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

Author: Julie M. Haney

Updated: July 22, 2002
Version 1.1.1

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

W2KGuides@nsa.gov
### Change Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>22 Jan. 2002</td>
<td>Added this change control section to track version modifications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On pp. 19 and 23, removed references to a “companion CD.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Chapter 2, renamed the section “Undoing Security Changes” to “Before Making Security Changes” and moved the section to before the “Checklist for Applying the Recommendations in this Guide” section. In this same section changed “(described later)” to “(described in Chapter 10).”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 23, added the line “ENPASFLT.DLL is available to U.S. government agencies only” under the “Passwords must meet complexity requirements” table entry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 25 under the Account Lockout Policy section, changed “thousands of well-known passwords are tried” to “thousands of words are tried.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 26, changed “Maximum lifetime for user ticket removal” to “Maximum lifetime for user ticket renewal.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 30, added the “ENTERPRISE DOMAIN CONTROLLERS” group to the “Access this computer from network” user right.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 37, under the table entry for “Allow Server Operators to schedule tasks,” corrected the registry entry to be HKLM\System\CurrentControlSet\Control\Lsa\SubmitControl=0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 54, under the Maximum log size table entry, changed the last sentence in the note to read “This ensures that the system will still halt if the event log exceeds 4 GB, even if there is space on the hard drive.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 84, moved the incorrect entry for %SystemRoot%\Program Files\Resource Pro Kit to page 80, %ProgramFiles%\Resource Pro Kit.</td>
</tr>
<tr>
<td>1.1.1</td>
<td>22 July 2002</td>
<td>On page 41, under the “LAN Manager authentication leve” entry, added “Send NTLMv2 response only — System will still accept LM and NTLM.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 48, under the “Send unencrypted password to connect to third-party SMB servers” entry, corrected the registry path to be HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 70, corrected the security setting for \MACHINE\SYSTEM\CurrentControlSet\Control\Wmi\Security to be Full Control for the Administrators group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 71, corrected the security setting for USERS.DEFAULT to read Users instead of Authenticated Users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On page 80, changed the description of %SystemDirectory%\rcp.exe to read “Remote copy command.”</td>
</tr>
</tbody>
</table>
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.
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

Change Control ........................................................................................................................................... ii
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
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
Before Making Security Changes .......................................................................................................... 19
Checklist for Applying the Recommendations in this Guide .............................................................. 19

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
Table of Contents

Managing the Event Logs ........................................................................................................................ 54

Chapter 6 Managing Restricted Groups with Security Templates .......................................................... 57
  Modifying Restricted Groups via the Security Templates Snap-in ....................................................... 57

Chapter 7 Managing System Services with Security Templates .......................................................... 59
  Modifying System Services via the Security Templates Snap-in ....................................................... 59
  System Services Security ..................................................................................................................... 60

Chapter 8 Modifying Registry Security Settings with Security Templates ............................................. 63
  Inheritance model ............................................................................................................................... 63
  Registry permissions ............................................................................................................................ 63
  Modifying Registry settings via the Security Templates snap-in ....................................................... 65
  Recommended Registry Key Permissions .......................................................................................... 67

Chapter 9 Modifying File System Security Settings with Security Templates ....................................... 73
  File and folder permissions ............................................................................................................... 73
  Modifying File System settings via the Security Template snap-in ..................................................... 76
  Recommended File and Folder Permissions ....................................................................................... 78

Chapter 10 Security Configuration and Analysis .................................................................................. 87
  Loading the Security Configuration and Analysis snap-in into the MMC ......................................... 87
  Security Configuration Databases ....................................................................................................... 88
  Seccedit Command Line Options ..................................................................................................... 89
  Performing a Security Analysis .......................................................................................................... 90
  Configuring a System ......................................................................................................................... 92

Appendix A Example Logon Banner ..................................................................................................... 95

Appendix B References .......................................................................................................................... 96
# Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Templates snap-in</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>Password Policy Recommended Settings</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>Recommended User Rights</td>
<td>29</td>
</tr>
<tr>
<td>4</td>
<td>System Services</td>
<td>60</td>
</tr>
<tr>
<td>5</td>
<td>Advanced Registry Permissions Dialog Box</td>
<td>66</td>
</tr>
<tr>
<td>6</td>
<td>File/Folder Permission Inheritance Options</td>
<td>79</td>
</tr>
<tr>
<td>7</td>
<td>Configuration File Selection</td>
<td>89</td>
</tr>
<tr>
<td>8</td>
<td>Results of a Security Analysis</td>
<td>92</td>
</tr>
</tbody>
</table>
Table of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Default Security Configuration Files</td>
<td>18</td>
</tr>
<tr>
<td>Table 2</td>
<td>Enhanced Security Configuration Files</td>
<td>19</td>
</tr>
<tr>
<td>Table 3</td>
<td>Password Policy Options</td>
<td>23</td>
</tr>
<tr>
<td>Table 4</td>
<td>Account Lockout Options</td>
<td>25</td>
</tr>
<tr>
<td>Table 5</td>
<td>Kerberos Policy Options</td>
<td>26</td>
</tr>
<tr>
<td>Table 6</td>
<td>Audit Policy Options</td>
<td>28</td>
</tr>
<tr>
<td>Table 7</td>
<td>User Rights Options</td>
<td>35</td>
</tr>
<tr>
<td>Table 8</td>
<td>Security Options</td>
<td>50</td>
</tr>
<tr>
<td>Table 9</td>
<td>Domain-wide Security Options</td>
<td>50</td>
</tr>
<tr>
<td>Table 10</td>
<td>Event Log Options</td>
<td>54</td>
</tr>
<tr>
<td>Table 11</td>
<td>Registry Permissions and Descriptions</td>
<td>64</td>
</tr>
<tr>
<td>Table 12</td>
<td>Registry Permission Options</td>
<td>64</td>
</tr>
<tr>
<td>Table 13</td>
<td>Recommended Registry Permissions</td>
<td>71</td>
</tr>
<tr>
<td>Table 14</td>
<td>File Permissions and Descriptions</td>
<td>74</td>
</tr>
<tr>
<td>Table 15</td>
<td>Folder Permissions Options</td>
<td>75</td>
</tr>
<tr>
<td>Table 16</td>
<td>File Permissions Options</td>
<td>76</td>
</tr>
<tr>
<td>Table 17</td>
<td>Recommended File Permissions</td>
<td>86</td>
</tr>
<tr>
<td>Table 18</td>
<td>Secedit Command Line Parameters</td>
<td>90</td>
</tr>
</tbody>
</table>
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).
- 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.
Chapter 1 - Important Information on Using this Guide

- 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
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 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.

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 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.
Chapter 1 - Important Information on Using this Guide

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.
Chapter 2 – 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.

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.

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.
Chapter 2 – Introduction to the Security Configuration Tool Set

- 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.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defltdc.inf</td>
<td>Windows 2000 Server/Advanced Server Domain Controller</td>
</tr>
<tr>
<td>Defltsv.inf</td>
<td>Windows 2000 Server/Advanced Server</td>
</tr>
<tr>
<td>Defltwk.inf</td>
<td>Windows 2000 Professional</td>
</tr>
</tbody>
</table>

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).
### Table 2 Enhanced Security Configuration Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>W2K Server.inf</td>
<td>Windows 2000 Server/Advanced Server</td>
<td>Enhanced security settings for Windows 2000 member or standalone servers</td>
</tr>
<tr>
<td>W2K Domain Policy</td>
<td>Windows 2000 domain</td>
<td>Enhanced account policy settings to be applied in a domain-level Group Policy Object</td>
</tr>
</tbody>
</table>

### Before Making 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 in Chapter 10) 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.

### 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.

- Download the appropriate configuration files (the .INF files available on the website www.nsa.gov) 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.
Several new security options have been added to the NSA templates. To make these options available, download the NSA \sceregvl.inf file from the website into the %SystemRoot%\inf folder. You should rename the original copy of \sceregvl.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.
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.

<table>
<thead>
<tr>
<th>Password Policy Options</th>
<th>Recommended Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enforce password history</strong></td>
<td>24 Passwords</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Password Age</strong></td>
<td>90 days</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Minimum Password Age</strong></td>
<td>1 Day</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Minimum Password Length</strong></td>
<td>12 Characters</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**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.

**NOTE:** It is recommended that privileged users (such as administrators) have passwords longer than 12 characters if possible.
**Password Policy Options**

<table>
<thead>
<tr>
<th>Passwords must meet complexity requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. Complexity requirements will take effect the next time a user changes his password. Already-existing passwords will not be affected.</td>
</tr>
</tbody>
</table>

NOTE: NSA provides an enhanced password complexity filter, `ENPASFLT.DLL`, that can be used in place of the Microsoft-provided `PASSFILT.DLL`. `ENPASFLT.DLL` is available to U.S. government agencies only. 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 `PASSFILT`, you may want to set this option to “Disabled” to avoid conflicts between the two DLLs.

<table>
<thead>
<tr>
<th>Store password using reversible encryption for all users in the domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

**Recommended Settings**

<table>
<thead>
<tr>
<th>Passwords must meet complexity requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Store password using reversible encryption for all users in the domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
</tr>
</tbody>
</table>
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 words are tried. If the account is locked out after each invalid attempt to logon, the attacker 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.

<table>
<thead>
<tr>
<th>Account Lockout Policy Options</th>
<th>Recommended Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account lockout duration</strong></td>
<td>15 minutes</td>
</tr>
<tr>
<td>Sets the number of minutes an account will be locked out. Allowable values are 0 (account is locked out until administrator unlocks it) or between 1 and 99999 minutes.</td>
<td></td>
</tr>
<tr>
<td><strong>WARNING:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Account lockout threshold</strong></td>
<td>3 Invalid logon attempts</td>
</tr>
<tr>
<td>Prevents brute-force password cracking/guessing attacks on the system.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> Failed logons on machines that have been locked via CTRL-ALT-DEL or a password-protected screen saver do not count as failed attempts.</td>
<td></td>
</tr>
<tr>
<td><strong>Reset account lockout counter after</strong></td>
<td>15 minutes</td>
</tr>
<tr>
<td>Sets the number of minutes until the invalid logon count is reset. Allowable values range from 1 to 99999 minutes.</td>
<td></td>
</tr>
</tbody>
</table>

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).

<table>
<thead>
<tr>
<th>Kerberos Policy Options</th>
<th>Recommended Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce user logon restrictions</td>
<td>Enabled</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Maximum lifetime for service ticket</td>
<td>600 minutes</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Maximum lifetime for user ticket</td>
<td>10 hours</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Maximum lifetime for user ticket renewal</td>
<td>7 days</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Maximum tolerance for computer clock synchronization</td>
<td>5 minutes</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

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.
## Chapter 4 – Modifying Local Policy Settings with Security Templates

### Audit Policy Options

<table>
<thead>
<tr>
<th>Audit Policy Options</th>
<th>Recommended Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit account logon events</strong></td>
<td>Tracks user logon events on other computers in which the local computer was used to authenticate the account.</td>
</tr>
<tr>
<td><strong>Audit account management</strong></td>
<td>Tracks changes to the Security Account database (i.e., when accounts are created, changed, or deleted).</td>
</tr>
<tr>
<td><strong>Audit directory service access</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Audit logon events</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Audit object access</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Audit policy change</strong></td>
<td>Tracks changes in security policy, such as assignment of privileges or changes in the audit policy.</td>
</tr>
<tr>
<td><strong>Audit privilege use</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Audit process tracking</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Audit system events</strong></td>
<td>Tracks events that affect the entire system or the Audit log. Records events such as restart or shutdown.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Access this computer from network</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to connect over the network to the computer.</td>
<td>Administrators Users</td>
<td>Administrators Authenticated Users (DCs only) ENTERPRISE DOMAIN CONTROLLERS (DCs only) Users (Member Servers only)</td>
</tr>
<tr>
<td><strong>NOTE:</strong> 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 &lt;machine_name&gt; and IWAM_&lt;machine_name&gt; 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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Act as part of the operating system</th>
<th>(No one)</th>
<th>(No one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Add workstations to domain</th>
<th>(No one)</th>
<th>(No one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> 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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Back up files and directories</th>
<th>Administrators</th>
<th>Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to back up files and directories. This right supersedes file and directory permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> If the network makes use of the Backup Operators or similar group, also assign this right to that group.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bypass traverse checking</th>
<th>Users</th>
<th>Authenticated Users (DCs only) Users (Member Servers only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Rights</td>
<td>Windows 2000 Workstations</td>
<td>Windows 2000 Domain Controllers and Member Servers</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Change the system time</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allows a user to set the time for the internal clock of the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create a pagefile</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allows a user to create new pagefiles for virtual memory swapping and change the size of a pagefile.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create a token object</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create permanent shared objects</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>Allows a user to create special permanent directory objects, such as \Device, that are used within the Windows 2000 object manager.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debug programs</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>Allows a user to debug various low-level objects such as threads.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOTE: Software developers working on the system may need this right. Assign the right to developer users/groups only when necessary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deny access to this computer from the network</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>Prevents specific users and/or groups from accessing the computer via the network. This setting supersedes the “Access this computer from the network” setting if an account is subject to both policies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deny logon as a batch job</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>Prevents specific users and/or groups from logging on as a batch job. This setting supersedes the “Logon as a batch job” setting if an account is subject to both policies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deny logon as a service</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>Prevents specific service accounts from registering a process as a service. This setting supersedes the “Log on as a service” setting if an account is subject to both policies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deny logon locally</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>Prevents specific users and/or groups from logging on directly at the computer. This setting supersedes the “Log on locally” setting if an account is subject to both policies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable computer and user accounts to be trusted for delegation</td>
<td>(No one)</td>
<td>Administrators (domain controllers)</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td>(No one) (member servers)</td>
</tr>
</tbody>
</table>
### User Rights

<table>
<thead>
<tr>
<th>User Right</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Force shutdown from a remote system</strong></td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allows a user to shutdown a Windows 2000 system remotely over a network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Generate security audits</strong></td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>Allows a process to generate security audit log entries.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Increase quotas</strong></td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allows a user to increase the processor quota assigned to a process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Increase scheduling priority</strong></td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allows a user to boost the execution priority of a process. This can be performed via the Task Manager user interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Load and unload device drivers</strong></td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allows a user to install and remove device drivers. This right is necessary for Plug and Play device driver installation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Lock pages in memory</strong></td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOTE: This right is obsolete in this version of Windows 2000.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Log on as a batch job</strong></td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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_&lt;machine_name&gt; and IWAM_&lt;machine_name&gt; 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 &quot;Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0&quot; for information on a workaround for this issue.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### User Rights

<table>
<thead>
<tr>
<th>Log on as a service</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a process to register with the system as a service.</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
<tr>
<td>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. WARNING: The provided template files will remove all users/groups from this right unless you modify the setting.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Log on locally</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Administrators Users</td>
<td>Administrators</td>
</tr>
<tr>
<td>NOTE: If the system is an IIS 5.0 Server, the IUSR_&lt;machine_name&gt; and IWAM_&lt;machine_name&gt; accounts (or whatever account has been designated as the anonymous web user) must be assigned this right. NOTE: If the network makes use of the Backup Operators or similar group, also assign this right to that group.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 4 – Modifying Local Policy Settings with Security Templates

**User Rights**

<table>
<thead>
<tr>
<th>Manage auditing and security log</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

**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.

**WARNING:** If running Exchange 2000 on the network, the Exchange Enterprise Servers group must be assigned this user right on domain controllers.

<table>
<thead>
<tr>
<th>Modify firmware environment variables</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profile single process</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to perform profiling (performance sampling) on a process.</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

**NOTE:** Software developers working on the system may need this right. Assign the right to developer users/groups only when necessary.

<table>
<thead>
<tr>
<th>Profile system performance</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to perform profiling (performance sampling) on the system.</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remove computer from docking station</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to undock a laptop from a docking station.</td>
<td>Administrators Users</td>
<td>(No one)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replace a process-level token</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to modify a process’s security access token. This is a powerful right used only by the system.</td>
<td>(No one)</td>
<td>(No one)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Restore files and directories</th>
<th>Windows 2000 Workstations</th>
<th>Windows 2000 Domain Controllers and Member Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows a user to restore backed-up files and directories. This right supercedes file and directory permissions.</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

**NOTE:** If the network makes use of the group to Restore backups, also assign this right to that group.
User Rights

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

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

<table>
<thead>
<tr>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
</table>

#### Additional restrictions for anonymous connections

Places restrictions on anonymous users. The options are:

- **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.

- **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.

- **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.

  **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](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).

- **HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous = 2**

#### Allow Automatic Administrator Logon

Allows a system to automatically logon as an administrator when the machine is started. By default, this setting is disabled.

**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.

- **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon = 0**

  **Disabled**

  **Disabled**
<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow Server Operators to schedule tasks (domain controllers only)</strong></td>
<td>Not defined</td>
<td>Disabled</td>
</tr>
<tr>
<td>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:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Disabled</strong></td>
<td>Only allow Administrators to schedule tasks</td>
<td></td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Allow Administrators and Server Operators to schedule tasks</td>
<td></td>
</tr>
<tr>
<td><strong>HKLM\System\CurrentControlSet\Control\Lsa\SubmitControl= 0</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Allow system to be shut down without having to log on</strong></td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon = 0</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Allowed to eject removable NTFS media</strong></td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>By default, only Administrators are allowed to eject removable NTFS media. This setting allows for the following options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Administrators</strong></td>
<td>Administrators and Power Users</td>
<td></td>
</tr>
<tr>
<td><strong>Administrators and Interactive Users</strong></td>
<td>Administrators and Power Users</td>
<td></td>
</tr>
<tr>
<td><strong>HKLM\Software\Microsoft\Windows NT\CurrentVersion\winlogon\AllocateDASD = 0</strong></td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td><strong>Amount of idle time required before disconnecting session</strong></td>
<td>30 minutes</td>
<td>30 minutes</td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect = 15</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Security Attribute

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit the access of global system objects</strong>&lt;br&gt;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, <strong>Audit Object Access</strong> must be enabled under auditing.</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Audit use of Backup and Restore privilege</strong>&lt;br&gt;Enables auditing of all user rights in conjunction with <strong>Audit Privilege Use</strong> auditing being enabled. If this option is disabled, the Backup and Restore rights will not be audited even if <strong>Audit Privilege Use</strong> is enabled.</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Automatically log off users when logon time expires</strong>&lt;br&gt;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.</td>
<td>Not Defined</td>
<td>Not defined</td>
</tr>
<tr>
<td><strong>Automatically log off users when logon time expires (local)</strong>&lt;br&gt;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.</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Clear virtual memory pagefile when system shuts down</strong>&lt;br&gt;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 (hiberfil.sys) to be cleared when hibernation is disabled on a laptop system.</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**HKLM\System\CurrentControlSet\Control\Lsa\AuditBaseObjects = 1**

**HKLM\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing = 1**

**HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogoff = 1**

**HKLM\CurrentControlSet\Control\SessionManager\MemoryManagement\ClearPageFileAtShutdown = 1**
### Security Attribute

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digitally sign client communication (always)</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOTE: To use SMB digital signing, this option must be enabled on both the SMB client and server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature = 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitally sign client communication (when possible)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature = 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitally sign server communication (always)</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOTE: To use SMB digital signing, this option must be enabled on both the SMB client and server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\RequireSecuritySignature = 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitally sign server communication (when possible)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\EnableSecuritySignature = 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Security Attribute

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable CTRL+ALT+DEL requirement for logon</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

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.

HKLM:Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD = 0

### Disable Media Autoplay

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:

#### CDROM drives

Disables autorun on CDROMs. Registry value = 0x00000095

#### All drives

Disables autorun on all media. Registry value = 0x000000FF

**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.

**NOTE:** CDROM autoplay/autorun can also be disabled by setting the registry value

HKLM\System\CurrentControlSet\Services\Cdrom\AutoRun = 0

HKLM:Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun = 0

All Drives | All Drives
### Security Attribute

**Do not display last user name in logon screen**

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.

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUsername= 1

---

### Recommended Security Setting For Workstations and Member Servers

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not display last user name in logon screen</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

---

### LAN Manager authentication level

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:

- **Send LM & NTLM responses** - Registry value = 0.
- **Send LM & NTLM – use NTLMv2 session security if negotiated** - Registry value = 1.
- **Send NTLM response only** - Registry value = 2.
- **Send NTLMv2 response only** - System will still accept LM and NTLM. Registry value = 3.
- **Send NTLMv2 response only\refuse LM** - Registry value = 4.
- **Send NTLMv2 response only\refuse LM & NTLM** - Registry value = 5.

---

**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/Q272/129.ASP](http://support.microsoft.com/support/kb/articles/Q272/129.ASP)

**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...
<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows for Workgroups® or only NTLM (Windows NT 4.0 prior to Service Pack 4). The Active Directory Services client may be installed on Windows 9x machines to allow for NTLMv2 security.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel = 5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Security Attribute

<table>
<thead>
<tr>
<th>Message text for users attempting to log on</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText = &quot;Text you want displayed&quot;</td>
<td>&lt;Configure locally - see Appendix for sample&gt;</td>
<td>&lt;Configure locally - see Appendix for sample&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message title for users attempting to log on</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption = &quot;Text you want displayed on title bar&quot;</td>
<td>&lt;Configure locally - see Appendix for sample&gt;</td>
<td>&lt;Configure locally - see Appendix for sample&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of previous logons to cache (in case domain controller is not available)</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. 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. WARNING: Not having cached logons may slow down the authentication process. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount = 0</td>
<td>0 logons</td>
<td>0 logons</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prevent system maintenance of computer account password</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>By default, computer account passwords are changed every seven days. Enabling this option prevents machines from requesting a weekly password change. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange = 0</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
### Security Attribute

<table>
<thead>
<tr>
<th>Prevent users from installing printer drivers</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevents members of the users group from adding printer drivers on the local machine.</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Users can still connect to Network Print shares to which they have permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WARNING:</strong> After enabling this option, users will not be able to add printers that have not been previously installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers = 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prompt user to change password before expiration</th>
<th>14 days</th>
<th>14 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets how far in advance users are warned that their passwords will expire.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning = 14</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recovery Console: Allow automatic administrative logon</th>
<th>Disabled</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>If this option is enabled, the Recovery Console will not prompt for an administrator password and will automatically log on to the system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel = 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recovery Console: Allow floppy copy and access to all drives and folders</th>
<th>Disabled</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables the Recovery Console SET command, which allows setting of console environment variables such as AllowWildCards, AllowAllPaths, AllowRemovableMedia, and NoCopyPrompt.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand = 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Rename administrator account
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.

**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.

**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](http://support.microsoft.com/support/kb/articles/Q260/7/15.asp) for more information.

### Rename guest Account
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.

**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.
### Security Attribute

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Restrict CD-ROM access to locally logged on user only</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRom = 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:

- Install the software from across the network
  - Or
- Copy the contents of the CD to the hard drive, then install
  - Or
- Temporarily disable this setting, install the software, then re-enable it.

For more information, refer to KB Article Q230895

http://support.microsoft.com/support/kb/articles/Q230/8/95.asp

### Restrict floppy access to locally logged on user only

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.

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRom = 1

**Recommended Security Setting For Workstations and Member Servers**

- Enabled

**Recommended Security Setting For Domain Controllers**

- Enabled
### Security Attribute

<table>
<thead>
<tr>
<th>Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>CurrentVersion\Winlogon\AllocateFloppies = 1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Secure channel: Digitally encrypt or sign secure channel data (always)**

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.

**NOTE:** ALL domain controllers in ALL trusted domains must support digital encryption and signing if this option is enabled.

HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignorSeal = 0

**Secure channel: Digitally encrypt secure channel data (when possible)**

Enables a computer to digitally encrypt secure channel data. See the explanation of secure channel communication in the previous option.

If this option is enabled, all outgoing secure channel traffic should be encrypted.

HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel = 1

**Secure channel: Digitally sign secure channel data (when possible)**

Enables a computer to digitally sign secure channel data. See the explanation of secure channel communication in the previous option.

If this option is enabled, all outgoing secure channel traffic should be signed.

**NOTE:** If Digitally encrypt secure channel data (when possible) is enabled, it will override any setting for this option and automatically enable it.

HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel = 1

<table>
<thead>
<tr>
<th>Secure channel: Digitally encrypt or sign secure channel data (always)</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure channel: Digitally encrypt secure channel data (when possible)</th>
<th>Enables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure channel: Digitally sign secure channel data (when possible)</th>
<th>Enables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
### Security Attribute

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure channel: Require strong (Windows 2000 or later) session key</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Requires strong encryption keys for all outgoing secure channel communications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option should be enabled only if ALL domain controllers in ALL trusted domains also support strong session keys.</td>
<td>HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey = 0</td>
<td></td>
</tr>
<tr>
<td>Secure system partition (for RISC platforms only)</td>
<td>Not defined</td>
<td>Not defined</td>
</tr>
<tr>
<td>Restricts access of the RISC system partition (which is FAT) to administrators only when the operating system is running.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send unencrypted password to connect to third-party SMB servers</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>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.</td>
<td>HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword = 0</td>
<td></td>
</tr>
</tbody>
</table>
### Security Attribute

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Security Setting For Workstations and Member Servers</th>
<th>Recommended Security Setting For Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shut down system immediately if unable to log security audits</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>If events cannot be written to the security log, the system is halted immediately.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If the system halts as a result of a full log, an administrator must log onto the system and clear the log.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> Before clearing the security log, save the data to disk.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WARNING:</strong> 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail = 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart card removal behavior</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Determines the action taken when a smart card for a logged-on user is removed from the smart card reader. Options are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>No action</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Lock Workstation</strong></td>
<td>Lock Workstation</td>
<td>Lock Workstation</td>
</tr>
<tr>
<td>Users can remove their smart card, leave the area, then return to their same session at a later time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Force Logoff</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users are automatically logged off when the card is removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption = 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strengthen default permissions of global system objects (e.g., Symbolic Links)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\Software\CurrentControlSet\Session Manager\ProtectionMode = 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4 – Modifying Local Policy Settings with Security Templates

### Security Attribute

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

#### 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**.

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically log off users when logon time expires</td>
<td>Enabled</td>
</tr>
<tr>
<td>Rename Administrator account</td>
<td>&lt;Configure Locally&gt;</td>
</tr>
<tr>
<td>Rename Guest Account</td>
<td>&lt;Configure Locally&gt;</td>
</tr>
</tbody>
</table>

#### 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` (where `%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`
Chapter 4 – Modifying Local Policy Settings with Security Templates

- **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_MULTI_SZ (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 `sceregvl.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 `sceregvl.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 `sceregvl.inf` file and re-registering the DLL. To ensure that options are permanently deleted from the templates, perform the following actions:

- Open `sceregvl.inf` in a text editor (e.g. Notepad)
- Delete the specific security option from the `sceregvl.inf` file under the [Register Registry Values] section
- Under the `sceregvl.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 `sceregvl.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 `sceregvl.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.
Chapter 4 – Modifying Local Policy Settings with Security Templates

This Page Intentionally Left Blank
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.
Chapter 5 – Modifying Event Log Settings with Security Templates

Event Log Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Recommended Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum application log size</td>
<td>4194240 KBytes</td>
</tr>
<tr>
<td>Maximum security log size</td>
<td></td>
</tr>
<tr>
<td>Maximum system log size</td>
<td></td>
</tr>
<tr>
<td>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. 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 ensures that the system will still halt if the event log exceeds 4 GB, even if there is space on the hard drive.</td>
<td></td>
</tr>
</tbody>
</table>

Restrict guest access to application Log
Restrict guest access to security Log
Restrict guest access to system Log
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.

Retain application log
Retain security log
Retain system log
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.

Retention method for application Log
Retention method for security Log
Retention method for system Log
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.

Shut down the computer when the security audit log is full
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.

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.

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
**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 to 1.
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
Chapter 6 – Managing Restricted Groups with Security Templates

- 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.

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.
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.
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…
Chapter 8 – Modifying Registry Security

Settings with Security Templates

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.

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

**Table 11 Registry Permissions and Descriptions**

<table>
<thead>
<tr>
<th>Special Permissions</th>
<th>Full Control</th>
<th>Read</th>
<th>Write</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Value</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set Value</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Create Subkey</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Enumerate Subkeys</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Notify</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Create Link</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Write DAC</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write Owner</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Control</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**Table 12 Registry Permission Options**
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.
Chapter 8 – Modifying Registry Security Settings with Security Templates

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 (hisecws.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

<table>
<thead>
<tr>
<th>REGISTRY KEY</th>
<th>USER GROUPS</th>
<th>RECOMMENDED PERMISSIONS</th>
<th>INHERIT METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASSES_ROOT:</td>
<td>Administrators</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>CREATOR OWNER</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MACHINE:SOFTWARE</td>
<td>Administrators</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>CREATOR OWNER</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MACHINESOFTWARE:Microsoft'NetDDE</td>
<td>Administrators</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>CREATOR OWNER</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MACHINE:SOFTWARE:Machinesoftware:OS/2SubsystemforNT</td>
<td>Administrators</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>CREATOR OWNER</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MACHINE:SOFTWARE:Microsoft:ProtectedStorageSystemProvider</td>
<td>Ignore</td>
<td>Ignore</td>
<td>Ignore</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MACHINE:SOFTWARE:Microsoft:WindowsNT:CurrentVersion:AstrCommands</td>
<td>Administrators Backup Operators</td>
<td>Full Control, Query, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>CREATOR OWNER</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MACHINE:SOFTWARE:Microsoft:WindowsNT:CurrentVersion:Perflib</td>
<td>Administrators INTERACTIVE</td>
<td>Full Control, Read</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>CREATOR OWNER</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** If not using the Backup Operators group, remove the group from these permissions.
<table>
<thead>
<tr>
<th>REGISTRY KEY</th>
<th>USER GROUPS</th>
<th>RECOMMENDED PERMISSIONS</th>
<th>INHERIT METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies</td>
<td>Administrators, Authenticated Users, SYSTEM</td>
<td>Full Control, Read, Full Control</td>
<td>Propagate</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset001</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control (Subkeys only), Full Control, Read</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset002</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control (Subkeys only), Full Control, Read</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset003</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control (Subkeys only), Full Control, Read</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset004</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control (Subkeys only), Full Control, Read</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset005</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control (Subkeys only), Full Control, Read</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset006</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control (Subkeys only), Full Control, Read</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset007</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control (Subkeys only), Full Control, Read</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REGISTRY KEY</td>
<td>USER GROUPS</td>
<td>RECOMMENDED PERMISSIONS</td>
<td>INHERIT METHOD</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>-------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset008</td>
<td>Administrators CREATOR OWNER SYSTEM Users</td>
<td>Full Control Full Control (Subkeys only) Full Control Read</td>
<td>Propagate</td>
</tr>
<tr>
<td></td>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset009</td>
<td>Administrators CREATOR OWNER SYSTEM Users</td>
<td>Full Control Full Control (Subkeys only) Full Control Read</td>
<td>Propagate</td>
</tr>
<tr>
<td></td>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\controlset010</td>
<td>Administrators CREATOR OWNER SYSTEM Users</td>
<td>Full Control Full Control (Subkeys only) Full Control Read</td>
<td>Propagate</td>
</tr>
<tr>
<td></td>
<td>Contains a control set that may be used to start and run Windows 2000.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg</td>
<td>Administrators Backup Operators SYSTEM</td>
<td>Full Control Read (Key only) Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: If not using the Backup Operators group, remove the group from these permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\CurrentControlSet\Control\Wmi\Security</td>
<td>Administrators CREATOR OWNER SYSTEM</td>
<td>Full Control Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>Security settings for the Windows Management Instrumentation (WMI). WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\MACHINE\SYSTEM\CurrentControlSet\Enum</td>
<td>Ignore</td>
<td>Ignore</td>
<td>Ignore</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Chapter 8 – Modifying Registry Security Settings with Security Templates

### Table 13 Recommended Registry Permissions

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>User Groups</th>
<th>Recommended Permissions</th>
<th>Inherit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles</code></td>
<td>Administrators, Creator, Owner, System, Users</td>
<td>Full Control, Full Control (Subkeys only), Full Control, Read</td>
<td>Propagate</td>
</tr>
<tr>
<td><code>\MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers</code></td>
<td>Administrators, Creator, Owner, System</td>
<td>Full Control, Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td><code>\MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities</code></td>
<td>Administrators, Creator, Owner, System</td>
<td>Full Control, Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td><code>USERS\.DEFAULT</code></td>
<td>Administrators, Users, Creator, Owner, System</td>
<td>Full Control, Read, Full Control (Subkeys only), Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td><code>USERS\.DEFAULT\Software\Microsoft\NetDDE</code></td>
<td>Administrators, System</td>
<td>Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td><code>USERS\.DEFAULT\Software\Microsoft\Protected Storage Systems Provider</code></td>
<td>Ignore</td>
<td>Ignore</td>
<td>Ignore</td>
</tr>
</tbody>
</table>


NB: These settings 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).
This Page Intentionally Left Blank
Chapter 9

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

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traverse Folder/Execute File</td>
<td><strong>Traverse Folder</strong> 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 <strong>Execute File</strong> permission allows a user to run program files (files only).</td>
</tr>
<tr>
<td>List Folder/Read Data</td>
<td><strong>List Folder</strong> allows the reading of file names and subfolders within a folder (folders only). <strong>Read Data</strong> allows file data to be read (files only).</td>
</tr>
<tr>
<td>Read Attributes</td>
<td>Allows viewing of a file’s NTFS attributes (e.g., “Read only” or “Hidden”).</td>
</tr>
<tr>
<td>Read Extended Attributes</td>
<td>Allows viewing of a file’s extended attributes. Extended attributes may vary as they are defined by specific programs.</td>
</tr>
<tr>
<td>Create Files/Write Data</td>
<td><strong>Create Files</strong> allows the creation of files within a folder (folders only). <strong>Write Data</strong> allows modification and/or overwriting of files (files only).</td>
</tr>
<tr>
<td>Create Folders/Append Data</td>
<td><strong>Create Folders</strong> allows the creation of folders within a folder (folders only). <strong>Append Data</strong> allows making changes to the end of file (files only).</td>
</tr>
<tr>
<td>Write Attributes</td>
<td>Allows the modification of a file’s NTFS attributes (e.g., “Read only” or “Hidden”).</td>
</tr>
<tr>
<td>Write Extended Attributes</td>
<td>Allows the modification of a file’s program-specific extended attributes.</td>
</tr>
<tr>
<td>Delete Subfolders and Files</td>
<td>Allows the deletion of subfolders and files regardless if the Delete permission was granted on the subfolder or file.</td>
</tr>
<tr>
<td>Delete</td>
<td>Allows deletion of a file or folder.</td>
</tr>
<tr>
<td>Read Permissions</td>
<td>Allows viewing of the permissions on a file or folder.</td>
</tr>
<tr>
<td>Change Permissions</td>
<td>Allows the modification of the permissions on a file or folder.</td>
</tr>
<tr>
<td>Take Ownership</td>
<td>Allows taking ownership of a file or folder.</td>
</tr>
</tbody>
</table>

**Table 14 File Permissions and Descriptions**
**Folder Permissions:**

<table>
<thead>
<tr>
<th>Special Permissions</th>
<th>Full Control</th>
<th>Modify</th>
<th>Read &amp; Execute</th>
<th>List Folder Contents</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traverse Folder/Execute File</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List Folder/Read Data</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Read Attributes</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Read Extended Attributes</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Create Files/Write Data</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Create Folders/Append Data</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Write Attributes</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Write Extended Attributes</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Delete Subfolders and Files</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Permissions</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Change Permissions</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take Ownership</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:**

<table>
<thead>
<tr>
<th>Special Permissions</th>
<th>Full Control</th>
<th>Modify</th>
<th>Read &amp; Execute</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traverse Folder/Execute File</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List Folder/Read Data</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Read Attributes</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Read Extended Attributes</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Create Files/Write Data</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Create Folders/Append Data</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Write Attributes</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Write Extended Attributes</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Delete Subfolders and Files</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Permissions</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Change Permissions</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Take Ownership</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
Configuring 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 (hisecws.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.
<table>
<thead>
<tr>
<th>FOLDER OR FILE</th>
<th>USER GROUPS</th>
<th>RECOMMENDED PERMISSIONS</th>
<th>INHERIT METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ProgramFiles%</td>
<td>Administrators, CREATOR, OWNER, SYSTEM, Users</td>
<td>Full Control (subfolders and files)</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>Folder in which applications are installed. By default, this is %SystemDrive%\Program Files.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%ProgramFiles%\Resource Kit (servers and domain controllers)</td>
<td>Administrators, SYSTEM</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>%ProgramFiles%\Resource Pro Kit (workstations)</td>
<td></td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Folder where the Windows 2000 server Resource Kit (or professional resource kit) is installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%</td>
<td>Administrators, CREATOR, OWNER, SYSTEM, Users</td>
<td>Full Control (subfolders and files)</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>Contains many operating system DLLs, drivers, and executable programs.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\appmgmt</td>
<td>Administrators, SYSTEM, Users</td>
<td>Full Control</td>
<td>Propagate</td>
</tr>
<tr>
<td></td>
<td>Contains application management files used for software installation.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\config</td>
<td>Administrators, SYSTEM, Users</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>Contains registry hive files.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\dillcache</td>
<td>Administrators, CREATOR, OWNER, SYSTEM, Users</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>Contains copies of protected system files. These copies are used by the System File Checker to repair corrupted or modified system files.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\DTCLog</td>
<td>Administrators, CREATOR, OWNER, SYSTEM, Users</td>
<td>Full Control (subfolders and files)</td>
<td>Propagate</td>
</tr>
<tr>
<td></td>
<td>Log file for MS Distributed Transaction Coordinator, which is required for Microsoft Transaction Server.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\GroupPolicy</td>
<td>Administrators, Authenticated Users, SYSTEM</td>
<td>Full Control</td>
<td>Propagate</td>
</tr>
<tr>
<td></td>
<td>Folder containing local Group Policy Objects.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\ias</td>
<td>Administrators, CREATOR, OWNER, SYSTEM</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>Contains databases for the Internet Authentication Service.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\Ntbbackup.exe</td>
<td>Administrators, SYSTEM</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>File system backup program.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\NTMSData</td>
<td>Administrators, SYSTEM</td>
<td>Full Control</td>
<td>Propagate</td>
</tr>
<tr>
<td></td>
<td>Default location for the Removable Storage database.</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\rcp.exe</td>
<td>Administrators, SYSTEM</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>Remote copy command</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\Regedt32.exe</td>
<td>Administrators, SYSTEM</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td></td>
<td>Registry editing tool</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemDirectory%\ReinstallBackups</td>
<td>Ignore</td>
<td></td>
<td>Ignore</td>
</tr>
<tr>
<td></td>
<td>Contains files used for reinstallations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOLDER OR FILE</td>
<td>USER GROUPS</td>
<td>RECOMMENDED PERMISSIONS</td>
<td>INHERIT METHOD</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------</td>
<td>-------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>%SystemDirectory%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table><p>epl        | Administrators           | Full Control            | Propagate      |
| Folder containing scripts and files to be replicated or that have been replicated. | SYSTEM                  | Full Control            |                |
|                               | Users                    | Read, Execute           |                |
| %SystemDirectory%epl\export | Administrators           | Full Control            | Propagate      |
| Folder containing scripts and files to be replicated to other replication servers. | Replicator               | Read, Execute           |                |
|                               | SYSTEM                   | Full Control            |                |
|                               | Users                    | Read, Execute           |                |
| %SystemDirectory%epl\import | Administrators           | Full Control            | Propagate      |
| Folder containing scripts and files that have been replicated from other replication servers. | Replicator               | Modify                |                |
|                               | SYSTEM                   | Full Control            |                |
|                               | Users                    | Read, Execute           |                |
| %SystemDirectory%\reexec.exe  | Administrators           | Full Control            | Replace        |
| Program used to execute remote calls. | SYSTEM                  | Full Control            |                |
|                               |                          | Replace                 |                |
| %SystemDirectory%\rsh.exe     | Administrators           | Full Control            | Replace        |
| Program used to execute a remote shell. | SYSTEM                  | Full Control            |                |
| %SystemDirectory%\secedit.exe | Administrators           | Full Control            | Replace        |
| Security configuration and analysis tool. | SYSTEM                  | Full Control            |                |
| %SystemDirectory%\Setup       | Administrators           | Full Control            | Propagate      |
| Contains setup DLLs.          | SYSTEM                   | Full Control            |                |
|                               | Users                    | Read, Execute           |                |
| %SystemDirectory%\spool\Printers | Administrators   | Full Control            | Replace        |
| Printer spool.                | CREATOR OWNER            | Full Control (subfolders and files) |                |
|                               | SYSTEM                   | Full Control            |                |
|                               | Users                    | Read attributes         |                |
|                               |                          | Read extended attributes|                |
|                               |                          | Create files            |                |
|                               |                          | Create folders (folder and subfolders) |        |
| %SystemDrive%                 | Administrators           | Full Control            | Propagate      |
| Drive on which Windows 2000 is installed. Contains important system startup and configuration files. | CREATOR OWNER            | Full Control (subfolders and files) |                |
|                               | SYSTEM                   | Full Control            |                |
|                               | Users                    | Read, Execute           |                |
| %SystemDrive%\autoexec.bat c:\autoexec.bat | Administrators   | Full Control            | Replace        |
| Initialization file for DOS applications. | SYSTEM                  | Full Control            |                |
|                               | Users                    | Read, Execute           |                |
| %SystemDrive%\boot.ini        | Administrators           | Full Control            | Replace        |
| Boot menu.                    | SYSTEM                   | Full Control            |                |
| %SystemDrive%\config.sys c:\config.sys | Administrators   | Full Control            | Replace        |
| Initialization file for DOS applications. | SYSTEM                  | Full Control            |                |
| %SystemDrive%\Documents and Settings | Administrators | Full Control            | Propagate      |
| Folder containing user and default profiles. | SYSTEM                  | Full Control            |                |
|                               | Users                    | Read, Execute           |                |</p>
### Chapter 9 – Modifying File System Security Settings with Security Templates

#### FOLDER OR FILE

<table>
<thead>
<tr>
<th>FOLDER OR FILE</th>
<th>USER GROUPS</th>
<th>RECOMMENDED PERMISSIONS</th>
<th>INHERIT METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%SystemDrive%\Documents and Settings\Administrator</code></td>
<td>Administrators SYSTEM</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Folder containing the built-in Administrator profile.</td>
<td>SYSTEM Full Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WARNING:</strong> 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>%SystemDrive%\Documents and Settings\All Users</code></td>
<td>Administrators SYSTEM</td>
<td>Full Control Read, Execute</td>
<td>Propagate</td>
</tr>
<tr>
<td>Folder containing desktop and profile attributes for all users.</td>
<td>SYSTEM Full Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users Full Control Read, Execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>%SystemDrive%\Documents and Settings\Default User</code></td>
<td>Administrators SYSTEM</td>
<td>Full Control Read, Execute</td>
<td>Replace</td>
</tr>
<tr>
<td>Folder containing default desktop and profile attributes for users logging on for the first time.</td>
<td>SYSTEM Full Control Read, Execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users Full Control Read, Execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson</code></td>
<td>Administrators CREATOR OWNER Full Control Read, Execute</td>
<td>Replace</td>
<td></td>
</tr>
<tr>
<td>Folder containing the Dr. Watson application error log.</td>
<td>SYSTEM Full Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users Full Control Read, Execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(subfolders and files)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traverse folder, Create files, Create folders</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log</code></td>
<td>Administrators CREATOR OWNER Full Control</td>
<td>Replace</td>
<td></td>
</tr>
<tr>
<td>Dr. Watson application error log file.</td>
<td>SYSTEM Full Control Read, Execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users Full Control Modify</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>%SystemDrive%\Inetpub</code></td>
<td>Administrators CREATOR OWNER Full Control</td>
<td>Replace</td>
<td></td>
</tr>
<tr>
<td>(Servers only)</td>
<td>SYSTEM Full Control Read, Execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS web server folder. Only exists if IIS 5.0 is installed. Ignored in this document. See NSA’s Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0 for recommended file settings on this folder.</td>
<td>Users Full Control Modify</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>%SystemDrive%\Inetpub</code></td>
<td>Ignore</td>
<td></td>
<td>Ignore</td>
</tr>
<tr>
<td>Ignore</td>
<td>Ignore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOLDER OR FILE</td>
<td>USER GROUPS</td>
<td>RECOMMENDED PERMISSIONS</td>
<td>INHERIT METHOD</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>%SystemDrive%\io.sys</td>
<td>Administrators, SYSTEM, Users</td>
<td>Full Control, Full Control, Read, Execute</td>
<td>Replace</td>
</tr>
<tr>
<td>Initialization file for DOS apps.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemDrive%\msdos.sys</td>
<td>Administrators, SYSTEM, Users</td>
<td>Full Control, Full Control, Read, Execute</td>
<td>Replace</td>
</tr>
<tr>
<td>Initialization file for DOS apps.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemDrive%\My Download Files</td>
<td>Administrators, SYSTEM, Owner</td>
<td>Full Control, Full Control, Read, Execute</td>
<td>Replace</td>
</tr>
<tr>
<td>A default folder for downloaded docs.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemDrive%\ntdetect.com</td>
<td>Administrators, SYSTEM</td>
<td>Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Hardware detector during Windows 2000 boot.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemDrive%\ntldr</td>
<td>Administrators, SYSTEM</td>
<td>Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Windows 2000 operating system loader.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemDrive%\System Volume Information</td>
<td>Ignore</td>
<td></td>
<td>Ignore</td>
</tr>
<tr>
<td>Accessible only by SYSTEM.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemDrive%\Temp</td>
<td>Administrators, Owner, SYSTEM, Users</td>
<td>Full Control, Full Control, Traverse folder, Create files, Create folders (folders and subfolders)</td>
<td>Replace</td>
</tr>
<tr>
<td>Folder containing temporary files.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%</td>
<td>Administrators, Owner, SYSTEM, Users</td>
<td>Full Control, Full Control (subfolders and files)</td>
<td>Replace</td>
</tr>
<tr>
<td>Folder in which the Windows 2000 operating system is installed. By default, this is called winnt.</td>
<td></td>
<td>Traverse folder, Create files, Create folders (folders and subfolders)</td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%$NtServicePackUninstall$</td>
<td>Administrators, SYSTEM</td>
<td>Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Contains older versions of system files necessary to back off a service pack.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%$NtUninstall* (all uninstall folders)</td>
<td>Administrators, SYSTEM</td>
<td>Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Contains uninstall files for hotfixes and other applications.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Substitute the name of the folder(s) for "$NtUninstall". The security template will not recognize the wildcard character "*".
### Chapter 9 – Modifying File System Security Settings with Security Templates

<table>
<thead>
<tr>
<th>Folder or File</th>
<th>User Groups</th>
<th>Recommended Permissions</th>
<th>Inherit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>%SystemRoot%\CSC</td>
<td>Administrators, SYSTEM</td>
<td>Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Contains all offline files requested by any user on the computer. CSC means “client side caching”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\debug</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains various system and Active Directory logs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\debug\UserMode</td>
<td>Administrators, SYSTEM, Users</td>
<td>Full Control, Full Control</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains logs for group policy application to users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\NTDS (Domain Controllers only)</td>
<td>Administrators, SYSTEM</td>
<td>Full Control, Full Control</td>
<td>Propagate</td>
</tr>
<tr>
<td>Active Directory database folder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> The %SystemRoot% portion of the path name may need to be changed depending on where the default Active Directory folder is located</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\security</td>
<td>Administrators, CREATOR OWNER, SYSTEM, Users</td>
<td>Full Control, Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Contains security templates and analysis databases</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\SYSVOL (Domain Controllers only)</td>
<td>Administrators, AUTHENTICATED USERS, CREATOR OWNER, SYSTEM</td>
<td>Full Control, Read, Execute</td>
<td>Propagate</td>
</tr>
<tr>
<td>Default Active Directory location for files that must be shared throughout a domain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> The %SystemRoot% portion of the path name may need to be changed depending on where the default Active Directory folder is located</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\SYSVOL\domain\Policies (Domain Controllers only)</td>
<td>Administrators, AUTHENTICATED USERS, CREATOR OWNER, GROUP POLICY CREATOR OWNERS, SYSTEM</td>
<td>Full Control, Read, Execute</td>
<td>Propagate</td>
</tr>
<tr>
<td>Contains group policy objects</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> The %SystemRoot% portion of the path name may need to be changed depending on where the default Active Directory folder is located</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOLDER OR FILE</td>
<td>USER GROUPS</td>
<td>RECOMMENDED PERMISSIONS</td>
<td>INHERIT METHOD</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------</td>
<td>-------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>%SystemRoot%\Offline Web Pages</td>
<td>Ignore</td>
<td></td>
<td>Ignore</td>
</tr>
<tr>
<td>Folder containing web pages that have been downloaded for off-line viewing.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\regedit.exe</td>
<td>Administrators</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Registry editing tool.</td>
<td>SYSTEM</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\Registration</td>
<td>Administrators</td>
<td>Full Control</td>
<td>Propagate</td>
</tr>
<tr>
<td>Folder containing Component Load Balancing (CLB) registration files read by COM+ applications.</td>
<td>SYSTEM</td>
<td>Full Control Read</td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\repair</td>
<td>Administrators</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Backup files of SAM database and other important registry and system files to be used during a system repair.</td>
<td>SYSTEM</td>
<td>Full Control</td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\Tasks</td>
<td>Ignore</td>
<td></td>
<td>Ignore</td>
</tr>
<tr>
<td>Folder containing jobs scheduled by Task Scheduler.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SystemRoot%\Temp</td>
<td>Administrators</td>
<td>Full Control</td>
<td>Replace</td>
</tr>
<tr>
<td>Folder containing temporary files.</td>
<td>CREATOR OWNER</td>
<td>Full Control (subfolders and files)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
<td>Full Control (folders and subfolders)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 17 Recommended File Permissions

<table>
<thead>
<tr>
<th>FOLDER OR FILE</th>
<th>USER GROUPS</th>
<th>RECOMMENDED PERMISSIONS</th>
<th>INHERIT METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\ntbootdd.sys</td>
<td>Administrators&lt;br&gt;SYSTEM</td>
<td>Full Control&lt;br&gt;Full Control</td>
<td>Replace</td>
</tr>
</tbody>
</table>
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
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:

```plaintext
```

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/analyze</td>
<td>Performs an analysis</td>
</tr>
<tr>
<td>/configure</td>
<td>Performs a configuration</td>
</tr>
<tr>
<td>/cfg filename</td>
<td>Path to a configuration file that will be appended to the database prior to performing the analysis</td>
</tr>
</tbody>
</table>
| /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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/quiet</td>
<td>Suppress screen and log output</td>
</tr>
<tr>
<td>/overwrite</td>
<td>Overwrite the named database with the given configuration information.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING:</strong> 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.</td>
</tr>
<tr>
<td>/areas Areas</td>
<td>Only relevant when using the /configure switch. Specifies the security areas to be processed. The following areas are available:</td>
</tr>
<tr>
<td></td>
<td>SECURITYPOLICY - Local policy and domain policy for the system, including account policies, audit policies, etc.</td>
</tr>
<tr>
<td></td>
<td>GROUP_MGMT - Restricted Group settings</td>
</tr>
<tr>
<td></td>
<td>USER_RIGHTS - User rights assignments</td>
</tr>
<tr>
<td></td>
<td>DOBJECTS - Security on directory objects</td>
</tr>
<tr>
<td></td>
<td>REGKEYS - Security permissions on local registry keys</td>
</tr>
<tr>
<td></td>
<td>FILESTORE - Security permissions on local file system</td>
</tr>
<tr>
<td></td>
<td>SERVICES - Security configuration for all defined services</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If the /areas switch is not used, the default is all security areas. If used, each area name should be separated by a space.</td>
</tr>
</tbody>
</table>

Table 18 Secedit Command Line Parameters

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/export</td>
<td>Exports a stored template from a security database to a security template file</td>
</tr>
<tr>
<td>/refreshpolicy (machine_policy</td>
<td>user_policy) / (enforce)</td>
</tr>
<tr>
<td></td>
<td><strong>machine_policy</strong> – reapply machine-related settings; this option will be most used for security settings since the recommended settings are machine-specific</td>
</tr>
<tr>
<td></td>
<td><strong>user_policy</strong> – reapply user-related settings</td>
</tr>
<tr>
<td></td>
<td>/enforce – reapply settings regardless of whether they have changed</td>
</tr>
<tr>
<td>/validate &lt;filename&gt;</td>
<td>Validates the syntax of a template to be imported into a database for analysis or configuration</td>
</tr>
</tbody>
</table>

### 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:

```
```

*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
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:


**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 secedit. 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:

- `secedit /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.
Chapter 10 – Security
Configuration and Analysis

This Page Intentionally Left Blank
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


“Default Access Control Settings in Windows 2000,”
http://www.microsoft.com/windows2000/techinfo/planning/security/secdefs.asp,

“Event ID 1000 and 1202 After Configuring Policies,” KB article Q260715
http://support.microsoft.com/support/kb/articles/Q260/7/15.asp,

“How to Use the RestrictAnonymous Registry Value in Windows 2000,” KB article Q246261
http://support.microsoft.com/support/kb/articles/Q246/2/61.asp,


KB article Q230895 http://support.microsoft.com/support/kb/articles/Q230/8/95.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,


“Security Configuration Toolset,”
http://www.microsoft.com/windows2000/techinfo/howitworks/security/sctoolset.asp,

Smith, Randy Franklin, “Dangerous Services,” Windows IT Security web site,

“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