating system just before it crashes due to a full audit log. While the value is 2, only the administrator can log on to the computer. This value confirms the cause of the crash. Reset the value 1

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Managing Restricted Groups with Security Templates

The Restricted Groups option allows the administrator to manage the membership of sensitive groups. For example, if the Administrators group is to only consist of the built-in Administrator account, the Administrators group can be added to the Restricted Groups option and Administrator can be added in the **Members of Administrators** column. This setting could prevent other users from elevating their privilege to the Administrators group through various attack tools and hacks.

Not all groups need to be added to the Restricted Group list. It is recommended that only sensitive groups be configured through security templates. Any groups not listed will retain their membership lists.

For all groups listed for this option, any groups and/or users listed which are not currently members of that group are added, and any users and/or groups currently members of the group but not listed in the configuration file are removed.

Modifying Restricted Groups via the Security Templates Snap-in

Since the settings in the Restricted Groups option should be environment-specific, only one restricted group setting is configured in the companion configuration (*inf*) files. However, a site may need to restrict the membership of additional sensitive groups within the domain.

To view restricted group settings of an SCM template double-click the following:

- Security Templates**
- Default configuration file directory (%SystemRoot%\Security\Templates)
- Specific configuration file
- Restricted Groups**



NOTE: After making any modifications to the configuration files make sure the changes are saved and then test the changes before installing them on an operational network.

The following steps describe how to add a restricted group to the list:

- Right-click **Restricted Groups**
- Select **Add Group**
- Click the **Browse** button

UNCLASSIFIED

- ❑ Double-click each group that needs to be added and **OK → OK**
- ❑ Double-click newly added group in the right frame
- ❑ Click **Add**
- ❑ Double-click each group and/or user who wish to be members of the group
- ❑ Click **OK → OK**

The recommended setting in the provided workstation and member server templates restricts the Power Users group to having no members.

Managing System Services with Security Templates

The System Services option allows for configuration of startup modes and access control lists for all system services. Configuration options include startup settings (Automatic, Manual, or Disabled) for services such as network, file, and print services. Security settings can also be established that control which users and/or groups can read and execute, write to, delete, start, pause, or stop a service.

Modifying System Services via the Security Templates Snap-in

Because of the broad nature of this area, system service configuration is environment-specific. Services not listed in this option can be added. However, a new DLL attachment will need to be created and attached. For more information on creating service attachments, refer to the white paper *Security Configuration Toolset* <http://www.microsoft.com/windows2000/library/howitworks/security/sctoolset.asp>.

To view system services settings of a security template double-click the following in the MMC:

- ❑ **Security Templates**
- ❑ Default configuration file directory (%SystemRoot%\Security\Templates)
- ❑ Specific configuration file
- ❑ **System Services**



NOTE: After making any modifications to the configuration files make sure the changes are saved, and then test the changes before installing them on an operational network.

The following steps describe how to configure system service settings;

- ❑ Double-click the service to configure
- ❑ Check the **Define this policy setting in the template** checkbox
- ❑ If this is policy was previously undefined, the Security dialog box will automatically appear. Otherwise, click **Edit Security**
- ❑ Click **Add** (to add groups and/or users to the access list)
- ❑ Double-click each user or group to add and **OK**
- ❑ Check the permissions that each user or group should have for that service
- ❑ Click **Remove** (to remove groups and/or users from the access list)

- ❑ When finished entering the permissions, click **OK**
- ❑ Under **Select service startup mode**, select **Automatic**, **Manual**, or **Disabled**

Figure 4 shows the System Services entries in the Security Templates snap-in.

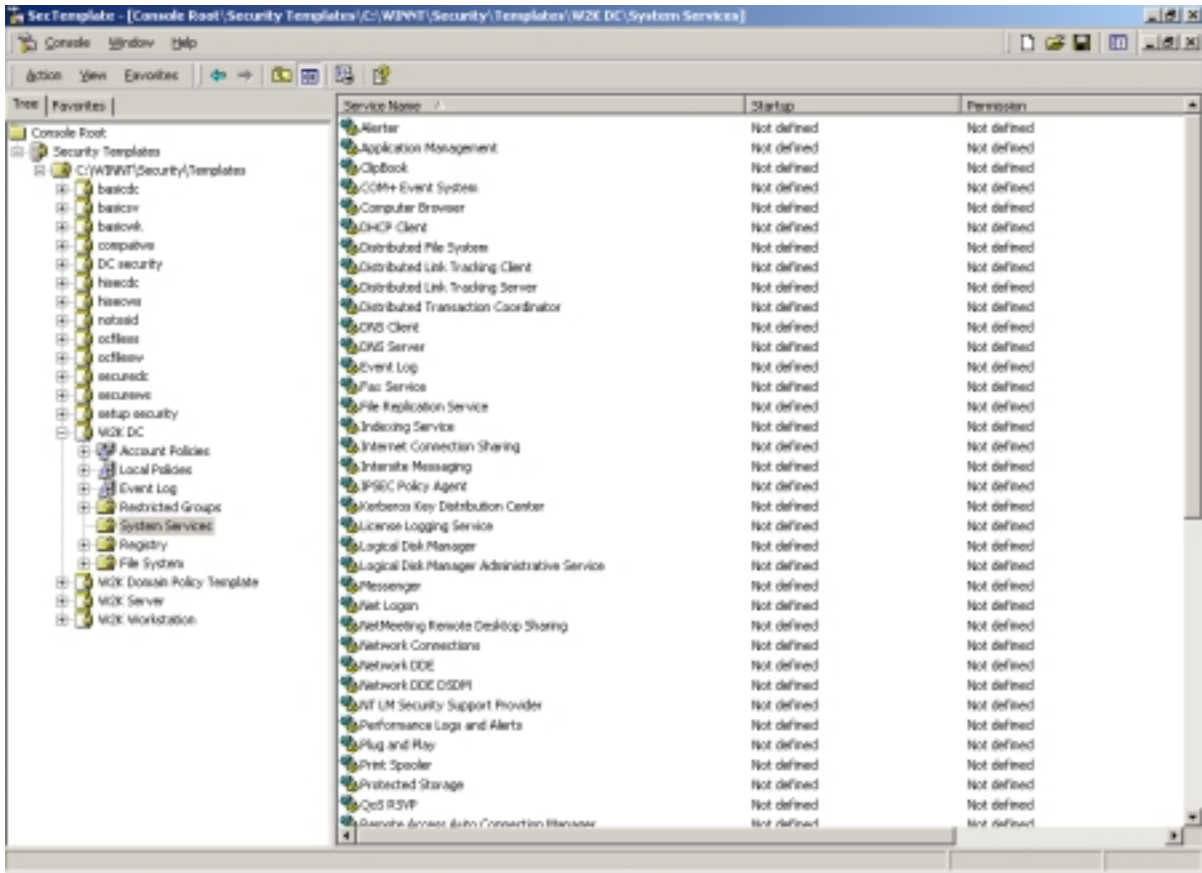


Figure 4 System Services

System Services Security

If compromised, services may offer direct access to system resources or fall victim to buffer overflows or denial of service attacks. Therefore, the proper configuration of services is an important security step. Since services are environment and application specific, no services are configured in this document. However, there are a few guidelines to consider when configuring services:

- ❑ Only run necessary services. For example, if the telnet service or FTP service is running on a system, but not being used, disable them.
- ❑ Ensure that only a limited number of users/groups can start, stop, or change a service.
- ❑ If a service is listed, but not needed, change the startup mode to Disabled instead of Manual. This will ensure that the service cannot be restarted by an unauthorized or malicious user.

UNCLASSIFIED

- When configuring either the startup mode or access control list for a service, you must configure the other as well. When a service is explicitly disabled, its ACL should also be secured by changing the default ACL from Everyone Full Control to grant Administrators and SYSTEM Full Control and Authenticated Users Read access.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Modifying Registry Security Settings with Security Templates

The Security Configuration Tool Set can be used to configure discretionary access control lists (DACLS) for registry keys. In order to implement adequate security in a Windows 2000 environment, some registry key permissions should be changed. The recommended changes can also be made manually using `regedt32.exe`; however, this method is more time-consuming and leaves more room for error.



WARNING: By default, some protections are set on the various components of the registry that allow work to be done while providing standard-level security. For high-level security, additional access rights must be added to specific registry keys. This should be done with caution because programs that users need to do their jobs often require access to certain keys on the users' behalf. Care should be taken to follow these steps exactly, as additional, unnecessary changes to the registry can render a system unusable and even unrecoverable.

Inheritance model

Those who used the Security Configuration Manager with Windows NT 4.0 Service Pack 4 or higher may remember a new inheritance model with respect to registry and file discretionary access control lists (DACLS), i.e., permissions. Windows 2000 and NTFS version 5 implement the full functionality of this inheritance model. Within the new inheritance model, permissions on child objects are automatically inherited from their parent. This can be seen by the check in the **Allow inheritable permissions from parent to propagate to this object** checkbox in the DACL editor. More permissions can be explicitly defined for a child object in addition to those the child inherits from its parent.

When the checkbox is not checked, the DACLS defined on that object apply only to that object and its children. No permissions are inherited from the parent object.

Registry permissions

To manually view permissions on a specific registry key:

- Run `regedt32.exe`
- Select the desired registry key
- In the Registry Editor, select the **Security** menu
- Select **Permissions...**

Only Read and Full Control permissions appear in the permissions dialog box. However, permissions may be set with more granularity by clicking the **Advanced** button. **Table 11** shows a list of granular registry permissions. **Table 12** shows which granular permissions to select in order to achieve certain higher-level permissions.



NOTE: Any time a permission is not a pure Read or Full Control, the permission is noted as Special in the Advanced Access Control Settings window.

Special Permissions	Description
Query Value	Allows querying the registry for a specific value
Set Value	Allows new values to be created for a key and old values to be overwritten
Create Subkey	Allows the creation of subkeys
Enumerate Subkeys	Allows viewing of a list of subkeys under a registry key
Notify	Allows registration of a callback function that is triggered when the value changes
Create Link	Allows the creation of link to a specific key
Delete	Allows deletion of a value or key
Write DAC	Allows modification of access controls on the key
Write Owner	Allows a user to take ownership of a key
Read Control	Allows reading of the key's access control list

Table 11 Registry Permissions and Descriptions

Special Permissions	Full Control	Read	Write	Delete
Query Value	x	x		
Set Value	x		x	
Create Subkey	x		x	
Enumerate Subkeys	x	x		
Notify	x	x		
Create Link	x			
Delete	x			x
Write DAC	x			
Write Owner	x			
Read Control	x	x	x	

Table 12 Registry Permission Options

Modifying Registry settings via the Security Templates snap-in

Within a security template, registry permissions may be customized by either modifying existing registry keys in an `inf` file, or by adding your own registry keys and permissions.

To view registry settings of a security template select the following:

- Security Templates**
- Default file directory (%SystemRoot%\Security\Templates)
- Specific configuration file
- Registry**

Modifying Permissions on a Registry Key

To modify the security settings on a particular registry key already specified in the `inf` file:

- In the right frame, double-click on the key to be changed
- Ensure that the **Configure this key then** radio button is selected. Under this option, there are two other options:
 - **Propagate inheritable permissions to all subkeys** – all subkeys that already inherit permissions from the key being configured will inherit the new permissions. This option will have no effect on subkeys that do not have **Allow inheritable permissions from parent to propagate to this object** enabled in their DACLs.
 - **Replace existing permissions on all subkeys with inheritable permissions** – all subkeys will have their permissions set to the new permissions and will inherit from the key being configured regardless of any inheritance or blocking of inheritance on subkeys.
- Click **Edit Security**
- Ensure that the **Allow inheritable permissions from parent to propagate to this object** checkbox is unchecked
- Modify users and groups to reflect the recommended permissions by clicking the **Add** or **Remove** buttons
- For each user and/or group, set the permissions by clicking on the permission checkboxes.
- The only permissions that appear in the **Permissions** dialog box are Read and Full Control. If these permissions are all that is desired, and if the key permissions should encompass the key itself and all subkeys below the key, click **Apply** → **OK**. Stop here.

If extra granularity needs to be added to the permissions:

- Click the **Advanced** button. **Figure 5** shows the Advanced dialog box



NOTE: More granular permissions (special access) for a user and/or group can be configured through the Advanced dialog box.

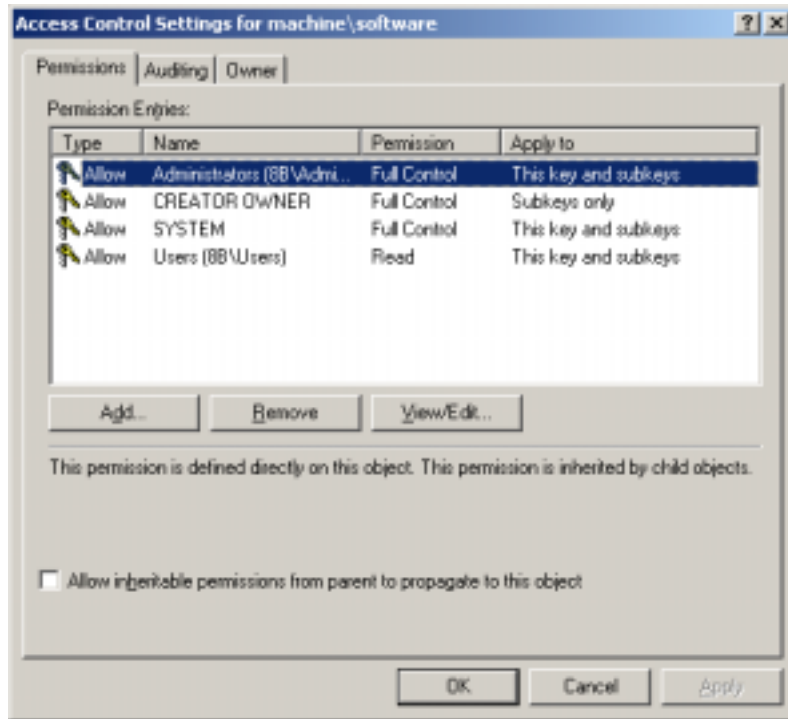


Figure 5 Advanced Registry Permissions Dialog Box

- ❑ Click on a user and/or group
- ❑ Click **View/Edit**. A **Permission Entry** dialog box will appear
- ❑ In the **Apply** onto pull-down menu, select the correct configuration. Possible values are: **This key only**, **This key and subkeys**, and **Subkeys only**
- ❑ In the Permissions pane, select the desired permissions. Refer to the earlier section on registry permissions
- ❑ Click **OK** → **OK** → **OK** → **OK** to exit

Adding registry keys to the security configuration

To add a registry key to the security configuration:

- ❑ Right-click on **Registry**
- ❑ Select **Add Key** from the pull-down menu
- ❑ Select the registry key to be added
- ❑ Click **OK**
- ❑ A **Configuration Security** dialog box will appear
- ❑ Click **OK**
- ❑ Double-click on the registry key in the right frame when it appears
- ❑ Configure the permissions according to the steps detailed in the previous **Modifying permissions on a registry key** section.

Excluding registry keys from the security configuration

There are occasions where a specific registry key should retain its current security settings. To ensure that parent keys do not propagate their new permissions down to such registry keys, the object may be excluded from configuration.

To exclude an object:

- In the right frame of **Registry**, double-click on the key to be changed
- Click the **Do not allow permissions on this key to be replaced** radio button.
- Click **OK**

Recommended Registry Key Permissions

Registry keys not explicitly listed below in **Table 13** are assumed to inherit the permissions of their parent key if they already have **Allow inheritable permissions from parent to propagate to this object** checked in their DACL. Keys with “Ignore” selected are explicitly excluded from security configuration and retain their original permissions.

In the table, the term “Propagate” indicates that the **Propagate inheritable permissions to all subkeys** radio button should be enabled while “Replace” indicates that the **Replace existing permissions on all subkeys with inheritable permissions** radio button should be enabled.




NOTE: Several of the security settings listed below are based on Microsoft’s high security template (hisecls.inf). Microsoft chose to exclude several keys by setting the “Ignore” attribute in order to maintain the default security settings. It cannot be assumed that these default settings have not been modified in the past. Therefore, it was decided to explicitly set permissions on some of these keys to reflect what the default permissions should be. In such cases, the “Propagate” option was selected.



The following notation is used in this section of the security templates:

- CLASSES_ROOT indicates HKEY_CLASSES_ROOT hive
- MACHINE indicates HKEY_LOCAL_MACHINE hive
- USERS indicates HKEY_USERS hive

In the domain controller security template, “W2K DC.inf,” all instances of the **Users** group have been replaced with the **Authenticated Users** group.

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<p><u>CLASSES_ROOT</u></p> <p>Alias to MACHINE\SOFTWARE\Classes. Contains file associations and COM (Common Object Model) associations.</p>	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
<p><u>MACHINE\SOFTWARE</u></p> <p>Contains information about the software installed on the local system.</p>	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
<p><u>MACHINE\SOFTWARE\Microsoft\NetDDE</u></p> <p>Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data.</p>	Administrators SYSTEM	Full Control Full Control	Replace
<p><u>MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT</u></p> <p>Contains support for OS/2 standards. Even if this key is removed, it will reappear at next boot up.</p>	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (Subkeys only) Full Control	Replace
<p><u>MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider</u></p> <p>Used to protect user data. Inaccessible.</p>	Ignore		Ignore
<p><u>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AsrCommands</u></p> <p>Automatic Server Recovery commands.</p> <p> NOTE: If not using the Backup Operators group, remove the group from these permissions.</p>	Administrators Backup Operators CREATOR OWNER SYSTEM Users	Full Control Query, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions Full Control (Subkeys only) Full Control Read	Replace
<p><u>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib</u></p> <p>Parameters for the Performance Library, which collects information for Performance Monitor. Contains a language code subkey for each spoken language configured on the Windows 2000 system. For example, a subkey named 009 contains counters and descriptions for the language code English (United States).</p>	Administrators INTERACTIVE CREATOR OWNER SYSTEM	Full Control Read Full Control Full Control	Replace
<p><u>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy</u></p> <p>Contains data for Group Policy settings that configure the Group Policy components of Windows 2000. Contains subkeys representing each of the client-side extensions used to create settings in Group Policy.</p>	Administrators Authenticated Users SYSTEM	Full Control Read Full Control	Propagate
<p><u>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer</u></p> <p>Contains configuration information for the Windows Installer.</p>	Administrators SYSTEM Users	Full Control Full Control Read	Propagate

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<p><u>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies</u></p> <p>Stores registry entries managed by Group Policy. Manages entries for the following subkeys:</p> <p>HKLM\SOFTWARE\Policies</p> <p>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies</p> <p>HKCU\SOFTWARE\Policies</p> <p>HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies</p>	<p>Administrators Authenticated Users SYSTEM</p>	<p>Full Control Read Full Control</p>	<p>Propagate</p>
<p><u>MACHINE\SYSTEM</u></p> <p>Stores values for the current control set or control sets that have been previously used to start Windows 2000.</p>	<p>Administrators CREATOR OWNER SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Replace</p>
<p><u>MACHINE\SYSTEM\clone</u></p>	<p>Ignore</p>		<p>Ignore</p>
<p><u>MACHINE\SYSTEM\controlset001</u></p> <p>Contains a control set that may be used to start and run Windows 2000.</p>	<p>Administrators CREATOR OWNER SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Propagate</p>
<p><u>MACHINE\SYSTEM\controlset002</u></p> <p>Contains a control set that may be used to start and run Windows 2000.</p>	<p>Administrators CREATOR OWNER SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Propagate</p>
<p><u>MACHINE\SYSTEM\controlset003</u></p> <p>Contains a control set that may be used to start and run Windows 2000.</p>	<p>Administrators CREATOR OWNER SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Propagate</p>
<p><u>MACHINE\SYSTEM\controlset004</u></p> <p>Contains a control set that may be used to start and run Windows 2000.</p>	<p>Administrators CREATOR OWNER SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Propagate</p>
<p><u>MACHINE\SYSTEM\controlset005</u></p> <p>Contains a control set that may be used to start and run Windows 2000.</p>	<p>Administrators CREATOR OWNER SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Propagate</p>
<p><u>MACHINE\SYSTEM\controlset006</u></p> <p>Contains a control set that may be used to start and run Windows 2000.</p>	<p>Administrators CREATOR OWNER SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Propagate</p>
<p><u>MACHINE\SYSTEM\controlset007</u></p> <p>Contains a control set that may be used to start and run Windows 2000.</p>	<p>Administrators CREATOR OWNER SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Propagate</p>

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<u>MACHINE\SYSTEM\controlset008</u> Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
<u>MACHINE\SYSTEM\controlset009</u> Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
<u>MACHINE\SYSTEM\controlset010</u> Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
<u>MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg</u> The security permissions set on this key define which users or groups can connect to the system for remote registry access. If the key does not exist, anyone can remotely connect to the registry. It is highly recommended that only administrators have remote access to the registry.  NOTE: If not using the Backup Operators group, remove the group from these permissions.  WARNING: Microsoft Exchange 2000 requires remote registry access. Therefore, on Exchange servers and domain controllers within the domain, add the Exchange Domain Servers group with Full Control access on this registry key.	Administrators Backup Operators SYSTEM	Full Control Read (Key only) Full Control	Replace
<u>MACHINE\SYSTEM\CurrentControlSet\Control\Wmi\Security</u> Security settings for the Windows Management Instrumentation (WMI). WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM).	Administrators CREATOR OWNER SYSTEM	Read Full Control Full Control	Replace
<u>MACHINE\SYSTEM\CurrentControlSet\Enum</u> Contains configuration data for hardware devices installed on the system. Changing permissions on this key may result in damage to the Plug and Play function of Windows 2000.	Ignore		Ignore



REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<p><u>MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles</u></p> <p>Contains system hardware profiles (changes to the initial hardware configuration stored in the Software and System keys).</p>	<p>Administrators CREATOR OWNER</p> <p>SYSTEM Users</p>	<p>Full Control Full Control (Subkeys only) Full Control Read</p>	<p>Propagate</p>
<p><u>MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers</u></p> <p>Only exists if the SNMP service has been started on the system. The default permissions for this key allow Users to gather SNMP information that may in turn be used to attack the network.</p> <p> NOTE: These permissions are also set via a Windows 2000 post Service Pack 1 hotfix, http://www.microsoft.com/windows2000/library/planning/security/secconfsteps.asp.</p>	<p>Administrators CREATOR OWNER SYSTEM</p>	<p>Full Control Full Control Full Control</p>	<p>Replace</p>
<p><u>MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities</u></p> <p>Only exists if the SNMP service has been started on the system. The default permissions for this key allow Users to gather SNMP information that may in turn be used to attack the network.</p> <p> NOTE: These permissions are also set via a Windows 2000 post Service Pack 1 hotfix, SNMP Parameters Vulnerability, KB Article Q266794 http://www.microsoft.com/technet/support/kb.asp?ID=266794.</p>	<p>Administrators CREATOR OWNER SYSTEM</p>	<p>Full Control Full Control Full Control</p>	<p>Replace</p>
<p>USERS\DEFAULT</p> <p>Profile that is used while the Windows 2000 CTRL+ALT+DEL logon message is displayed.</p>	<p>Administrators Authenticated Users CREATOR OWNER</p> <p>SYSTEM</p>	<p>Full Control Read Full Control (Subkeys only) Full Control</p>	<p>Replace</p>
<p><u>USERS\DEFAULT\Software\Microsoft\NetDDE</u></p> <p>Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data.</p>	<p>Administrators SYSTEM</p>	<p>Full Control Full Control</p>	<p>Replace</p>
<p><u>USERS\DEFAULT\Software\Microsoft\Protected Storage Systems Provider</u></p> <p>Used to protect user data. Inaccessible.</p>	<p>Ignore</p>		<p>Ignore</p>

Table 13 Recommended Registry Permissions

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Modifying File System Security Settings with Security Templates

NTFS is a secure file system that provides a reliable way to safeguard valuable information. NTFS works in concert with the Windows 2000 user account system to allow authenticated users access to files. The system provides extended permissions for controlling access to files and prohibits easy access to data on disk if someone manages to boot the system with another operating system. **To implement the highest level of security, always format Windows 2000 partitions with the NT File System.**

The security provided by NTFS is based on system controls that are managed by the Windows 2000 operating system. As long as Windows 2000 is operating, NTFS permissions and user access control lists prevent unauthorized users from accessing files either locally or over the network.

NTFS allows for varying levels of file access permissions to users or groups of users. Combined with file access permissions, is the concept of “inheritance.” By default, newly created files or folders inherit the parent folder’s file access permissions. Refer to the previous chapter on the registry for more information on Windows 2000 inheritance.

File and folder permissions

To manually view permissions on a specific file or folder:

- In Windows Explorer, right-click on the file or folder
- Select **Properties** from the pull-down menu
- Click the **Security** tab
- Click **Advanced** to see more detailed permission information

File permissions may be set with more granularity than those listed in the Permissions dialog box by clicking the **Advanced** button. **Table 14** shows a list of granular file permissions. **Table 15** and **Table 16** show which granular permissions to select in order to achieve certain higher-level permissions for folders and files.

Special Permissions	Description
Traverse Folder/Execute File	Traverse Folder allows users to move through a folder to access other files or folders, regardless of permissions the user may or may not have on that folder (folders only). This permission only has meaning when the user has not been granted the Bypass Traverse Checking user right. The Execute File permission allows a user to run program files (files only).
List Folder/Read Data	List Folder allows the reading of file names and subfolders within a folder (folders only). Read Data allows file data to be read (files only).
Read Attributes	Allows viewing of a file's NTFS attributes (e.g., "Read only" or "Hidden").
Read Extended Attributes	Allows viewing of a file's extended attributes. Extended attributes may vary as they are defined by specific programs.
Create Files/Write Data	Create Files allows the creation of files within a folder (folders only). Write Data allows modification and/or overwriting of files (files only).
Create Folders/Append Data	Create Folders allows the creation of folders within a folder (folders only). Append Data allows making changes to the end of file (files only).
Write Attributes	Allows the modification of a file's NTFS attributes (e.g., "Read only" or "Hidden").
Write Extended Attributes	Allows the modification of a file's program-specific extended attributes.
Delete Subfolders and Files	Allows the deletion of subfolders and files regardless if the Delete permission was granted on the subfolder or file.
Delete	Allows deletion of a file or folder.
Read Permissions	Allows viewing of the permissions on a file or folder.
Change Permissions	Allows the modification of the permissions on a file or folder.
Take Ownership	Allows taking ownership of a file or folder.

Table 14 File Permissions and Descriptions

Folder Permissions:

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					

Table 15 Folder Permissions Options



NOTE: List Folder Contents is inherited by folders but not files while Read and Execute is inherited by both folders and files.

File Permissions:

Special Permissions	Full Control	Modify	Read & Execute	Read	Write
Traverse Folder/Execute File	x	x	x		
List Folder/Read Data	x	x	x	x	
Read Attributes	x	x	x	x	
Read Extended Attributes	x	x	x	x	
Create Files/Write Data	x	x			x
Create Folders/Append Data	x	x			x
Write Attributes	x	x			x
Write Extended Attributes	x	x			x
Delete Subfolders and Files	x				
Delete	x	x			
Read Permissions	x	x	x	x	x
Change Permissions	x				
Take Ownership	x				

Table 16 File Permissions Options

Modifying File System settings via the Security Template snap-in

The recommended changes to system files and folders are listed in **Table 17**.

The necessary changes can be made in one of two ways. The first method is to use the Security Configuration Tool Set to apply the recommended file and folder permissions. The alternative and more time-consuming method is to change permissions on each file and folder manually.

To view file system settings of a security template select the following in the MMC:

- Security Templates**
- Default file directory (%SystemRoot%\Security\Templates)
- Specific configuration file
- File System**

Modifying Permissions on a File or Folder

To modify the security settings on a particular file or folder already specified in the `inf` file:

- In the right frame, double-click on the file or folder to be changed

- ❑ Ensure that the **Configure this file or folder then** radio button is selected. Under this option, there are two other options:
 - **Propagate inheritable permissions to all subfolders and files** – all subfolders and files that already inherit permissions from the folder being configured will inherit the new permissions. This option will have no affect on subfolders or files that do not have **Allow inheritable permissions from parent to propagate to this object** enabled in their DACLs
 - **Replace existing permissions on all subfolders and files with inheritable permissions** – all subfolders and files will have their permissions set to the new permissions and will inherit from the key being configured regardless of any inheritance or blocking of inheritance on those subfolders or files
- ❑ Click **Edit Security**
- ❑ Ensure that the **Allow inheritable permissions from parent to propagate to this object** checkbox is unchecked
- ❑ Modify users and groups to reflect the recommended permissions by clicking the **Add** or **Remove** buttons
- ❑ For each user and/or group, set the permissions by clicking on the permission checkboxes
- ❑ The permissions that appear in the **Permissions** dialog box are Full Control, Modify, Read and Execute, List Folder Contents, Read, and Write. If these permissions are all that is desired and if the folder permissions encompass the folder itself and all subfolders and files below the key, click **Apply → OK**. Stop here

If extra granularity of permissions needs to be applied:

- ❑ Click the **Advanced** button



NOTE: More granular permissions (special access) for a user and/or group can be configured through the Advanced dialog box.

- ❑ Click the user or group to be edited.
- ❑ Click **View/Edit**. A **Permission Entry** dialog box will appear.
- ❑ In the **Apply** onto pull-down menu, select the correct configuration (e.g., **This folder only**).
- ❑ Click **OK → OK → OK → OK** to exit

Adding files or folders to the security configuration

To add a file or folder to the security configuration:

- ❑ Right-click on **File System**
- ❑ Select **Add File** from the pull-down menu
- ❑ Select the file or folder to be added
- ❑ Click **OK**
- ❑ A **Configuration Security** dialog box will appear

- ❑ Configure the permissions according to the steps detailed in the previous **Modifying permissions on a file or folder** section

Excluding files or folders from the security configuration

There are occasions when a specific file or folder should retain its current security settings. To ensure that parent folders do not propagate their new permissions down to such files or folders, the object may be excluded from configuration.

To exclude an object:

- ❑ In the right frame of **File System**, double-click on the file or folder to be changed
- ❑ Click the **Do not allow permissions on this file or folder to be replaced** radio button
- ❑ Click **OK**

Recommended File and Folder Permissions

Folders and files not explicitly listed below are assumed to inherit the permissions of their parent folder. Folders with “Ignore” are explicitly excluded from security configuration and retain their original permissions. The term “Replace” indicates that the **Replace existing permissions on all subfolders and files with inheritable permissions** radio button should be enabled while “Propagate” indicates that the **Propagate inheritable permissions to all subfolders and files** radio button should be enabled. **Figure 6** shows these options. Unless otherwise noted, permissions are assumed to apply to all subfolders and files below the configured folder.



NOTE: Several of the security settings listed below are based on Microsoft’s high security template (`hisecls.inf`). Microsoft chose to exclude several folders by setting the “Ignore” attribute in order to maintain the default security settings. However, it cannot be assumed that these default settings have not been modified in the past. Therefore, permissions have been set explicitly on most of these folders to reflect what the default permissions should be. In such cases, the “Propagate” option was selected.

In the domain controller security template, “W2K DC.inf,” all instances of the **Users** group have been replaced with the **Authenticated Users** group.




Figure 6 File/Folder Permission Inheritance Options

Folders and files in **Table 16** are alphabetized as they appear in the security templates GUI.



FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<u>%ProgramFiles%</u> Folder in which applications are installed.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
<u>%SystemDirectory%</u> Contains many operating system DLLs, drivers, and executable programs.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
<u>%SystemDirectory%\appmgmt</u> Contains application management files used for software installation.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
<u>%SystemDirectory%\config</u> Contains registry hive files.	Administrators SYSTEM	Full Control Full Control	Replace
<u>%SystemDirectory%\dllcache</u> Contains copies of protected system files. These copies are used by the System File Checker to repair corrupted or modified system files.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
<u>%SystemDirectory%\DTCLog</u> Log file for MS Distributed Transaction Coordinator, which is required for Microsoft Transaction Server.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate
<u>%SystemDirectory%\GroupPolicy</u> Folder containing local Group Policy Objects.	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control	Propagate
<u>%SystemDirectory%\ias</u> Contains databases for the Internet Authentication Service.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
<u>%SystemDirectory%\Ntbackup.exe</u> File system backup program.	Administrators SYSTEM	Full Control Full Control	Replace
<u>%SystemDirectory%\NTMSData</u> Default location for the Removable Storage database.	Administrators SYSTEM	Full Control Full Control	Propagate
<u>%SystemDirectory%\rcp.exe</u> Program used to execute remote procedure calls.	Administrators SYSTEM	Full Control Full Control	Replace
<u>%SystemDirectory%\Regedt32.exe</u> Registry editing tool	Administrators SYSTEM	Full Control Full Control	Replace
<u>%SystemDirectory%\ReinstallBackups</u> Contains files used for reinstallations.	Ignore		Ignore
<u>%SystemDirectory%\repl</u> Folder containing scripts and files to be replicated or that have been replicated.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate


UNCLASSIFIED

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<u>%SystemDirectory%\repl\export</u> Folder containing scripts and files to be replicated to other replication servers.	Administrators Replicator SYSTEM Users	Full Control Read, Execute Full Control Read, Execute	Propagate
<u>%SystemDirectory%\repl\import</u> Folder containing scripts and files that have been replicated from other replication servers.	Administrators Replicator SYSTEM Users	Full Control Modify Full Control Read, Execute	Propagate
<u>%SystemDirectory%\rexec.exe</u> Program used to execute remote calls.	Administrators SYSTEM	Full Control Full Control	Replace
<u>%SystemDirectory%\rsh.exe</u> Program used to execute a remote shell.	Administrators SYSTEM	Full Control Full Control	Replace
<u>%SystemDirectory%\secedit.exe</u> Security configuration and analysis tool.	Administrators SYSTEM	Full Control Full Control	Replace
<u>%SystemDirectory%\Setup</u> Contains setup DLLs.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
<u>%SystemDirectory%\spool\Printers</u> Printer spool.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (folder and subfolders)	Replace
<u>%SystemDrive%</u> Drive on which Windows 2000 is installed. Contains important system startup and configuration files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate
<u>%SystemDrive%\autoexec.bat</u> <u>c:\autoexec.bat</u> Initialization file for DOS applications.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
<u>%SystemDrive%\boot.ini</u> <u>c:\boot.ini</u> Boot menu.	Administrators SYSTEM	Full Control Full Control	Replace
<u>%SystemDrive%\config.sys</u> <u>c:\config.sys</u> Initialization file for DOS applications.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
<u>%SystemDrive%\Documents and Settings</u> Folder containing user and default profiles.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<p><u>%SystemDrive%\Documents and Settings\Administrator</u></p> <p>Folder containing the built-in Administrator profile.</p>  <p>WARNING: There may be other administrator profiles on the system, such as local administrator profiles (for example, Administrator.localmachine name). Some of these profiles may inherit from its parent folder, Documents and Settings. To prevent these folders from inheriting the parent permissions (which give Users RX), add these folders into the security template and grant only Administrators and SYSTEM Full Control, removing the Users and/or Authenticated Users group from the ACL.</p>	Administrators SYSTEM	Full Control Full Control	Replace
<p><u>%SystemDrive%\Documents and Settings>All Users</u></p> <p>Folder containing desktop and profile attributes for all users.</p>	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
<p><u>%SystemDrive%\Documents and Settings\Default User</u></p> <p>Folder containing default desktop and profile attributes for users logging on for the first time.</p>	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
<p><u>%SystemDrive%\Documents and Settings>All Users\Documents\DrWatson</u></p> <p>Folder containing the Dr. Watson application error log.</p>	Administrators CREATOR OWNER SYSTEM Users Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (subfolders and files) Read, Execute	Replace
<p><u>%SystemDrive%\Documents and Settings>All Users\Documents\DrWatson\drwtsn32.log</u></p> <p>Dr. Watson application error log file.</p>	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control Full Control Modify	Replace
<p><u>%SystemDrive%\Inetpub</u> (Servers only)</p> <p>IIS web server folder. Only exists if IIS 5.0 is installed. Ignored in this document. See NSA's <i>Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0</i> for recommended file settings on this folder.</p>	Ignore		Ignore

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<p><u>%SystemDrive%\io.sys</u> Initialization file for DOS applications.</p>	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
<p><u>%SystemDrive%\msdos.sys</u> Initialization file for DOS applications.</p>	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
<p><u>%SystemDrive%\My Download Files</u> A default folder for downloaded documents.</p>	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Write, Execute	Replace
<p><u>%SystemDrive%\ntdetect.com</u> <u>c:\ntdetect.com</u> Hardware detector during Windows 2000 boot.</p>	Administrators SYSTEM	Full Control Full Control	Replace
<p><u>%SystemDrive%\ntldr</u> <u>c:\ntldr</u> Windows 2000 operating system loader.</p>	Administrators SYSTEM	Full Control Full Control	Replace
<p><u>%SystemDrive%\System Volume Information</u> Accessible only by SYSTEM.</p>	Ignore		Ignore
<p><u>%SystemDrive%\Temp</u> Folder containing temporary files.</p>	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders)	Replace
<p><u>%SystemRoot%</u> Folder in which the Windows 2000 operating system is installed. By default, this is called winnt.</p>	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
<p><u>%SystemRoot%\\$NtServicePackUninstall\$</u> Contains older versions of system files necessary to back off a service pack.</p>	Administrators SYSTEM	Full Control Full Control	Replace
<p><u>%SystemRoot%\\$NtUninstall* (all uninstall folders)</u> Contains uninstall files for hotfixes and other applications.</p> <p> NOTE: Substitute the name of the folder(s) for \$NtUninstall*. The security template will not recognize the wildcard character *.</p>	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<p><u>%SystemRoot%\CSC</u></p> <p>Contains all offline files requested by any user on the computer. CSC means “client side caching”.</p>	Administrators SYSTEM	Full Control Full Control	Replace
<p><u>%SystemRoot%\debug</u></p> <p>Contains various system and Active Directory logs.</p>	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate
<p><u>%SystemRoot%\debug\UserMode</u></p> <p>Contains logs for group policy application to users.</p>	Administrators SYSTEM Users Users	Full Control Full Control Traverse folder, List folder, Create files (folder only) Create files, Create folders (files only)	Propagate
<p><u>%SystemRoot%\NTDS</u> (Domain Controllers only)</p> <p>Active Directory database folder.</p> <p> NOTE: The %SystemRoot% portion of the path name may need to be changed depending on where the default Active Directory folder is located.</p>	Administrators SYSTEM	Full Control Full Control	Propagate
<p><u>%SystemRoot%\Program Files\ Resource Kit</u> (servers and domain controllers) <u>%SystemRoot%\Program Files\ Resource Pro Kit</u> (workstations)</p> <p>Folder where the Windows 2000 server Resource Kit (or professional resource kit) is installed.</p>	Administrators SYSTEM	Full Control Full Control	Replace
<p><u>%SystemRoot%\security</u></p> <p>Contains security templates and analysis databases.</p>	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (subfolders and files) Full Control	Replace
<p><u>%SystemRoot%\SYSVOL</u> (Domain Controllers only)</p> <p>Default Active Directory location for files that must be shared throughout a domain.</p> <p> NOTE: The %SystemRoot% portion of the path name may need to be changed depending on where the default Active Directory folder is located.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control (subfolders and files) Full Control	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<p><u>%SystemRoot%\SYSVOL\domain\Policies</u> (Domain Controllers only)</p> <p>Contains group policy objects.</p>  <p>NOTE: The %SystemRoot% portion of the path name may need to be changed depending on where the default Active Directory folder is located.</p>	<p>Administrators Authenticated Users CREATOR OWNER</p> <p>Group Policy Creator Owners SYSTEM</p>	<p>Full Control Read, Execute Full Control (subfolders and files) Modify</p> <p>Full Control</p>	<p>Propagate</p>
<p><u>%SystemRoot%\Offline Web Pages</u></p> <p>Folder containing web pages that have been downloaded for off-line viewing.</p>	<p>Ignore</p>		<p>Ignore</p>
<p><u>%SystemRoot%\regedit.exe</u></p> <p>Registry editing tool.</p>	<p>Administrators SYSTEM</p>	<p>Full Control Full Control</p>	<p>Replace</p>
<p><u>%SystemRoot%\Registration</u></p> <p>Folder containing Component Load Balancing (CLB) registration files read by COM+ applications.</p>	<p>Administrators SYSTEM Users</p>	<p>Full Control Full Control Read</p>	<p>Propagate</p>
<p><u>%SystemRoot%\repair</u></p> <p>Backup files of SAM database and other important registry and system files to be used during a system repair.</p>	<p>Administrators SYSTEM</p>	<p>Full Control Full Control</p>	<p>Replace</p>
<p><u>%SystemRoot%\Tasks</u></p> <p>Folder containing jobs scheduled by Task Scheduler.</p>	<p>Ignore</p>		<p>Ignore</p>
<p><u>%SystemRoot%\Temp</u></p> <p>Folder containing temporary files.</p>	<p>Administrators CREATOR OWNER</p> <p>SYSTEM Users</p>	<p>Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders)</p>	<p>Replace</p>

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
<p><u>C:\ntbootdd.sys</u></p> <p>Copy of the SCSI device driver. Used when using SCSI or Signature syntax in boot.ini.</p>	Administrators SYSTEM	Full Control Full Control	Replace

Table 17 Recommended File Permissions

Security Configuration and Analysis

Once the appropriate security templates have been modified, security analysis and configuration can be performed via the Security Configuration and Analysis snap-in or command line operations. This procedure should be conducted when applying a security configuration to a local system. For instructions on importing security templates into Group Policy, see the *Guide to Securing Microsoft Windows 2000 Group Policy*.



WARNING: Applying a secure configuration to a Windows 2000 system may result in a loss of performance and functionality.

Loading the Security Configuration and Analysis snap-in into the MMC

To load the Security Configuration and Analysis snap-in into the MMC:

- Run the Microsoft Management Console (`mmc .exe`)
- Select **Console** → **Add/Remove Snap-in**
- Click **Add**
- Select **Security Configuration and Analysis**
- Click **Add**
- Click **Close**
- Click **OK**

To avoid having to reload the snap-in every time the MMC is exited and reopened, save the current console settings by performing the following:

- In the **Console** menu, select **Save**. By default, the file will be saved in the Administrative Tools menu of the currently logged-on user.
- Enter the file name under which the current console settings will be saved

From then on, the console can be accessed from **Start** → **Program Files** → **Administrative Tools**.



NOTE: More than one snap-in can be loaded into the MMC at one time. E.g., the Security Templates and Security Configuration and Analysis templates can both be loaded into a console that is saved for future use.

Security Configuration Databases

The Security Configuration and Analysis snap-in uses a database to store settings for an analysis or configuration. To open an existing database or new database while using the GUI:

- ❑ In the MMC, right click on the **Security Configuration and Analysis** node
- ❑ Select **Open Database**
- ❑ Enter the name of an existing database or a new database
- ❑ Click **Open**



NOTE: It is recommended that a new database be created for each analysis and configuration coupling.

Configuration files may be imported into the database by executing the following procedure:

- ❑ If a new database name was entered when opening a database, user will automatically be prompted to enter the configuration file to import. Otherwise:
- ❑ Right click on the **Security Configuration and Analysis** node in the left pane of the MMC
- ❑ Select **Import Template**
- ❑ In the **Import Template** dialog box, select the appropriate `inf` configuration file.
- ❑ Check the **Clear this database before importing** box to remove any previous settings stored in the database as illustrated in **Figure 7**.



NOTE: Import operations can append to or overwrite database information that has been previously imported. Appending is the default. If user does not want to combine templates in a configuration, check the “Clear this database before importing” checkbox to overwrite the current database.



WARNING: To avoid confusion and accidental combining of configurations, it is recommended that this option be checked every time a new analysis or configuration is performed.

- ❑ Click **Open**

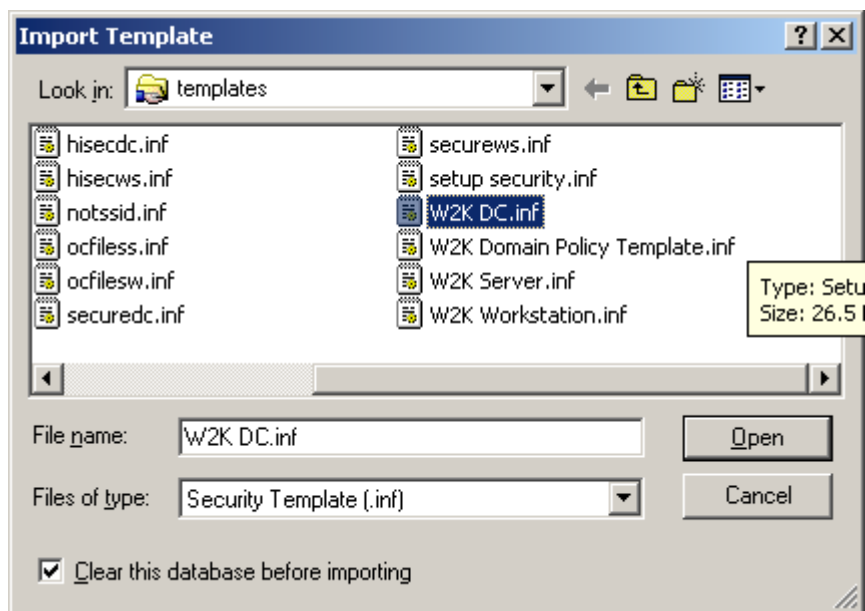




Figure 7 Configuration File Selection

Secedit Command Line Options

Secedit.exe, introduced in Chapter 1, is useful for performing security analyses and configurations via the command line and batch and/or scheduled programs. The command line syntax for secedit when used for system analysis or configuration is:

```
secedit {/analyze | /configure} [/cfg filename] [/db filename]
[/log LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]
```

Table 18 explains the parameter syntax for secedit.exe options.

Parameter	Description
/analyze	Performs an analysis
/configure	Performs a configuration
/cfg filename	Path to a configuration file that will be appended to the database prior to performing the analysis
/db filename	Path to the database that secedit will perform the analysis against. If this parameter is not specified, the last configuration/analysis database is used. If there is no previous database, %SystemRoot%\Security\Database\secedit.sdb is used.  NOTE: It is recommended that a new database be created for each analysis and configuration coupling.
/log LogPath	Path to log file for the process. If not provided, progress information is output to the console.  NOTE: Log information is appended to the specified log file. User must specify a new file name if a new log file is to be created.
/verbose	Specify detailed progress information




Parameter	Description
/quiet	Suppress screen and log output
/overwrite	<p>Overwrite the named database with the given configuration information.</p>  <p>NOTE: Configuration files can be appended to or overwrite database information that has been previously created. Appending is the default. Specify the /overwrite option to overwrite the current database.</p>  <p>WARNING: To avoid confusion and accidental combining of configurations, it is recommended that this option be included every time a new analysis or configuration is performed.</p>
/areas Areas	<p>Only relevant when using the /configure switch. Specifies the security areas to be processed. The following areas are available:</p> <p>SECURITYPOLICY - Local policy and domain policy for the system, including account policies, audit policies, etc.</p> <p>GROUP_MGMT - Restricted Group settings</p> <p>USER_RIGHTS - User rights assignments</p> <p>DSOBJECTS - Security on directory objects</p> <p>REGKEYS - Security permissions on local registry keys</p> <p>FILESTORE - Security permissions on local file system</p> <p>SERVICES - Security configuration for all defined services</p>  <p>NOTE: If the /areas switch is not used, the default is all security areas. If used, each area name should be separated by a space.</p>

Table 18 Secedit Command Line Parameters

Secedit has several other options available as well. These are detailed in

Parameter	Description
/export	Exports a stored template from a security database to a security template file
/refreshpolicy {machine_policy user_policy} {/enforce}	<p>Refreshes system security by reapplying the security settings to the Group Policy object (or Local Group Policy Object). The parameters available with this option are:</p> <p><i>machine_policy</i> – reapply machine-related settings; this option will be most used for security settings since the recommended settings are machine-specific</p> <p><i>user_policy</i> – reapply user-related settings</p> <p>/enforce – reapply settings regardless of whether they have changed</p>
/validate <filename>	Validates the syntax of a template to be imported into a database for analysis or configuration

Performing a Security Analysis

A security analysis is performed against a database. The configuration file(s) that have been imported into the database define the *baseline* for the analysis. Security settings within the configuration file(s) are compared to the current system security settings, and the results are stored back into a database. The baseline settings are presented alongside the current system settings. Configuration information can be modified as a

result of the analysis. The modified configuration information can be exported into a configuration file for subsequent use.

Performing a Security Analysis via the Command Line

To perform a security analysis via the command line, execute the following in a CMD prompt window:

```
❑ secedit /analyze [/cfg filename] [/db filename] [/log
    LogPath] [/verbose] [/quiet] [/overwrite] [>> results_file]
```

results_file is the name of a file to contain the analysis results. This is especially useful for reviewing the results at a later time. If the >> *results_file* is omitted, output will be written to the screen.

Performing a Security Analysis via the GUI

Figure 8 shows a sample result of a security analysis via the Security Configuration and Analysis snap-in. The following steps should be followed to perform a security analysis via the GUI:

- ❑ Right-click on the **Database** node
- ❑ Select **Analyze Computer Now...**
- ❑ In the **Perform Analysis** dialog box, enter the error log file path.



NOTE: Log information is appended to the specified log file. A new file name must be specified if a new log file is to be created.

- ❑ Click **OK**

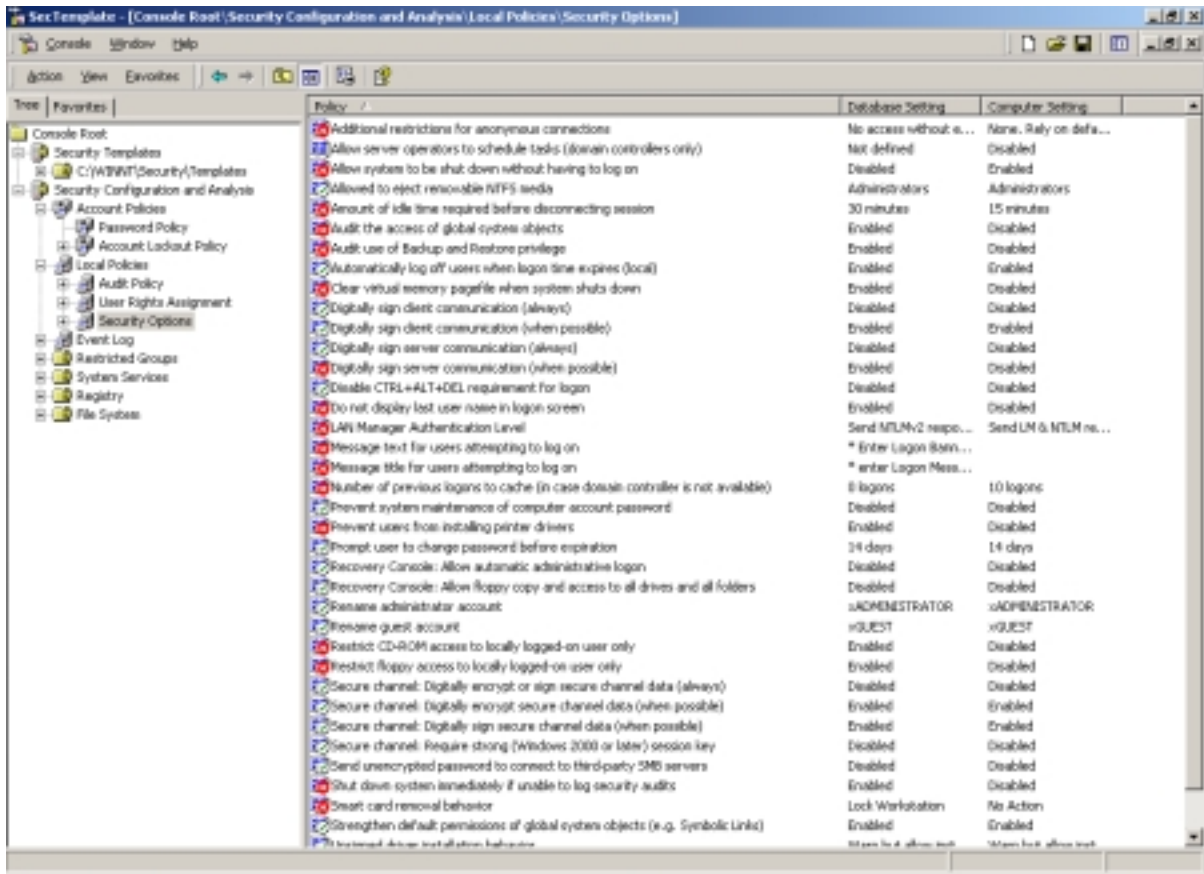


Figure 8 Results of a Security Analysis

Configuring a System

During configuration, errors may result if specific files or registry keys do not exist on the system, but exist in the `inf` configuration file. Do not be alarmed. The `inf` files attempt to cover many different scenarios and configurations that your system may or may not match.

Configuring a System via the Command Line

To configure all of the available security options at one time via the command line:

- ❑ `secdit /configure [/cfg filename] [/db filename] [/log LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]`



WARNING: Failure to enter a new database name each time a configuration is made or specify the `/overwrite` option may result in unpredictable behavior by `secdit`. For example, imported configuration files could get merged with other files and report unexpected analyses.

Following is an example of using the command line tool to configure only specific security areas:

- ❑ `secdit /configure /cfg "W2K workstation.inf" /db newdb.sdb /log logfile.txt /overwrite /areas REGKEYS FILESTORE`

This example will import the "W2K workstation.inf" file system and registry permission security settings and configure the local system.

Configuring a System via the GUI

The following steps should be followed to configure a system using the Security Configuration and Analysis snap-in:

- ❑ Right-click on the **Database** node
- ❑ Select **Configure Computer Now...**
- ❑ In the **Configure System** dialog box, enter the error log file path.



NOTE: Log information is appended to the specified log file. A new file name must be specified if a new log file is to be created.

- ❑ Click **OK**



NOTE: When a system is configured via the GUI, all settings in the template are applied. There is no option, as with `secedit.exe`, to specify that only parts of the template, e.g. file permissions or account policies, are to be applied.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Example Logon Banner

The DoD uses a standard warning banner that can be downloaded from the United States Navy INFOSEC Web Information Service <http://infosec.nosc.mil/infosec.html>. Select the text under the United States Department of Defense Warning Statement and copy it to the clipboard. This banner should resemble the following message:

"This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access), is provided only for authorized U. S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes."

Windows 2000 displays a message box with a caption and text that can be configured before a user logs on to the machine. The DoD requires organizations to use this message box to display a warning that notifies users that they can be held legally liable if they attempt to log on without authorization to use the computer. The absence of such a notice could be construed as an invitation, without restriction, to log on to the machine and browse the system.

References

- Ackerman, Pilar, et. al., *Microsoft Windows 2000 Professional Resource Kit*, Redmond, Washington: Microsoft Press, 2000.
- Bartock, Paul, Julie Haney, et. al., *Guide to Securing Microsoft Windows NT Networks version 4.1*, National Security Agency, September 2000.
- “Default Access Control Settings in Windows 2000,”
<http://www.microsoft.com/windows2000/techinfo/planning/security/secdefs.asp>,
Microsoft white paper, 2000.
- “Event ID 1000 and 1202 After Configuring Policies,” KB article Q260715
<http://support.microsoft.com/support/kb/articles/Q260/7/15.asp>,
Microsoft, 2000.
- “How to Use the RestrictAnonymous Registry Value in Windows 2000,” KB article Q246261
<http://support.microsoft.com/support/kb/articles/Q246/2/61.asp>,
Microsoft, 2000.
- McLean, Ian, *Windows 2000 Security Little Black Book*, Scottsdale, Arizona: Coriolis Group, 2000.
- Microsoft Technet, <http://www.microsoft.com/technet>.
- “OFF2000: ‘Installation Ended Prematurely Because of an Error’ When You Run Office Setup,”
KB article Q230895 <http://support.microsoft.com/support/kb/articles/Q230/8/95.asp>,
Microsoft, 2000
- Russel, Charlie and Sharon Crawford, *Microsoft Windows 2000 Server Administrator’s Companion*, Redmond, Washington: Microsoft Press, 2000.
- “Security Configuration Toolset,”
<http://www.microsoft.com/windows2000/techinfo/howitworks/security/sctoolset.asp>,
Microsoft white paper, 2000.
- Smith, Randy Franklin, “Dangerous Services,” Windows IT Security web site,

UNCLASSIFIED

<http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16301>, Dec. 7, 2000.

“SNMP Parameters Vulnerability,” KB article Q266794

<http://www.microsoft.com/technet/support/kb.asp?ID=266794>,

Microsoft, December 2000.

“Step-by-Step Guide to Using the Security Configuration Tool Set,”

<http://www.microsoft.com/windows2000/library/planning/security/secconfsteps.asp>,

Microsoft, February 2000