Report Number: C44-026-02

Guide to Securing Microsoft Windows XP®

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

Authors:
R. Bickel
M. Cook
J. Haney
M. Kerr, DISA
CT01 T. Parker, USN
H. Parkes

Updated: October 30, 2002
Version: 1.0

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

XPGuides@nsa.gov

This Page Intentionally Left Blank

Disclaimer

SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Acknowledgements

The authors would like to acknowledge the authors of the *"Guide to Securing Microsoft Windows 2000"* series.

The authors would also like to thank Sherri Bavis for reviewing this document and all the organizations that participated in beta testing this guide. Your comments and suggestions were invaluable.

Trademark Information

Table of Contents

Table of Figures

Table of Tables

This Page Intentionally Left Blank

Chapter

1

Important Information on Using this Guide

The purpose of this document is to inform the reader about Windows XP Professional recommended security settings. These security settings include those that can be set via the Security Configuration Manager, through Group Policy, as well as manual settings.

Windows XP Professional is a client operating system only. The corresponding server version has not yet been released. Therefore, this document will address Windows XP within a Windows 2000 domain and utilizing Windows 2000 Active Directory and Group Policy. 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.

NOTE: This guide does not address security concerns of Windows XP Home Edition or standalone (i.e. not joined to a domain) Windows XP Professional

Although the primary environment addressed in this guide is Windows XP in a Windows 2000 domain, Chapter 16 discusses modifications to the security recommendations that must be made when adding Windows XP to a Windows NT 4.0 domain.

Included with this document is a security template: `WinXP_workstation.inf`. The purpose and use of this template will be discussed later in this document.

This document is intended for Windows network administrators, but should be read by anyone involved or interested in Windows XP 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 and Microsoft Windows XP Professional clean-installed machines (i.e., not upgraded).

NOTE: Chapter 16 discusses issues involved when adding Windows XP to a Windows NT 4.0 domain.

- Windows XP machines are formatted using the NT File System (NTFS).
- Domain controllers are Windows 2000 machines and are running Active Directory.

NOTE: Chapter 16 discusses issues involved when Windows NT 4.0 domain controllers are present in the domain.

- The latest Windows 2000 and Windows XP service packs and hotfixes have been installed. For further information on critical Windows updates, see the Windows Update web page http://windowsupdate.microsoft.com or search for security hotfixes by service pack at the Technet Security Bulletin Search http://www.microsoft.com/technet/security/current.asp.
- All network machines are Intel-based architecture.
- Applications are Windows XP compatible.
- Users of this guide have a working knowledge of Windows XP and Windows 2000 installation and basic system administration skills.

Warnings to Review Before Using this Guide

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

- **Do not attempt to install any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore, this guide does not address site-specific configuration issues. Care must be taken when implementing this guide while using products such as Microsoft Exchange, IIS, and SMS.
- The security changes described in this document only apply to **Microsoft Windows XP Professional** systems and should not be applied to any other Windows operating systems.
- A Windows XP system can be severely impaired or disabled with incorrect changes or accidental deletions when using programs (examples: Security Configuration Manager, `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.

  NOTE: In Windows XP, regedt32.exe is now just a link to regedit.exe.

- Currently, no "undo" function exists for deletions made within the Windows XP registry. The registry editor (`Regedit.exe`) prompts the user to confirm the deletions. When a registry key is being deleted, the message does not include the name of the key being deleted. Check your selection carefully before proceeding with any deletion.

Conventions and Commonly Used Terms

Users and Authenticated Users

For Access Control Lists (ACLs) on Windows XP workstations, Microsoft 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 member. Membership in the Users group can be controlled by administrators, which is Microsoft's reasoning for using this group in access control lists. Looking at the default security template for workstations (see the next chapter for information on this

template), the Users group is used in file and registry permissions as well as user rights assignment.

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.

System Variables

The following system variables are referenced throughout this document:

- **%SystemDrive%** - The drive letter on which Windows XP is installed. This is usually C:\.
- **%SystemRoot%** - The folder containing the Windows XP operating system files. This is usually `%SystemDrive%\WINDOWS`.
- **%SystemDirectory%** - `%SystemRoot%\system32`
- **%ProgramFiles%** - Folder in which most applications are installed. This is usually `%SystemDrive%\Program Files.`
- **%AllUsersProfile%** - Folder in which the All Users profile is installed. This is usually `%SystemDrive%\Documents and Settings\All Users`.

Administrative Tools location

By default, the **Administrative Tools** menu does not appear in the Windows XP **Start** menu. To view **Administrative Tools** in the **Start** menu:

- Right-click on the taskbar (usually along the bottom of the screen)
- Select **Properties** from the pull-down menu
- Click the **Start Menu** tab
- Click the **Customize** button
- Click the **Advanced** tab
- Under the **Start menu items** section, scroll down to the **System Administrative Tools** section
- Select either the **Display on the All Programs menu** or **Display on the All Programs menu and the Start menu**

This guide will assume that the Administrative Tools will be accessed from the **All Programs** menu.

About the Guide to Securing Microsoft Windows XP

This document consists of the following chapters:

Chapter 1, "Important Information on Using this Guide," provides important assumptions and warnings to be read prior to using the guide.

Chapter 2, "What's New in Windows XP Security," gives a brief overview of new security features in Windows XP.

Chapter 3, "Introduction to the Security Configuration Manager Tools,'' provides an overview of the Security Configuration Manager Tool Set's 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 file included with this document and details a checklist for configuring a network using the provided settings.

Chapter 4, "Modifying Account Policy Settings with Security Templates," explains how to set domain wide account policies using the Security Templates snap-in. The section also covers Password Policy, Account Lockout, and Kerberos Policy.

Chapter 5, "**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 6, "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. Guidance for managing Event Logs is also included in this chapter.

Chapter 7, "Managing Restricted Groups with Security Templates," discusses how to manage the membership of sensitive groups using the Restricted Groups option.

Chapter 8, "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 9, "Modifying Registry Security Settings with Security Templates," discusses how to configure access control lists for Registry Keys. Discussion includes recommendations for registry key permissions.

Chapter 10, "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 11, "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 12, "Applying Windows XP Group Policy in a Windows 2000 Domain," discusses how to push down group policy to Windows XP clients from a Windows 2000 domain controller running Active Directory.

Chapter 13, "Remote Assistance/Desktop Configuration," gives recommendations for using and securing the Remote Assistance and Remote Desktop features in Windows XP.

Chapter 14, "Internet Connection Firewall," discusses the use of Windows XP's personal firewall capability.

Chapter 15, "Additional Security Settings," describes other miscellaneous security recommendations such as administrator account usage and share permissions.

Chapter 16, "Modifications for Windows XP in a Windows NT Domain," describes several recommended security settings if Windows XP is a member of a Windows NT domain.

This Page Intentionally Left Blank

Chapter

2

What's New in Windows XP Security

Windows XP has modified Windows 2000 security settings as well as introducing new security features. This chapter gives a brief overview of some of the features that are relevant to Windows XP systems in a domain environment. Features unique to stand-alone Windows XP machines will not be addressed in this document.

Changes to Security Features

The following features have been modified from Windows 2000.

Everyone group membership

In Windows NT and Windows 2000, the built-in Everyone group includes the anonymous user (null connection). This means a null session connection has access to the same resources as the Everyone group. By default, in Windows XP, the Everyone group no longer includes the anonymous user.

Administrative ownership

In Windows NT and Windows 2000, any object that is created by a member of the Administrators group is automatically assigned the whole group as the owner. In Windows XP, the administrative user that creates the object becomes the sole owner of the object.

Installation of printers

In Windows XP, a user must belong to either the Power Users or Administrators group to be able to install a local printer. Additionally, the user must be granted the Load/Unload Device Driver user right.

NOTE: Administrators have the Load/Unload Device Driver right by default.

Blank password restriction

Local Windows XP accounts that do not have passwords can only be used to log in at the console, not across the network.

NOTE: This restriction does not apply to domain user logons. It also does not apply to the Guest account. If the Guest account is enabled and has a blank password, it can log on remotely to resources granted Guest access.

Convert.exe

In Windows NT and Windows 2000, using the `convert.exe` command to convert FAT or FAT32 volumes to NTFS results in the Everyone group being given Full Control permissions on the converted volume. In Windows XP, however, `convert.exe` will automatically set default Windows XP file permissions on the volume.

Subsystems

Windows NT and Windows 2000 provide support for the OS/2 and POSIX subsystems. However, Windows XP no longer includes these subsystems. POSIX support is now included in a separate package as part of Microsoft Windows Interix 2.2. Refer to http://www.microsoft.com/windows2000/Interix for more information on Interix.

Encrypting File System

The Encrypting File System (EFS) allows users to encrypt files, folders, or entire data drives. Windows XP includes several new features for EFS:

- Other users can be authorized to access encrypted files
- Offline Files can be encrypted
- Data Recovery Agents are optional
- The triple-DES (3DES) encryption algorithm can be used in place of DESX
- A password reset disk can reset a user's password
- Encrypted files can be stored in web folders

New Security Features

This section discusses some of the new security features in Windows XP.

Software Restriction Policies

An increasing number of "stealth" programs distributed over the Internet and via e-mail in the form of worms and viruses take advantage of unsuspecting users in order to steal information or wreak havoc on the computer system. Windows XP now provides a mechanism for administrators to classify applications as trusted or untrusted.

Through Software Restriction Policies, software can be prevented from running based on the following rules:

- **Path** – applications can be allowed or disallowed based on the file path or folder. Path rules can incorporate wildcards. For example, all Visual Basic Script files can be disallowed by specifying *.vbs.

- **Hash** – applications can be allowed or disallowed based on the application's hashed file contents. A hash is based on the file's contents and uniquely identifies the file. If the file has been modified in any way, the hash will change.

- **Certificate** – applications can be allowed or disallowed based on digital certificates associated with the applications.

- **Internet Zone** – applications can be allowed or disallowed based on the Internet zone from which they were downloaded. The following zones can be specified: Internet, Intranet, Restricted Sites, Trusted Sites, and My Computer. These rules apply only to Windows Installer packages.

- **Enforcement Properties** – determines whether software library files (files containing common variable and function definitions) are included in the software restrictions policies. Also, this option can be used to prevent software restrictions from applying to local administrators.

- **Designated File Types** – allows addition or deletion of file types from the list of what is considered to be executable code.

- **Trusted Publishers** – determines which users can select trusted application publishers.

For more information, see Microsoft Knowledge Base article Q310791 "Description of the Software Restriction Policies in Windows XP" at http://support.microsoft.com/default.asp?scid=kb;EN=US;q310791.

Stored user names and passwords

User names and credentials needed to access network or Internet resources are stored on the system. **Pending further review of the storage mechanism, there is no recommendation for this feature at this time.**

New Service Accounts

Two new service accounts, Network Service and Local Service, replace the LocalSystem account as service accounts for certain services. This section describes all three service accounts.

LocalSystem Account

The LocalSystem account is a predefined local account with complete privileges on the local computer. The account is not associated with any regular user account and does not have credentials such as user name and password. The service account can open the registry key HKLM\Security. When LocalSystem accesses network resources, it does so as the computer's domain account.

Examples of services that run under the LocalSystem account are: WindowsUpdate Client, Clipbook, Com+, DHCP Client, Messenger Service, Task Scheduler, Server Service, Workstation Service, and Windows Installer.

Network Service Account

The Network Service Account is a predefined local account with limited privileges on the local computer. It has the ability to act access network resources as the computer. Services that run under the Network Service context present the computer's credentials to remote systems. The Network Service account generally

can access resources whose Access Control Lists (ACLs) allow access by the Network Service, Everyone, or Authenticated Users.

Examples of services that run as Network Service are: Distributed Transaction Coordinator, DNS Client, Performance Logs and Alerts, and RPC Locator.

Local Service Account

The Local Service account is a predefined account that has minimum privileges on the local computer and presents anonymous credentials on the network. The Local Service account generally can access resources whose ACLs allow access by the Local Service, Everyone, or Authenticated Users.

Examples of services that run as Local Service are: Alerter, Remote Registry, Smart Card, SSDP, and WebClient.

Chapter

3

Introduction to the Security Configuration Manager Tools

Windows XP includes support for the Security Configuration Manager (SCM). The SCM 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 XP machines either as part of a Group Policy Object (GPO) or through local computer configuration.

Several tools allow you to configure security settings on Windows XP

- Local Security Policy
- Security Settings extension to Group Policy
- The Security Configuration Manager, which consists of the following:
  - Security Templates snap-in
  - Security Configuration and Analysis snap-in
  - Secedit.exe command-line tool

These components allow 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
- **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 4 – 10 describe recommended settings and how to customize the templates, and Chapter 11 describes how to conduct a security analysis and configuration.

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

Security Configuration Functionality

The Security Configuration Manager tools support 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 XP. Tools are imported into the MMC via "snap-ins."

In actuality, the Security Configuration Manager 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 11, respectively.

The security configuration manager allows an administrator to:

- Create and/or edit security configuration templates
- 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 XP 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 XP computers either by being imported into a Group Policy Object, or by being directly applied to the local computer through the Security Configuration Manager.

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 installed by default on Windows XP systems. To load the Security Templates snap-in:

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

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

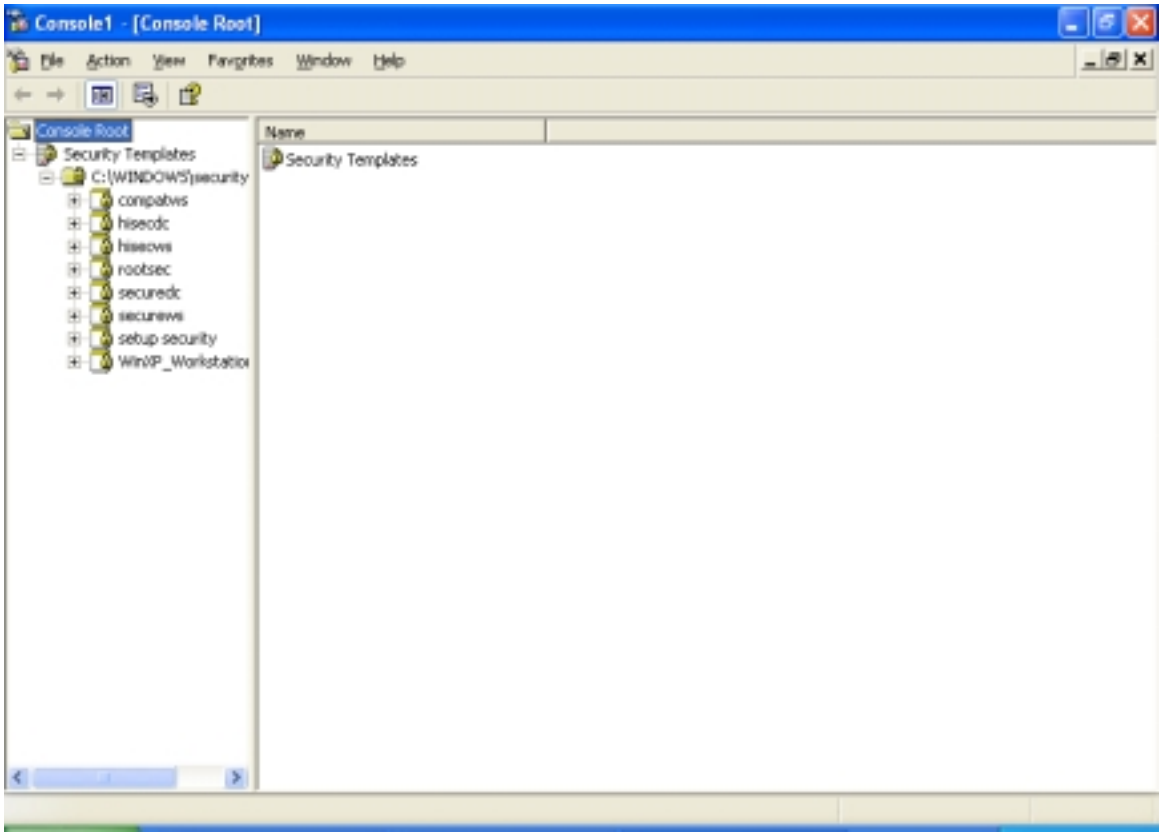


Figure 1 Security Templates snap-in

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

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

From then on, the console can be accessed from **Start → All Programs → Administrative Tools** as long as the users profile is configured to display the Administrative Tools on the start menu.

Viewing the Text of Security Templates

Although not recommended, security templates can be viewed via a text editor such as `notepad.exe`. Sections of the template addressing file and registry access control lists may seem cryptic at first. It is defined in a language called Security Descriptor Definition Language (SDDL). A Microsoft SDK article describing the SDDL syntax is available at http://msdn.microsoft.com/library/en-us/security/Security/security_descriptor_definition_language.asp.

Security Configuration Files

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

Default Security Templates

There is a security template that contains the default security settings applied to a clean-install (non-upgraded) Windows XP machine. The default security template is especially useful when wanting to return the system to its original state after making changes.

The template actually applied to a machine out-of-the-box is stored in `%SystemRoot%\security\templates` as "`setup security.inf`."

NOTE: "Setup security.inf" should never be applied via Group Policy from a domain controller and should only be applied to the local computer via the Security Configuration and Analysis snap-in or secedit.exe. This is because each setup template is customized during setup for that particular machine. Also, the template contains large numbers of configurations and could degrade network performance if periodically applied via a domain GPO.

Microsoft-provided Templates

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

NSA Security Template

This document has an accompanying security configuration file, `WinXP_workstation.inf`, which complies with the recommendations found in this manual. The security template can be found at http://nsa1.www.conxion.com/.

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, **test the settings 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 11) 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 4-10.**
- Backup your system. Backups are the only sure-fire way to restore your system.
- Download the appropriate configuration file to the template directory (`%Systemroot%\Security\Templates`), or add another template search path to wherever the templates are stored.
- It is suggested that you make copies of the template files under different names if you plan to perform modifications to the recommended settings. You can do this prior to opening the files in the MMC, or by performing a **Save As** after making modifications to the templates.
- 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`, after having downloaded the `sceregvl.inf` file to the `%SystemRoot%\inf` folder. The end of Chapter 5 discusses how other security options can be added to the templates.
- Review the recommended security settings in Chapters 4 – 10. 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 settings 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 5:
  - Accounts: Rename administrator account

- Accounts: Rename Guest account
- Interactive logon: Message text for users attempting to log on
- Interactive logon: Message title for users attempting to log on

- Once the templates have been customized to your network environment and saved, apply the templates. If the template will be applied locally, see Chapter 11 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 Chapter 12.
- Perform any additional security configurations described in Chapters 13-16 as applicable

This Page Intentionally Left Blank

Chapter

4

Modifying Account Policy Settings with Security Templates

A key component of controlling the security in a system 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), and via Local Security Policy on member servers and XP 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. Dictionary words should not be used.
- 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 1 lists the recommended password policy settings and **Figure 2** shows the password policy as it appears in the MMC.

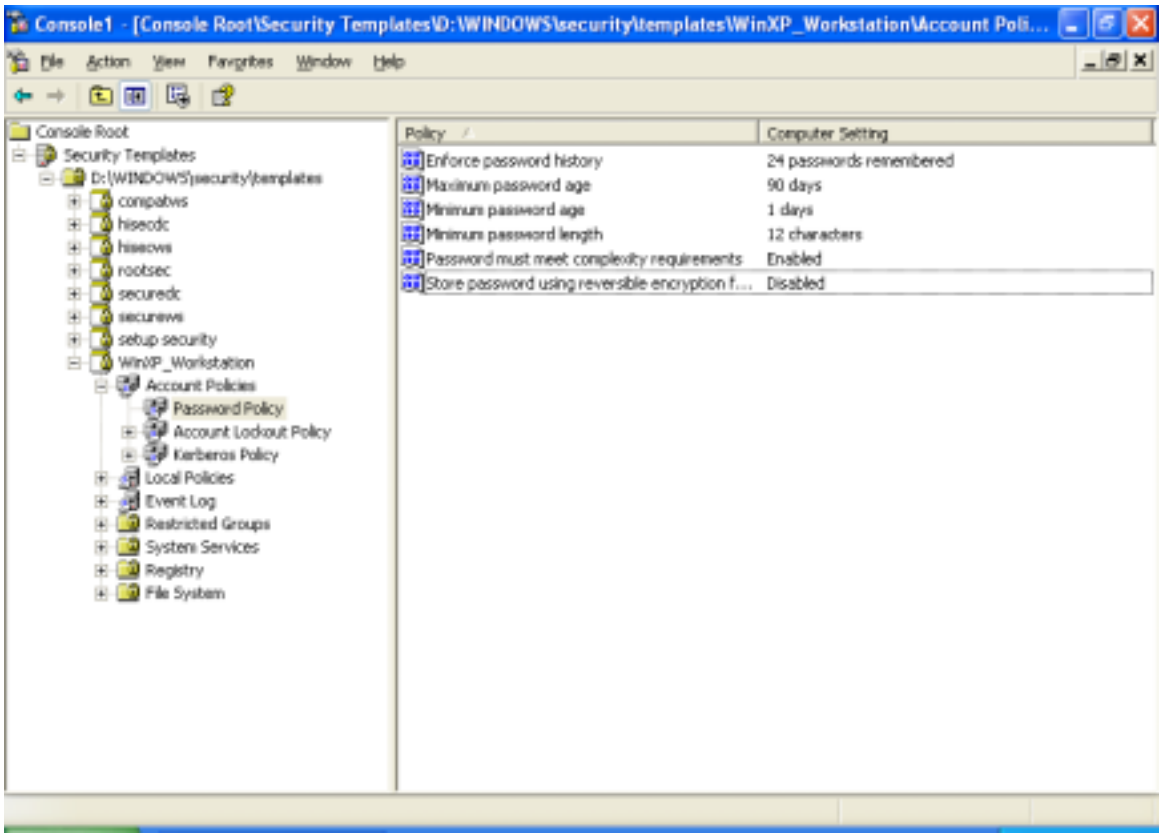


Figure 2 Password Policy recommendations

Password Policy Options	Recommended Settings
Enforce password history 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.	24 Passwords
Maximum Password Age 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.	90 days
Minimum Password Age 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.	1 Day
Minimum Password Length 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.  **NOTE: In actuality, Windows 2000 and XP support passwords up to 127 characters long. A password longer than 14 characters has a distinct advantage in that the LanManager hash of the password is invalid with these longer passwords, and, therefore, cannot be exploited as it normally could by password-cracking utilities. Unfortunately, the security templates interface will not allow setting of minimum password length to be greater than 14. Also, if a network contains Windows 9x or Windows NT 4.0 or earlier computers, the maximum password length cannot exceed 14 characters since those computers do not support entering passwords that long in the UI.**  **NOTE: It is recommended that privileged users (such as administrators) have passwords longer than 12 characters. An optional method of strengthening administrative passwords is to use characters that are not in the default character sets. For example, Unicode characters 0128 through 0159 have two advantages: (1) they cause the LanMan hash to be invalid, and (2) they are not in the character set for any common password crackers. Be careful using Unicode characters, however. Certain Unicode characters, such as 0200 (È), get converted into other characters, in this example 0069 (E) and then hashed, effectively weakening the password. To enter these passwords, hold the ALT key and type the number on the numeric key-pad. On a notebook, hold down the FN and ALT keys and type the number on the overlay numeric keypad.**	12 Characters

Password Policy Options	Recommended Settings
Passwords must meet complexity requirements Enforces strong password requirements for all users. 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. Pre-existing passwords will not be affected.  **NOTE: NSA provides an enhanced password complexity filter, ENPASFLT.DLL, that can be used in place of this option. 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 this option, you may want to set this option to "Disabled" to avoid conflicts.**  **NOTE: For information on creating your own custom password filter, see Microsoft Knowledge Base article Q151082 "HOWTO: Password Change Filtering and Notification in Windows NT" at** http://support.microsoft.com/default.asp?scid=kb;EN=US;q151082**.**	Enabled
Store password using reversible encryption for all users in the domain 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.	Disabled

Table 1 Password Policy Options

Account Lockout Policy

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

 **NOTE: The built-in Administrator account cannot be locked out due to settings in Account Lockout Policy. However, via the Remote Desktop, it possible to lock out the Administrator account from remote access. Local logon by Administrator is still permitted.**

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 2 lists the recommended account lockout policy settings.

Account Lockout Policy Options	Recommended Settings
Account lockout duration Sets the number of minutes an account will be locked out. Allowable values are 0 (account is lockout out until administrator unlocks it) or between 1 and 99999 minutes.  **WARNING: Setting this value to 0 (until administrator unlocks) may allow a potential denial of service attack. It is important to note that the built-in Administrator account cannot be locked out from logging on locally.**	15 minutes
Account lockout threshold Prevents brute-force password cracking/guessing attacks on the system. This option specifies the number of invalid logon attempts that can be made before an account is locked out. Allowable values range from 0 (account will not lockout) to 999 attempts. Although 3 invalid attempts is recommended in this guide, any number from 3 to 5 should provide adequate protection.  **NOTE: Failed logons on machines that have been locked via CTRL-ALT-DEL or a password-protected screen saver do not count as failed attempts.**	3 invalid logon attempts
Reset account lockout counter after Sets the number of minutes until the invalid logon count is reset. Allowable values range from 1 to 99999 minutes.	15 minutes

Table 2 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 Windows XP workstation that this document addresses, the Kerberos policies will not be defined. The following is for information purposes only.

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 3 lists the Kerberos Policy options that should be applied at the **domain group policy level.**

Kerberos Policy Options	Recommended Settings
Enforce user logon restrictions 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.	Enabled
Maximum lifetime for service ticket 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.  **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.**	600 minutes
Maximum lifetime for user ticket 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.	10 hours
Maximum lifetime for user ticket renewal 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.	7 days
Maximum tolerance for computer clock synchronization 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.	5 minutes

Table 3 Kerberos Policy Options

Chapter

5

Modifying Local Policy Settings with Security Templates

The Local Policies section of a security template organizes security attributes for Audit Policy, User Rights Assignment, and Security Options in a central location to ease security administration. 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 XP systems, auditing is not enabled by default. Each Windows XP 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**
- Right-click on the specific option to view or edit

Figure 3 and **Table 4** list recommended Audit Policy Settings for XP Professional. Recommended settings for Windows 2000 member servers and domain controllers are detailed in the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set*.

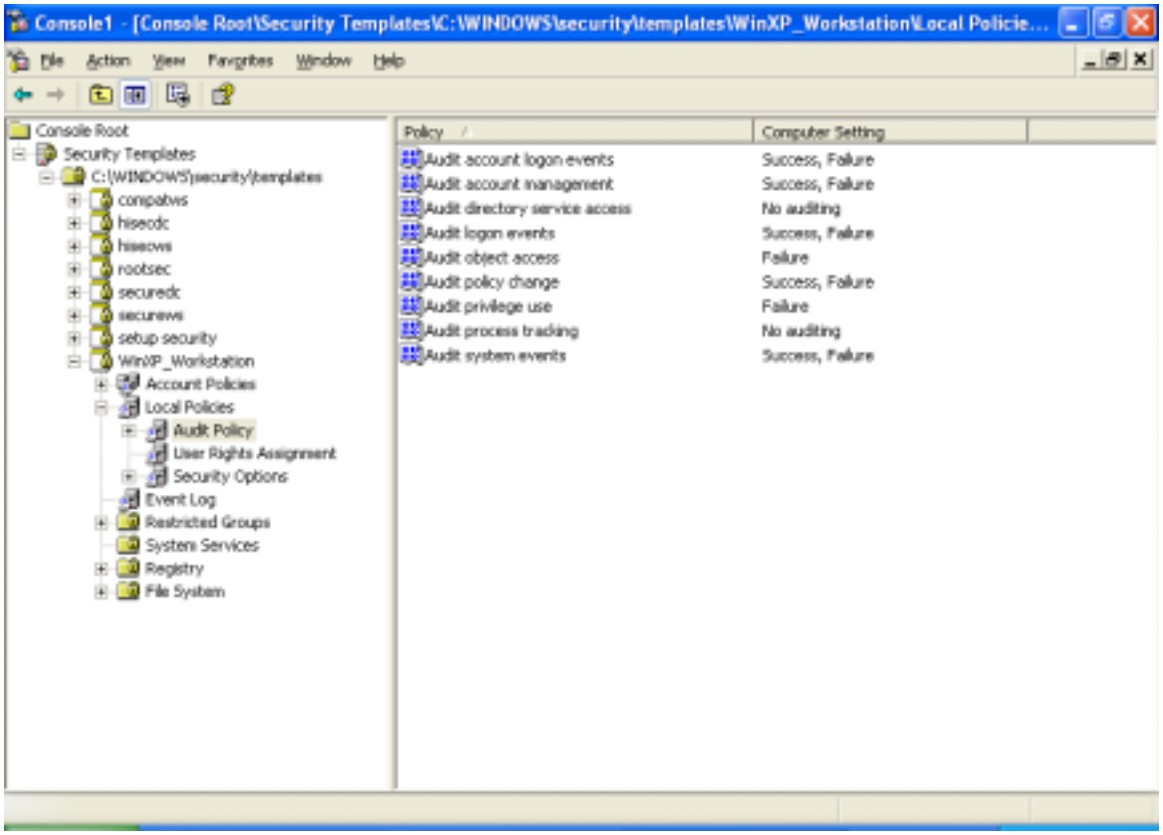


Figure 3 Recommended Audit Policy

Audit Policy Options	Recommended Settings
Audit account logon events Tracks user logon and logoff events on other computers in which the local computer was used to authenticate the account.	Success, Failure
Audit account management Tracks changes to the Security Accounts database (i.e., when accounts are created, changed, or deleted).	Success, Failure
Audit directory service access 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.	No auditing
Audit logon events 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.  **NOTE: The auditing of successful and failed logon events generates a large amount of data. Network, service, and user logons are all recorded. Auditing of success events is important for tracking users logged on during potential attacks. However, if log space is at a premium, at a minimum, failure of logon events should be recorded.**	Success, Failure
Audit object access 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.	Failure
Audit policy change Tracks changes in security policy, such as assignment of privileges or changes in the audit policy.  **NOTE: There exist problems with auditing successes of policy change. One such problem surfaces on the first system reboot after the "Audit: Shut down system immediately if unable to log security audits" (CrashOnAuditFail) security option is enabled. Upon reboot, the system will either blue screen or hang. Apparently, there is a problem writing a policy change event to the audit log, and thus, the system crashes. Subsequent reboots will be successful, but only an administrator can log on as designed. The administrator must then reset the CrashOnAuditFail registry key from 2 back to 0 or 1 in order for other users to access the system. This behavior does not exist if successful policy change audit is not enabled.**	Success, Failure
Audit privilege use Tracks unsuccessful attempts to use privileges. Privileges indicate rights assigned to 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.  **NOTE: The Audit use of all user rights including Backup and Restore setting under Security Options will audit those user rights excluded here. However, it will fill up the security event log very quickly and so is not recommended.**	Failure

Audit process tracking 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.	No Auditing
Audit system events Tracks events that affect the entire system or the Audit log. Records events such as restart or shutdown.	Success, Failure

Table 4 Audit Policy Options

User Rights Assignment

User Rights Assignments determine what actions users and groups are allowed to perform. Explicitly-granted user rights supplement implicit abilities of the user or group. The recommended user rights are listed and described in **Table 5**. Advanced user rights are assigned to Administrators or other trusted groups who are allowed to run administrative utilities, install service packs, create printers, and install device drivers. Administrators are not listed in **Table 5** for user rights this group has implicitly, unless the user right is modified from the default settings. For example, Backup Operators and Administrators have the right to "Back up files and directories", however, it is recommended that only Administrators have this right. Thus, Administrators is listed for this user right even though it is granted to Administrators implicitly.

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**
- Double-click on the desired Attribute in the right frame.
- To add a user or group, **Add User or Group** → Enter user or group **→ Add → OK → OK**
- To remove a user or group, select user or group **→ Remove → OK**

User Rights	Recommended Settings
Access this computer from network Allows a user to connect over the network to the computer.	Administrators Users
Act as part of the operating system Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.	(No one)
Add workstations to domain 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.	(No one)
Adjust memory quotas for a process Determines which accounts can use a process with Write Property access to another process to increase the processor quota assigned to the other process.	Administrators NETWORK SERVICE LOCAL SERVICE
Allow logon through Terminal Services Determines which users or groups have the right to log on as a Terminal Services client. This right is needed for Remote Desktop users. If Remote Assistance is being used, only administrators using this new feature should have this right.	(No one)
Back up files and directories Allows a user to back up files and directories. This right supersedes file and directory permissions.  **NOTE: If the network makes use of the Backup Operators or similar group, also assign this right to that group. Keep in mind, however, that users who have this right have the ability to bypass ACLs. Unless FullPrivilegeAuditing is turned on, such access is not logged.**	Administrators
Bypass traverse checking Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories.	Users
Change the system time Allows a user to set the time for the internal clock of the computer.	Administrators
Create a pagefile Allows a user to create new pagefiles for virtual memory swapping and change the size of a pagefile.	Administrators
Create a token object 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.	(No one)
Create permanent shared objects Allows a user to create special permanent directory objects, such as \\Device, that are used within the Windows XP object manager.	(No one)
Debug programs Allows a user to debug various low-level objects such as threads.  **NOTE: Software developers working on the system may need this right to debug programs running as other users. Assign the right to developer users/groups only when necessary.**	(No one)

User Rights	Recommended Settings
Deny access to this computer from the network Prevents specific users and/or groups from accessing the computer via the network. This setting supercedes the "Access this computer from the network" setting if an account is subject to both policies.  **NOTE: By default, the Guest and SUPPORT_388945a0 users are denied this right.**	(Not Defined)
Deny logon as a batch job Prevents specific users and/or groups from logging on as a batch job. This setting supercedes the "Logon as a batch job" setting if an account is subject to both policies.	(No one)
Deny logon as a service Prevents specific service accounts from registering a process as a service. This setting supercedes the "Log on as a service" setting if an account is subject to both policies.	(No one)
Deny logon locally Prevents specific users and/or groups from logging on directly at the computer. This setting supercedes the "Log on locally" setting if an account is subject to both policies.  **NOTE: By default, the Guest and SUPPORT_388945a0 users are denied this right.**	(Not Defined)
Deny logon through Terminal Services Determines which users and groups are prohibited from logging on as a Terminal Services client. This right is used for Remote Desktop users.  **NOTE: If Terminal Services is being used on the system, the Everyone entry should be removed from this deny option.**	Everyone
Enable computer and user accounts to be trusted for delegation 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.	(No one)
Force shutdown from a remote system Allows a user to shutdown a Windows XP computer from a remote location on the network.	Administrators
Generate security audits Allows a process to generate security audit log entries.	LOCAL SERVICE NETWORK SERVICE
Increase scheduling priority Allows a user to boost the execution priority of a process. This can be performed via the Task Manager user interface.	Administrators
Load and unload device drivers Allows a user to install and remove device drivers. This right is necessary for Plug and Play device driver installation.	Administrators
Lock pages in memory Allows a user to lock pages in physical memory so they cannot be paged out to a virtual memory on disk.	(No one)
Log on as a batch job Allows a user to log on by means of a batch-queue facility. In Windows XP, the Task Scheduler automatically grants this right as necessary.	(No one)

User Rights	Recommended Settings
Log on as a service Allows a process to register with the system as a service.  **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 (with the exception of NETWORK SERVICE) from this right unless you modify the setting.**	NETWORK SERVICE
Log on locally Allows a user to log on at a system's console.  **NOTE: If the network makes use of the Backup Operators or similar group, also assign this right to that group.**	Administrators Users
Manage auditing and security log Allows a user to view and clear the security log and specify what types of object access (such as file and registry key 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.  **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.**	Administrators
Mo[illegible]rmware environment variables Allows a user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.	Administrators
Perform volume maintenance tasks Allows a user to run volume maintenance tasks, such as Disk Cleanup and Disk Defragmenter.	Administrators
Profile single process Allows a user to perform profiling (performance sampling) on a process.  **NOTE: Software developers working on the system may need this right. Assign the right to developer users/groups only when necessary.**	Administrators
Profile system performance Allows a user to perform profiling (performance sampling) on the system.	Administrators
Remove computer from docking station Allows a user to undock a laptop from a docking station.	Administrators Users
Replace a process-level token Allows a user to modify a process's security access token. This is a powerful right used only by the system.	LOCAL SERVICE NETWORK SERVICE

User Rights	Recommended Settings
Restore files and directories Allows a user to restore backed-up files and directories. This right supercedes file and directory permissions.  **NOTE: If the network makes use of a group to restore backups, also assign this right to that group.**	Administrators
Shut down the system Allows a user to shut down Windows XP.	Administrators Users
Synchronize directory service data Allows users/groups to synchronize directory service data, also known as Active Directory synchronization.	(No one)
Take ownership of files or other objects Allows a user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Administrators

Table 5 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. Recommended Security Options settings are listed in **Table 6**. Customized security options added to the NSA templates are shaded in gray.

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 XP.

NOTE: Most security options are set via a registry key. The associated registry keys are listed for each item. Those options not containing a registry key are instead secured at the API level.

Security Attribute	Recommended Setting
Accounts: Administrator account status Controls the status of the default local Administrator account during normal operation. The Administrator account is always enabled in Safe Mode, regardless of this setting.	Enabled
Accounts: Guest account status Controls the status of the Guest account. Guest is disabled by default.  **NOTE: If the Guest account is disabled and the security option, "Network access: Sharing and security model for local accounts" is set to "Guest Only," network logons, such as those performed by the SMB Service, will fail.**	Disabled
Accounts: Limit local account use of blank passwords to console logon only Controls whether local accounts with blank passwords can log on from the network. If this setting is enabled, local accounts with blank passwords cannot be used to connect to the machine from across the network, including via Windows Network as well as Terminal Services.  **NOTE: This setting only affects local accounts. It does not affect domain accounts.** HKLM\System\CurrentControlSet\Control\Lsa\ LimitBlankPasswordUse = 1	Enabled
Accounts: Rename administrator account The Administrator account is created by default when installing Windows XP. 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 template does not define this setting due to the environment specificity of this option. However, renaming this account is a recommended setting.**  **NOTE: If anonymous accounts are not restricted from enumerating users on the system, renaming the administrator account will have limited benefit. However, if the anonymous user is prohibited from gathering account information, renaming the administrator account is provides much more benefit. See security options affecting anonymous privileges in the Network Access section of this table.**	<configure locally>

Security Attribute	Recommended Setting
Accounts: Rename guest account The Guest account is created by default when installing Windows XP, 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 template does not define this setting due to the environment specificity of this option. However, renaming this account is a recommended setting.**	<configure locally>
Audit: Audit the access of global system objects Controls the ability to audit access of global system objects. When this setting is enabled, system objects such as mutexes, events, semaphores, and DOS devices, are created with a default system access control list (SACL).  **WARNING: Enabling this option will result in large numbers of events being written to the security logs. Coupled with the fact that global system audit events are difficult to decipher, it is recommended that this option be enabled only when deemed absolutely necessary.**  **NOTE: To audit access to system objects, the "Audit object access" audit policy must be enabled.** HKLM\System\CurrentControlSet\Control\Lsa\AuditBaseObjects	Not defined
Audit: Audit the use of Backup and Restore privilege Controls the ability to audit the use of all user privileges, including Backup and Restore. If this policy is disabled, certain user rights will not be audited even if "Audit privilege use" audit policy is enabled.  **WARNING: Enabling this option will result in large numbers of events being written to the security log, especially during backup and restore operations. Therefore, it is recommended that this option be enabled only when deemed absolutely necessary.**  **NOTE: To audit user rights, the "Audit privilege use" audit policy must be enabled.** HKLM\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing	Not defined

Security Attribute	Recommended Setting
Audit: Shut down system immediately if unable to log security audits If events cannot be written to the security log, the system is halted immediately. The following Stop error appears: STOP: C0000244 {Audit Failed} An attempt to generate a security audit failed. If the system halts as a result of a full log, an administrator must log onto the system and clear the log.  **NOTE: It is generally recommended that this setting be enabled; however due to a problem that exists with auditing successful policy changes we are recommending that this setting be disabled until the issue is resolved. The problem surfaces on the first system reboot after the "Audit: Shut down system immediately if unable to log security audits" security option is enabled. Upon reboot, the system will either blue screen or hang. Apparently, there is a problem writing a policy change event to the audit log, and thus, the system crashes. Subsequent reboots will be successful. When the machine reboots, only an administrator can log on. The administrator must then reset the CrashOnAuditFail registry key from 2 back to 0 or 1 in order for other users to access the system. This behavior does not exist if successful policy change audit is not enabled.**  **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. It will also enable an attacker to effectively disable the system by simply causing the event log to fill up with garbage.** HKLM\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail =0	Disabled
Devices: Allow undock without having to log on Controls if a user can remove a computer from a docking station without being logged on. Disabling this setting requires the user to log on before requesting an undock. Once logged on, the user must have the "Remove computer from docking station" user right assignment.  **NOTE: This setting only pertains to controlled undocking, where appropriate services are stopped when the machine is undocked. There is nothing to prevent an attacker from simply ejecting the machine out of the docking station without doing a graceful disconnect.** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ UndockWithoutLogon = 0	Disabled
Devices: Allowed to format and eject removable media Determines who is allowed to format and eject NTFS media. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ AllocateDASD = 0	Administrators

Security Attribute	Recommended Setting
Devices: Prevent users from installing printer drivers This setting determines who is allowed to install a printer driver as part of adding a network printer. A print driver is a low-level device driver that has access to restricted system resources. A low-level device driver may perform actions that are not allowed by normal users. The administrator should install all drivers on a system after testing of the driver has been performed. Enabling this setting prevents unprivileged users from downloading and installing untrusted printer drivers.  **NOTE: If the printer driver already exists on the local machine, users can add network printers even with this setting enabled.** HKLM\System\CurrentControlSet\Control\Print\Providers\ LanMan Print Services\Servers\AddPrinterDrivers = 1	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only By default, any program can access the CD-ROM, possibly leaving sensitive data exposed. This setting determines whether the CD-ROM is accessible to both local and remote users simultaneously. When enabled, this setting allows only the interactively logged-on user access to the CD-ROM media. When this policy is enabled and no one is logged-on, the CD-ROM can be accessed over the network. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ AllocateCDRoms = 1	Enabled
Devices: Restrict floppy access to locally logged-on user only By default any program can access the floppy drive, possibly leaving sensitive data exposed. This setting determines whether the floppy drive is accessible to both local and remote users simultaneously. When enabled, this setting allows only the interactively logged-on user access to the floppy drive media. When this policy is enabled and no one is logged-on, the floppy drive can be accessed over the network. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ AllocateFloppies = 1	Enabled
Devices: Unsigned driver installation behavior This setting controls the response when an attempt is made to install a device driver (by means of Setup API) that has not been digitally signed. This setting allows for the following options: **Silently succeed** **Warn but allow installation** **Do not allow installation** HKLM\Software\Microsoft\Driver Signing\Policy = 1	Warn but allow installation
Domain controller: Allow server operators to schedule tasks This setting determines if Server Operators are allowed to submit jobs using the AT schedule utility. This does not affect the Task Scheduler. This setting is undefined on workstations.	Not defined
Domain controller: LDAP server signing requirements Requires that data signing be negotiated before Lightweight Directory Access Protocol (LDAP) clients can bind with the Active Directory LDAP server. This setting is undefined on workstations.	Not defined

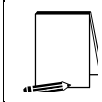
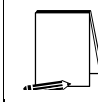
Security Attribute	Recommended Setting
Domain controller: Refuse machine account password changes Determines whether a domain controller will accept password requests for computer accounts. This setting is undefined on workstations.	Not defined
Domain member: Digitally encrypt or sign secure channel data (always) This setting controls the signing and encryption of data transmitted over the secure channel. This setting should be enabled only in an environment where all domain controllers in the domain are capable of signing or encrypting all secure channel data. This means that all domain controllers must be running Windows 2000 or Windows NT 4.0 with Service Pack 4 or higher. Otherwise, this setting should be disabled or not defined. When disabled, a secure channel can be established, but the level of encryption and signing is negotiated.  **NOTE: If this policy is enabled, the policy Domain member: Digitally sign secure channel data (when possible) is automatically enabled.** HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ RequireSignOrSeal	Not defined
Domain member: Digitally encrypt secure channel data (when possible) If enabled, this setting ensures that all secure channel traffic is encrypted if the partner domain controller is also capable of encrypting all secure channel traffic. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ SealSecureChannel = 1	Enabled
Domain member: Digitally sign secure channel data (when possible) If enabled, this setting ensures that all secure channel traffic is signed if both client and server can agree on a signing protocol. Digitally signing helps assure message integrity and authentication.  **NOTE: If Domain member: Digitally encrypt or sign secure channel data (always) is enabled, this setting is automatically enabled.** HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ SignSecureChannel=1	Enabled
Domain member: Disable machine account password changes This setting determines the ability of a domain member to change its computer account password. This setting should be disabled so domain members will attempt to change computer account passwords as specified by the setting, “Domain Member: Maximum age for machine account password.” HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ DisablePasswordChange=0	Disabled
Domain member: Maximum machine account password age This setting sets the maximum age for a computer account password to 7 days. The default setting is 30 days. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ MaximumPasswordAge=7	7 days

Security Attribute	Recommended Setting
Domain member: Require strong (Windows 2000 or later) session key When this setting is enabled, a secure channel can only be established with domain controllers that can encrypt secure channel data with a strong (128-bit) session key.  **WARNING: To enable this setting, all domain controllers in the domain must be capable of encrypting secure channel data with a strong key. This means that all domain controllers must be Windows 2000 or later. If communication to non-Windows 2000 domains is required, set this option to Disabled.** HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ RequireStrongKey=1	Enabled
Interactive logon: Do not display last user name This setting determines whether the name of the last user to log on to the computer will be displayed in the Windows logon dialog box.  **NOTE: In certain circumstances, this option may be disabled. For example, if administrators are concerned about unauthorized physical access to a sensitive system, seeing the last user logged on could be helpful.** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ DontDisplayLastUserName=1	Enabled
Interactive logon: Allow Automatic Administrator Logon Allows a system to automatically logon as 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 can be read across the network by any user that can connect to the registry. It should be deleted.** HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\AutoAdminLogon = 0	Disabled
Interactive logon: Do not require CTRL+ALT+DEL 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	Disabled
Interactive logon: Message text for users attempting to log on Systems should display a warning message before logon, indicating the private nature of the system. Many government organizations use this message box to notify 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. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ LegalNoticeText="Message text of your choice"	<Configure locally – see Appendix for sample>

Security Attribute	Recommended Setting
Interactive logon: Message title for users attempting to log on Used in conjunction with the logon text, systems should also display a warning statement on the title bar. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ LegalNoticeCaption="Caption of your choice to be displayed on the title bar"	<Configure locally – see Appendix for sample>
Interactive logon: Number of previous logons to cache (in case domain controller is not available) The number of cached logon credentials that the system retains is determined by this setting. Cached logon credentials enable users to log on to the system when the computer is not connected to the network or when the domain controller is not available.  **WARNING: With 0 cached logons, users will not be able to log on to the domain unless connected to the network. This is not a viable setting for mobile laptop users who use domain versus local accounts to log onto the laptop while away from the office.** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ CachedLogonsCount=0	0 logons
Interactive logon: Prompt user to change password before expiration This setting determines how far in advance users are warned that their password is about to expire. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ PasswordExpiryWarning=14	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation When enabled, a domain controller must authenticate the domain account that is being used to unlock the computer. When disabled, cached credentials can be used to unlock the computer.  **WARNING: If a domain controller goes down while a user's screen is locked, the user will not be able to unlock his workstation if this option is enabled.**  **NOTE: This option may not be viable for laptop systems.** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ ForceUnlockLogon=1	Enabled

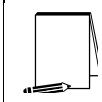
Security Attribute	Recommended Setting
Interactive logon: Smart card removal behavior This setting determines the system behavior for a logged-on user when a smart card is removed. The options follow: **No Action** **Lock Workstation** Users can remove the smart card and later return to the same session. **Force Logoff** Users are automatically logged off when the card is removed. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ ScRemoveOption=1	Lock Workstation
Microsoft network client: Digitally sign communications (always) When enabled, this setting forces SMB clients to always digitally sign SMB communications. Digitally signing SMB communications closes "man-in-the-middle" attacks and supports message authentication, which prevents active message attacks.  **NOTE: It is recommended that this option be enabled in a pure Windows 2000/XP environment** HKLM\System\CurrentControlSet\Services\LanmanWorkstation\ Parameters\RequireSecuritySignature	Not defined
Microsoft network client: Digitally sign communications (if server agrees) When enabled, the SMB client performs SMB packet signing when communicating with a SMB server that is either enabled or required to perform SMB packet signing. HKLM\System\CurrentControlSet\Services\LanmanWorkstation\ Parameters\EnableSecuritySignature=1	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers Disabling this setting prevents the SMB redirector from sending plaintext passwords to non-Microsoft SMB servers that do not support password encryption during authentication.  **WARNING: Enabling this will allow unencrypted (plain text) passwords to be sent across the network when authenticating to an SMB server that requests this option. This reduces the overall security of an environment and should only be done after careful consideration of the consequences of plain text passwords in your specific environment.** HKLM\System\CurrentControlSet\Services\LanmanWorkstation\ Parameters\EnablePlainTextPassword=0	Disabled
Microsoft network server: Amount of idle time required before suspending session Determines the amount of continuous idle time that must pass in a SMB session before the session is suspended. If client activity resumes after a disconnect, the session is automatically reestablished. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\ AutoDisconnect=15	15 minutes

Security Attribute	Recommended Setting
Microsoft network server: Digitally sign communications (always) Determines if the SMB server is required to perform SMB packet signing.  **NOTE: Enabling this option could be desirable in that it will prevent downlevel clients from using the workstation as a network server.** HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature	Not defined
Microsoft network server: Digitally sign communications (if client agrees) Determines if the SMB server performs SMB packet signing. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=1	Enabled
Microsoft network server: Disconnect clients when logon hours expire Determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogoff=1	Enabled
Network access: Allow anonymous SID/Name translation Determines if an anonymous user can request security identifier (SID) attributes for another user or use a SID to get the corresponding username.	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts This setting controls the ability of anonymous users to enumerate the accounts in the SAM. This security option allows additional restrictions to be placed on anonymous connections: **None. Rely on default permissions.** **Do not allow enumeration of SAM accounts.** This option replaces "Everyone" with "Authenticated Users" in the security permissions for resources. This setting is enabled by default on Windows XP.  **WARNING: Enabling this option will affect an administrator's ability to grant access to users in a trusted domain that does not maintain a reciprocal trust.** HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=1	Enabled

Security Attribute	Recommended Setting
Network access: Do not allow anonymous enumeration of SAM accounts and shares This setting controls the ability of anonymous users to enumerate SAM accounts and shares. This option is set to Disabled by default on Windows XP.  **NOTE: The system must be rebooted in order for the RestrictAnonymous setting to take effect.** HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=1	Enabled
Network access: Do not allow storage of credentials or .NET Passports This setting controls the storage of authentication credentials or passwords on the local system. HKLM\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=1	Enabled
Network access: Let Everyone permissions apply to anonymous users Determines what additional permissions are granted for anonymous connections to the computer. When this setting is disabled, permissions granted to the Everyone group do not apply to anonymous users. Anonymous users can only access resources for which the anonymous user has been explicitly given permissions. This option is disabled by default on Windows XP.  **NOTE: Disabling this option is the equivalent of setting RestrictAnonymous = 2 on Windows 2000.** HKLM\System\CurrentControlSet\Control\Lsa\ EveryoneIncludesAnonymous=0	Disabled
Network access: Named Pipes that can be accessed anonymously Pipes are internal communication processes that are identified by ID numbers that vary between systems. To facilitate access, pipes are given names that do not vary among systems. This setting determines which pipes will allow anonymous access. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\ NullSessionPipes	Not Defined
Network access: Remotely accessible registry paths This setting specifies registry paths that will be accessible from a remote computer. HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg\ AllowedPaths\Machine	Not Defined
Network access: Shares that can be accessed anonymously This setting specifies shares that can be accessed by anonymous users. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\ NullSessionShares	Not Defined

Security Attribute	Recommended Setting
Network access: Sharing and security model for local accounts This setting controls how network logons that use local accounts are authenticated. The "Classic" model forces network logons to use the local account credentials, whereas the "Guest only" model allows network logons to be mapped to the Guest account, regardless of the credentials presented by the user. The Classic model provides fine control over access to resources. Different types of access for a variety of users can be granted for the same resource. This option is set to Classic by default for Windows XP Professional machines joined to a domain. Standalone Windows XP machines set this option to Guest Only by default.  **NOTE: Network logons using domain accounts and interactive logons performed by using services such as Telnet or Terminal Services are not affected by this setting.**  **WARNING: The Guest only model allows any user who can access the computer over the network (including anonymous Internet users) the ability to access shared resources.** HKLM\System\CurrentControlSet\Control\Lsa\ForceGuest=0	Classic: local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password change Enabling this setting prevents the LAN Manager hash from being stored in the SAM at the next password change.  **NOTE: The LAN Manager hash is used for backwards compatibility with pre-Windows NT machines and some applications. Since it is a hash of the Windows password converted to all uppercase and treated as two 7-character passwords, it is easier to crack and is the primary target in password cracking utilities. For this reason, it is recommended that the LM hash not be stored in the SAM.**  **WARNING: Enabling this option will result in problems with communications to legacy operating systems or applications that only support LANManager authentication.** HKLM\System\CurrentControlSet\Control\Lsa\NoLMHash=1	Enabled
Network security: Force logoff when logon hours expire When this setting is enabled, client sessions with the SMB server are forcibly disconnected when the client's logon hours go beyond the user account's valid logon hours.	Enabled

Security Attribute	Recommended Setting
Network security: LAN Manager authentication level This parameter specifies the type of challenge/response authentication to be used for network logons with non-Windows 2000/XP 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 XP, Windows 2000, Windows NT 4.0 Service Pack 4 and higher as well as Windows 95/98 with the optional 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** - Registry value = 3. **Send NTLMv2 response only\refuse LM** - Registry value = 4. **Send NTLMv2 response only\refuse LM and NTLM** - Registry value = 5.  **WARNING: Some Windows 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/default.asp?scid=kb;EN=US;q272129  **WARNING: Setting this value higher than 2 on a Windows XP system could prevent some connectivity to systems that support only LM authentication (Windows 95®/98® and Windows for Workgroups®) or only NTLM (Windows NT 4.0 prior to Service Pack 4). The Active Directory Services client may be installed on Windows 9x machines to allow for NTLMv2 security.** HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel = 5	Send NTLMv2 response only\refuse LM and NTLM
Network security: LDAP client signing requirements This setting controls the signing requirements for LDAP clients. Requires that data signing be negotiated before Lightweight Directory Access Protocol (LDAP) clients can bind with the Active Directory LDAP server. HKLM\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=1	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients This setting determines the minimum security standards for an application-to-application communications session for a client. HKLM\System\CurrentControlSet\Control\Lsa\MSV1_0\ NTLMMinClientSec=537395200	Require NTLMv2 session security, Require 128-bit encryption

Security Attribute	Recommended Setting
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers This setting determines the minimum security standards for an application-to-application communications session on a server. HKLM\System\CurrentControlSet\Control\Lsa\MSV1_0\ NTLMMinServerSec=537395200	Require NTLMv2 session security, Require 128-bit encryption
Recovery console: Allow automatic administrative logon The recovery console is a command line environment that is used to recover from system problems. If this setting is enabled, the administrator account will be logged on automatically to the recovery console when it is invoked during startup. This setting should be disabled, thus, requiring a password from the recovery console. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\ RecoveryConsole\SecurityLevel=0	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders If this setting is enabled, a user has full access to all drives on the system and can copy files from the hard drive to the floppy disk. The Recovery Console SET command is available, which allows users to set the following Recovery Console environment variables: "AllowWildCards", "AllowAllPaths", AllowRemovableMedia", and "NoCopyPrompt". When this setting is disabled, copying files from the hard drive to the floppy drive is prohibited. In addition, the directories and drives that can be accessed are also limited. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\ RecoveryConsole\SetCommand=0	Disabled
Shutdown: Allow system to be shut down without having to log on This setting determines if a system can be shutdown without being logged on. If this policy is enabled, the shutdown command is available on the Windows logon screen. This setting should be disabled thus restricting the ability to shut down a system to users with credentials on the system. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ ShutdownWithoutLogon=0	Disabled
Shutdown: Clear virtual memory pagefile Virtual memory support uses a system pagefile to swap pages of memory to disk when not being used. When the pagefile is cleared at shutdown, any sensitive information that may be in virtual memory is not available to an unauthorized user who manages to directly access the pagefile.  **NOTE: Enabling this option will result in an increased shutdown time.** HKLM\System\CurrentControlSet\Control\Session Manager\ Memory Management\ClearPageFileAtShutdown=1	Enabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing This setting ensures that the TLS/SSL Security Provider uses algorithms that are FIPS compliant for encryption, hashing, and signing. FIPS compliant algorithms are those that meet standards established by the U.S. Government. HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=1	Enabled

Security Attribute	Recommended Setting
System objects: Default owner for objects created by members of the Administrators group This setting determines whether the Administrators group or an object creator is the default owner of any system objects that are created. For accountability, the object creator should be the default owner. HKLM\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=1	Object Creator
System objects: Require case insensitivity for non-Windows subsystems This setting determines whether case insensitivity is enforced for all subsystems. When this setting is enabled, case insensitivity is enforced for all directory objects, symbolic links, and IO objects. HKLM\System\CurrentControlSet\Control\Session Manager\Kernel\ ObCaseInsensitive=1	Enabled
System objects: Set safe search path for DLLs This key changes the default search order when a DLL is called from • Application directory • Current directory • System directories • Path To • Application directory • System directories • Current directory • Path This protects DLLs in the system folders from spoofing by DLLs in non-system folders. **NOTE: In Windows XP Service Pack 1 (SP1) this becomes the default behavior, *even if this setting is absent*. In other words, if the setting is missing in the registry, the default behavior in Windows XP RTM is to search the current directory before the system directories, while in Windows XP SP1, it is to search the system directories before the current directory.** HKLM\System\CurrentControlSet\Control\Session Manager\ SafeDllSearchMode = 1	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) Enabling this setting 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. HKLM\System\CurrentControlSet\Control\Session Manager\ ProtectionMode = 1	Enabled

Table 6 Security Options

Adding an Entry to Security Options

In the Windows XP, it is possible to add custom registry settings to the Security Configuration Tool Set. To accomplish this, perform the following actions:

- Copy the file `%SystemRoot%\inf\sceregvl.inf` to another file with a different name. This will ensure that a copy of the original exists in case of a problem.
- Open `%SystemRoot%\inf\sceregvl.inf` in Notepad, Wordpad, or another text editor
- Add a line in the form *regpath, type, displayname, displaytype* where
  - *regpath* – registry key value path, e.g., MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects
  - *type* – data type of the registry entry represented by a number. Possible values are REG_SZ (1), REG_EXPAND_SZ (2), REG_BINARY (3), REG_DWORD (4), REG_MULTISZ (7)
  - *displayname* – the name actually displayed in the security template, e.g., "Audit the access of global system objects"
  - *displaytype* – How the interface will display the registry value type. Possible values are Boolean (0), number (1), string (2), choices (3), multivalued (4), bitmask (5). Values 4 and 5 are available on Windows XP only. 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

NOTE: It is only necessary to modify sceregvl.inf on the system from which the security template and/or group policy are being edited. Other machines ultimately receiving the new settings via group policy need not be changed.

For more information on how to edit the Security Configuration Manager templates, refer to Microsoft Knowledge Base article Q214752, available at http://support.microsoft.com/?scid=kb;en-us;Q214752.

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 the UI," 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

6

Modifying Event Log Settings with Security Templates

Windows XP 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 7 lists recommended Event Log settings for the Application, Security, and System logs.

Event Log Settings	Recommended Settings
Maximum application log size **Maximum security log size** **Maximum system log size** 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.**	4194240 KBytes
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.	Enabled
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.  **NOTE: To ensure that no important data is lost, especially in the event of a security breach of the system, the event logs on workstations should be periodically collected via a third-party software tool before they are overwritten.**	14 days
Retention method for application Log **Retention method for security Log** **Retention method for system Log** This option sets 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.  **NOTE: This recommendation applies to workstations only. Server logs should be cleared manually.**	By days

Table 7 Event Log Options

Managing the Event Logs

This section describes basic administration of the Windows XP event logs.

Saving And Clearing the Audit Logs

To save and clear the logs:

- Select **Start → All 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** recommended **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 an audit failure, an administrator must restart the system and use the registry editor (`regedit.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 an audit log failure. While the value is 2, only the administrator can log on to the computer. This value confirms the cause of the crash. Reset the value 1

This Page Intentionally Left Blank

Chapter

7

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
- 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 template restricts the Power Users group to having no members. This is generally good security practice. However, environments using older applications or custom written line-of-business applications may require users to have additional privileges similar to the Power Users group on certain files, folders, or registry keys relating to those applications. Ideally, the needed permissions on these files and registry keys should be identified and implemented instead of adding users to the Power Users group. Under no circumstances should you add users to the Administrators group just to make your applications work.

Chapter

8

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 by editing the "Service General Setting" section of the security template. The syntax of that section is as follows:

<service name>,state,<sddl string specifying ACL>

State can take on the following values:

2 Automatic

3 Manual

4 Disabled

For example, to disable the IISADMIN service and deny all users access to it (remove any ACL), you could use the following string:

IISADMIN,4,"D:ARS:AR"

Services added to this area can be configured in the same way as the built-in services included by default. In addition, administrators can use a *security configuration attachment* to configure service-specific settings. Such an attachment consists of a DLL, an extension snap-in, and an installation kit. For more information on creating security configuration attachments, refer to the white paper *Security Configuration Toolset* http://www.microsoft.com/windows2000/techinfo/howitworks/security/sctoolset.asp.

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

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

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

The following steps describe how to configure system service settings;

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

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

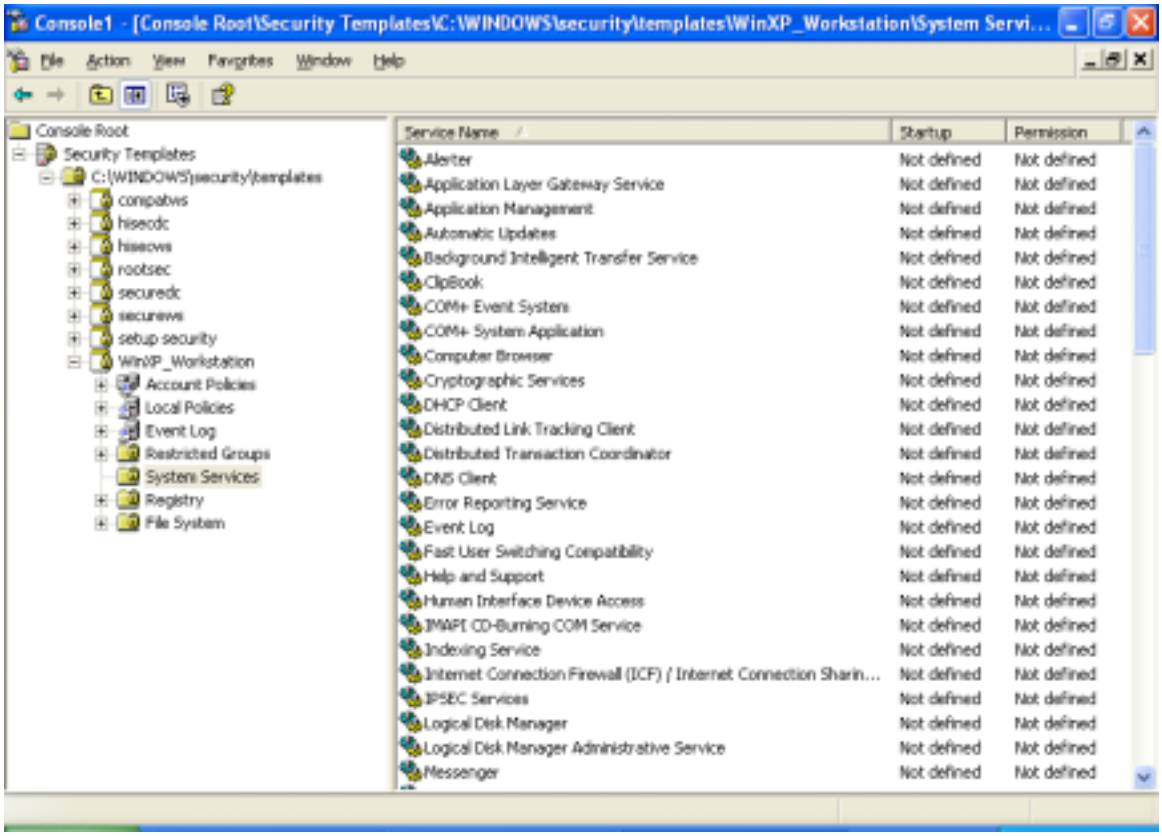


Figure 4 System Services

System Services Security

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

- Only run necessary services. For example, if the telnet service or FTP service is running on a system, but not being used, disable it.
- 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. Also, if a service is currently disabled and will remain that way, it is recommended that it be explicitly set to Disabled vice "Not defined."
- 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.

- Run services with the least privilege necessary. For example, do not run a service as a domain administrator if user privileges are sufficient.

Chapter

9

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 XP environment, some registry key permissions should be changed. The recommended changes can also be made manually using `regedit.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, some access rights will be modified. 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

Within the Windows XP inheritance model, permissions on child objects are automatically inherited from their parent. This can be seen by the check in the **Inherit from parent the permission entries that apply to child objects** checkbox in the DACL editor. Other 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 `regedit.exe`
- Right-click the desired registry key
- Select **Permissions…** from the pull-down menu

Only **Full Control**, **Read,** and **Special Permissions** appear in the permissions dialog box. However, permissions may be set with more granularity by clicking the **Advanced** button. **Table 8** shows a list of granular registry permissions. **Table 9**

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 Security Settings **window.**

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

Table 8 Registry Permissions and Descriptions

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

Table 9 Registry Permission Options

Effective Permissions

With both allow and deny permissions for multiple groups, determining what registry permissions apply to a particular user or group may be confusing. Windows XP allows an easy way to view which permissions are effectively granted to any particular user or group for a given object. To view these "effective permissions," perform the following:

- In a registry editor (e.g. regedit), right-click on a registry key
- Select **Permissions** from the pull-down menu
- Click **Advanced**
- Click the **Effective Permissions** tab
- In the **Group or username** section, click the **Select** button
- Under **Enter the object name to select**, enter the user or group name
- Click **OK**. Those permissions applying to the specified user or group will be checked.

Modifying Registry settings via the Security Templates snap-in

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

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

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

Modifying Permissions on a Registry Key

To modify the security settings on a particular registry key already specified in the security template:

- 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 shown in **Figure 5**:
  - **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 inheritance from their parent 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.

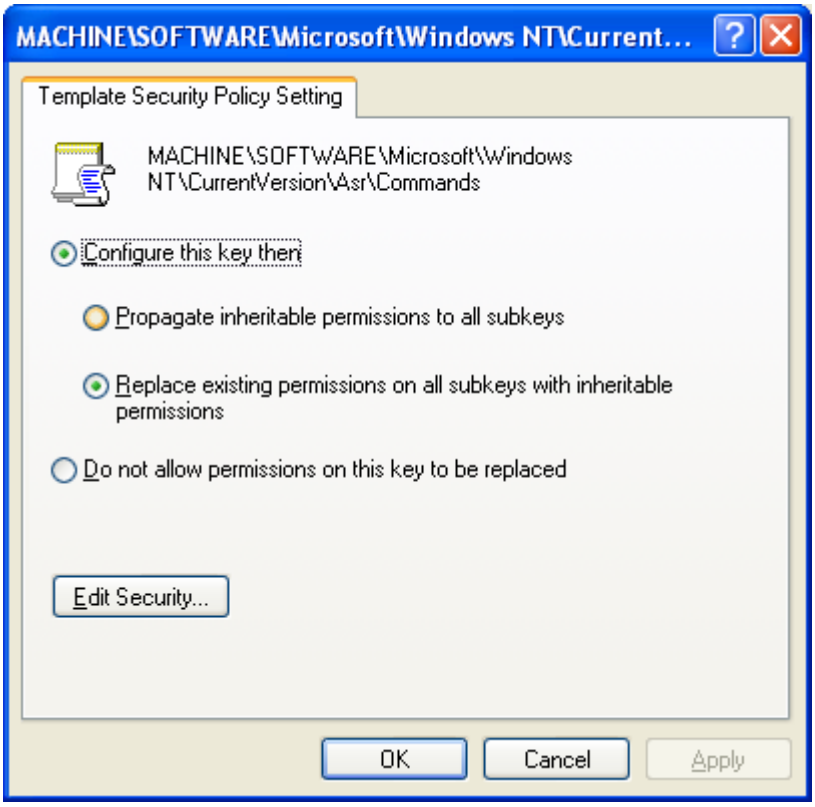


Figure 5 Registry permissions configuration options

- Click **Edit Security**
- Click the **Advanced** button. **Figure 6** shows the **Advanced Security Settings** window

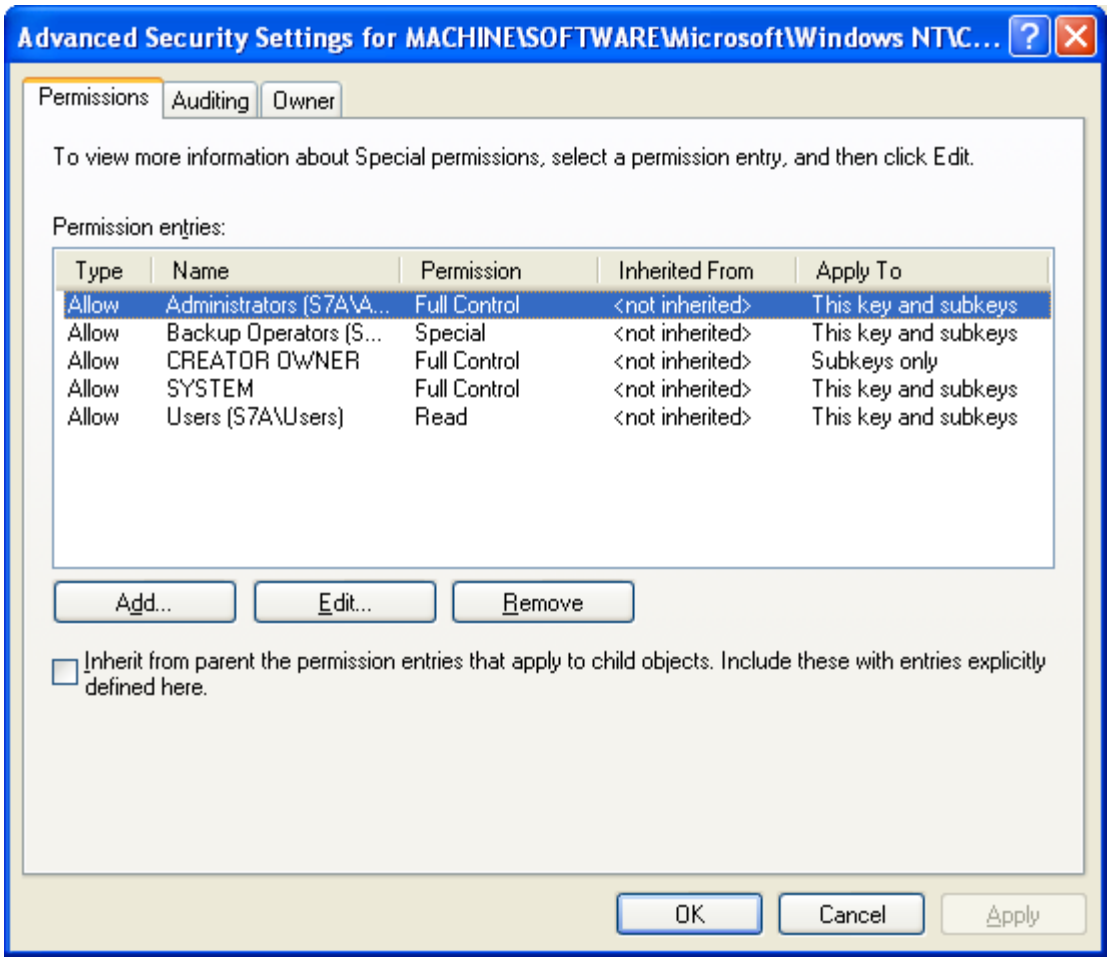


Figure 6 Advanced security settings

- If permissions from the parent key are NOT to be inherited, ensure that the **Inherit from parent the permission entries that apply to child objects** checkbox is cleared
- Modify users and groups to reflect the recommended permissions by clicking the **Add** or **Remove** buttons
- Click on a user and/or group
- Click **Edit**. A **Permission Entry** dialog box will appear as shown in **Figure 7**
- 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

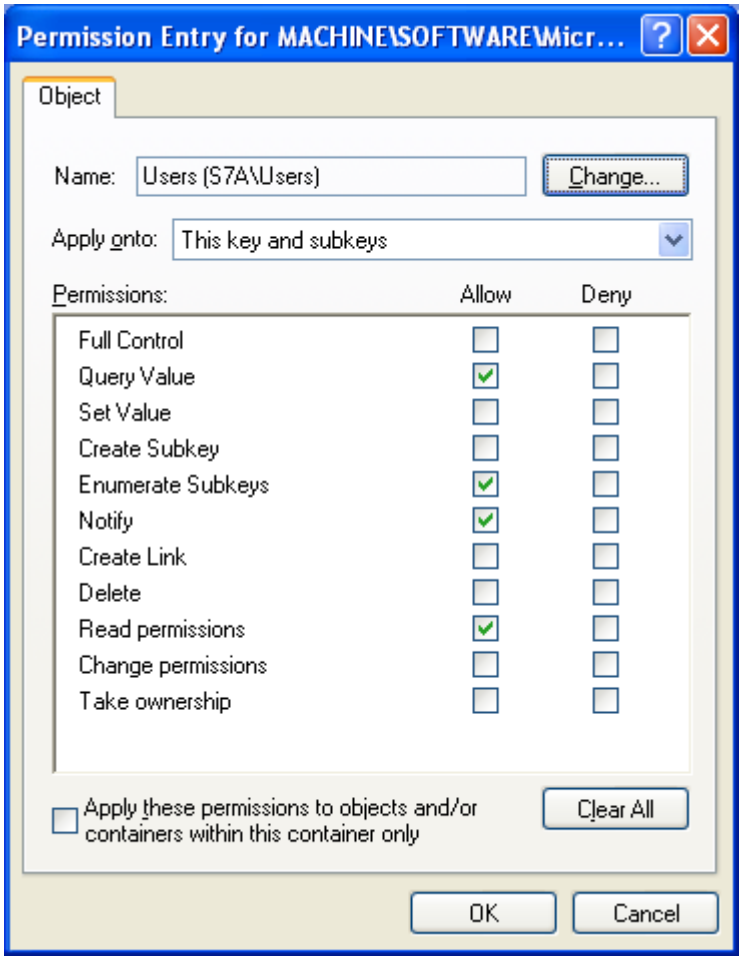


Figure 7 Permission Entry window for registry keys

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 **Database Security** dialog box will appear. This window contains the settings that are to be stored in the security configuration database for this key.
- Click **Advanced** and modify permissions according to the steps detailed in the previous **Modifying permissions on a registry key** section
- After exiting the Advanced and Database Security windows, select either the **Propagate inheritable permissions to all subkeys** or **Replace existing permissions on all subkeys with inheritable permissions** radio buttons
- Click **OK**

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 10** are assumed to inherit the permissions of their parent key if they already have **Inherit from parent the permission entries that apply to child objects** checked in their DACL. Keys with **Do not allow permissions on this key to be replaced** 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. "Ignore" means that the key is excluded from configuration.

NOTE: Many of the security settings listed below are based on Windows XP default security in the "setup security.inf" template. We have removed the Power Users and Everyone groups from the default permissions and modified some additional registry permissions.

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

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
CLASSES_ROOT Alias to MACHINE\SOFTWARE\Classes. Contains file associations and COM (Common Object Model) associations.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
\MACHINE\SOFTWARE Contains information about the software installed on the local system.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\ Cryptography\Calais	Administrators CREATOR OWNER LOCAL SERVICE SYSTEM Users	Full Control Full Control (Subkeys only) Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\MSDTC	Administrators NETWORK SERVICE SYSTEM Users	Full Control Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Read permissions Full Control Read	Propagate
\MACHINE\SOFTWARE\Microsoft\MSDTC\ Security\XAKey	Administrators NETWORK SERVICE SYSTEM	Full Control Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Read permissions Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\NetDDE Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (Subkeys only) Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\ UPnP Device Host	Administrators CREATOR OWNER LOCAL SERVICE SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\Asr\Commands Automatic Server Recovery commands. **NOTE: If using the Backup Operators group, grant this group the following permissions: Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions.**	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
\MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\Perflib Parameters for the Performance Library, which collects information for Performance Monitor. Contains a language code subkey for each spoken language configured on the Windows XP system. For example, a subkey named 009 contains counters and descriptions for the language code English (United States).	Administrators CREATOR OWNER INTERACTIVE NETWORK SERVICE SYSTEM	Full Control Full Control (Subkeys only) Read Read Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\SeCEdit Stores file locations and registry values available through the Security Configuration Editor.	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Group Policy Contains data for Group Policy settings that configure the Group Policy components of Windows XP. Contains subkeys representing each of the client-side extensions used to create settings in Group Policy.	Administrators Authenticated Users SYSTEM	Full Control Read Full Control	Propagate
\MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Installer Contains configuration information for the Windows Installer.	Administrators SYSTEM Users	Full Control Full Control Read	Propagate
\MACHINE\SOFTWARE\Microsoft\Windows \ CurrentVersion\Policies Stores registry entries managed by Group Policy. Manages entries for the following subkeys: HKLM\SOFTWARE\Policies HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies HKCU\SOFTWARE\Policies HKCU\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies	Administrators Authenticated Users SYSTEM	Full Control Read Full Control	Propagate
\MACHINE\SOFTWARE\Microsoft\Windows \ CurrentVersion\Policies\Ratings	Administrators Users	Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\Windows \ CurrentVersion\Telephony	Administrators CREATOR OWNER LOCAL SERVICE NETWORK SERVICE SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Full Control Full Control Read	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
\MACHINE\SYSTEM Stores values for the current control set or control sets that have been previously used to start Windows XP.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
\MACHINE\SYSTEM\clone	Ignore		Ignore
\MACHINE\SYSTEM\controlsetXXX (XXX represents the control set number 001-010) Contains a control set that may be used to start and run Windows XP.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Control\Class **Note: This entry is explicitly listed in the template file because it has subkeys with many different permissions. The "Propagate" property will affect only those subkeys that inherit permissions from this subkey, leaving those that do not inherit intact.**	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Control\Network **NOTE: If using the Network Configuration Operators group, grant this group the following permissions: Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions.**	Administrators LOCAL SERVICE NETWORK SERVICE SYSTEM Users	Full Control Full Control Full Control Full Control Read	Replace
\MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg The security permissions set on this key define which users or groups can connect to the system for remote registry access. If the key does not exist, anyone can remotely connect to the registry. It is highly recommended that only administrators have remote access to the registry. **NOTE: If using the Backup Operators group, grant this group the Read permission (this key only).**	Administrators LOCAL SERVICE	Full Control Read	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
\MACHINE\SYSTEM\CurrentControlSet\Control\Wmi\Security Security settings for the Windows Management Instrumentation (WMI). WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM).	Administrators Administrators CREATOR OWNER SYSTEM	Read Full Control (This key only) Full Control (Subkeys only) Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Enum 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 XP.	Ignore		Ignore
\MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles Contains system hardware profiles (changes to the initial hardware configuration stored in the Software and System keys).	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Services\AppMgmt\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\ClipSrv\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\CryptSvc\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\DNSCache **NOTE: If using the Network Configuration Operators group, grant this group the following permissions: Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions.**	Administrators LOCAL SERVICE NETWORK SERVICE SYSTEM Users	Full Control Full Control Full Control Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Services\Ersvc\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\IRENUM\Security	Administrators SYSTEM	Full Control Full Control	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
\MACHINE\SYSTEM\CurrentControlSet\Services\Netbt **NOTE: If using the Network Configuration Operators group, grant this group the following permissions: Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions.**	Administrators LOCAL SERVICE NETWORK SERVICE SYSTEM Users	Full Control Full Control Full Control Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Services\Netdde\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Netddedsdm\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess **NOTE: If using the Network Configuration Operators group, grant this group the following permissions: Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions.**	Administrators LOCAL SERVICE NETWORK SERVICE SYSTEM Users	Full Control Full Control Full Control Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Services\Rpcss\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Samss\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Scarddrv\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Scardsvr\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers Only exists if the SNMP service has been started on the system. Defines the users that can gather SNMP information.	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\ SNMP\Parameters\ValidCommunities Only exists if the SNMP service has been started on the system. Restricts normal users from gathering SNMP information.	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Stisvc\Security	Administrators SYSTEM	Full Control Full Control	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
\MACHINE\SYSTEM\CurrentControlSet\Services\SysmonLog\Log Queries	Administrators CREATOR OWNER NETWORK SERVICE SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Full Control Read	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Tapisrv\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip **NOTE: If using the Network Configuration Operators group, grant this group the following permissions: Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions.**	Administrators LOCAL SERVICE NETWORK SERVICE SYSTEM Users	Full Control Full Control Full Control Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Services\W32time\Security	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\Wmi\Security	Administrators SYSTEM	Full Control Full Control	Replace
USERS\.DEFAULT Profile that is used to generate new profiles when users first log on. It is also used while the Windows XP CTRL+ALT+DEL logon message is displayed.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
USERS\.DEFAULT\Software\Microsoft\NetDDE Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (Subkeys only) Full Control	Replace
USERS\.DEFAULT\Software\Microsoft\SystemCertificates\Root\ProtectedRoots	Administrators SYSTEM Users	Full Control Full Control Read	Replace

Table 10 Recommended Registry Permissions

This Page Intentionally Left Blank

Chapter

10

Modifying File System Security Settings with Security Templates

The NT File System (NTFS) provides a way to safeguard valuable information. NTFS works in concert with the Windows user account system to allow authenticated users access to files**. To implement the highest level of security, always format Windows XP partitions with the NT File System**.

The security provided by NTFS is based on system controls that are managed by the Windows XP operating system. As long as Windows XP 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 XP inheritance.

Converting to NTFS

A non-NTFS volume can be converted at any time using the Convert.exe program (`%SystemRoot%\system32\convert.exe`). The `convert` command must be executed from a command prompt window using an administrative account.

New in Windows XP, the `convert.exe` command automatically applies default NTFS permissions to the volume. Previously, in Windows NT 3.x, 4.0 and Windows 2000, converting a volume to NTFS would grant the Everyone group Full Control access to the entire volume.

The steps needed to convert a drive to NTFS are as follows:

- Select **Start → Run → cmd.exe** to open a command prompt
- At the command prompt, type:

```
convert volume /FS:NTFS [/V]
```

NOTE: Substitute the drive letter of the partition to be converted for *volume* (i.e. C:)

NOTE: The /v switch is optional and runs the program in verbose mode.

- Restart the system

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

Granularity of file permissions

File permissions may be set with more granularity than those listed in the **Permissions** dialog box by clicking the **Advanced** button. **Table 11** shows a list of granular file permissions. **Table 12** and **Table 13** File Permissions Option show which granular permissions to select in order to achieve certain higher-level permissions for folders and files.

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

Table 11 File Permissions and Descriptions

Folder Permissions:

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

Table 12 Folder Permissions Options

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

File Permissions:

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

Table 13 File Permissions Options

Effective Permissions

With both allow and deny permissions for multiple groups, determining what file permissions apply to a particular user or group may be confusing. Windows XP allows an easy way to view which permissions are effectively granted to any particular user or group for a given object. To view these "effective permissions," perform the following:

- In Windows Explorer, right-click on the file or folder
- Select **Properties** from the pull-down menu
- Click the **Security** tab
- Click **Advanced**
- Click the **Effective Permissions** tab
- In the **Group or username** section, click the **Select** button
- Under **Enter the object name to select**, enter the user or group name
- Click **OK**. Those permissions applying to the specified user or group will be checked.

Modifying File System settings via the Security Template snap-in

The recommended changes to system files and folders are listed in **Table 14.**

The necessary changes can be made in one of two ways. The first method is to use the Security Configuration Manager 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 security template:

- 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 as shown in **Figure 8**:
  - **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 **Inherit from parent the permission entries that apply to child objects** 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. However, folders which are defined in the template with the “Do not allow permissions on this file or folder to be replaced” setting will not be affected.

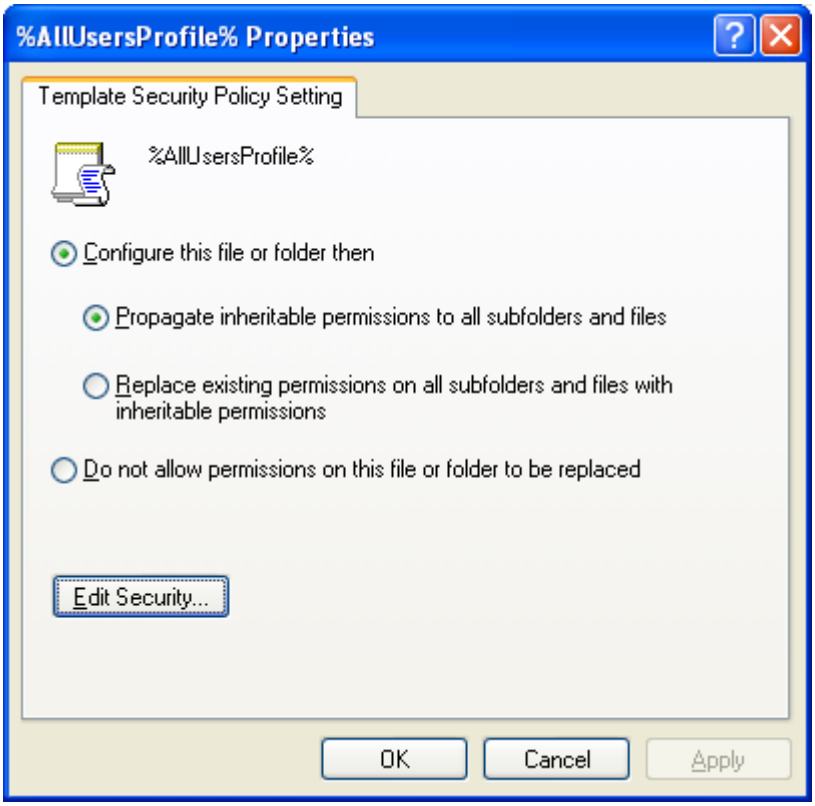


Figure 8 File permissions configuration options

- Click **Edit Security**
- Click **Advanced**
- If permissions from the parent key are NOT to be inherited, ensure that the **Inherit from parent the permission entries that apply to child objects** checkbox is unchecked
- Modify users and groups to reflect the recommended permissions by clicking the **Add** or **Remove** buttons
- Click the user or group to be edited.
- Click **Edit**. A **Permission Entry** dialog box will appear as shown in **Figure 9.**
- In the **Apply** onto pull-down menu, select the correct configuration (e.g., **This folder, subfolders, and files**).
- Click **OK → OK → OK → OK** to exit

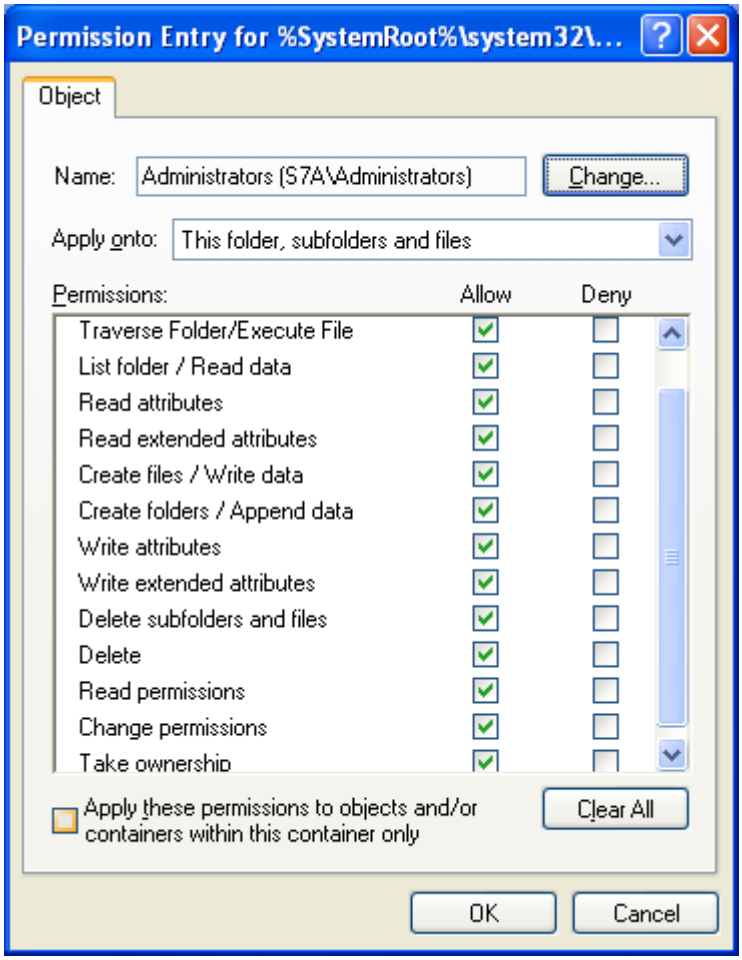


Figure 9 Permission Entry window for folders

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 **Database Security** dialog box will appear
- Configure the permissions according to the steps detailed in the previous **Modifying permissions on a file or folder** section

Excluding files or folders from the security configuration

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

To exclude an object:

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

Recommended File and Folder Permissions

Folders and files not explicitly listed below in **Table 14** are assumed to inherit the permissions of their parent folder. Folders with **Do not allow permissions on this file or folder to be replaced** 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. "Ignore" means that the folder is excluded from configuration.

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 Windows XP default security in the "setup security.inf" template. We have removed the Power Users and Everyone groups from the default permissions and modified additional folder and file permissions.

Folders and files in **Table 14** are alphabetized as they appear in the security templates GUI.

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%AllUsersProfile% Folder containing desktop and profile attributes for all users, usually C:\Documents and Settings\All Users.  **NOTE: If Windows XP has been reinstalled over another copy of the operating system, additional All Users profile folders will be created in the Documents and Settings folder. Typically, the new profile is called All Users.WINDOWS or All Users.COMPUTERNAME. Prior copies of the All Users folder, although still existing, will not be used. The %AllUsersProfile% environment variable will automatically point to the profile currently in use. To determine which profile is actually being used, see the HKLM\Software\Microsoft\ Windows NT\ CurrentVersion\ProfileList\ AllUsersProfile registry key value.**	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%AllUsersProfile%\Application Data Contains application state data.	Administrators CREATOR OWNER SYSTEM Users Users	Full Control Full Control (Subfolders and files only) Full Control Read, Execute Write (This folder and subfolders)	Propagate
%AllUsersProfile%\Application Data\ Microsoft Contains Microsoft application state data.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%AllUsersProfile%\Application Data\ Microsoft\Crypto\DSS\MachineKeys	Administrators SYSTEM Users	Full Control Full Control List folder, Read attributes, Read extended attributes, Create files, Create folders, Write attributes, Write extended attributes, Read permissions (This folder only)	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%AllUsersProfile%\Application Data\ Microsoft\Crypto\RSA\MachineKeys	Administrators SYSTEM Users	Full Control Full Control List folder, Read attributes, Read extended attributes, Create files, Create folders, Write attributes, Write extended attributes, Read permissions (This folder only)	Replace
%AllUsersProfile%\Application Data\ Microsoft\Dr Watson Folder containing the Dr. Watson application error log.	Administrators CREATOR OWNER SYSTEM Users Users	Full Control Full Control (Subfolders and files only) Full Control Read, Execute Traverse folder, Create files, Create folders (Subfolders and files only)	Replace
%AllUsersProfile%\Application Data\ Microsoft\Dr Watson\drwtsn32.log Dr. Watson application error log file. **NOTE: This setting only has significance if the drwtsn32.log file has already been created. Alternately, instead of writing the log file to a common location and risk all users on the system having access to it, the drwtsn32.exe application can be run and a new log and crash dump location can be specified.**	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subfolders and files only) Full Control Modify	Replace
%AllUsersProfile%\Application Data\ Microsoft\HTML Help	Administrators SYSTEM Users	Full Control Full Control Full Control	Replace
%AllUsersProfile%\Application Data\ Microsoft\Media Index	Administrators SYSTEM Users Users Users	Full Control Full Control Read, Execute Create files, Create folders, Write attributes, Write extended attributes, Read permissions (This folder only) Write (Subfolders and files only)	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%AllUsersProfile%\Documents **NOTE: When viewing the %AllUsersProfile% folder in Windows Explorer, the Documents subfolder appears as "Shared Documents."**	Administrators CREATOR OWNER SYSTEM Users Users	Full Control Full Control (Subfolders and files only) Full Control Read, Execute Write (This folder and subfolders)	Replace
%AllUsersProfile%\Documents\desktop.ini	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%AllUsersProfile%\DRM	Ignore		Ignore
%ProgramFiles% Folder in which applications are installed. By default, this is %SystemDrive%\Program Files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subfolders and files only) Full Control Read, Execute	Replace
%SystemDrive% Drive on which Windows XP is installed. Contains important system startup and configuration files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subfolders and files only) Full Control Read, Execute	Propagate
%SystemDrive%\autoexec.bat **c:\autoexec.bat** Required by some legacy DOS applications for path parsing. The actual initialization file for DOS applications is %SystemRoot%\system32\autoexec.nt.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\boot.ini **c:\boot.ini** Boot menu.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\config.sys **c:\config.sys** Required by some legacy DOS applications for path parsing. The actual initialization file for DOS applications is %SystemRoot%\system32\config.nt.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\Documents and Settings Folder containing user and default profiles.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemDrive%\Documents and Settings\ Administrator Folder containing the built-in Administrator profile.	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\Documents and Settings\ Default User Folder containing default desktop and profile attributes for users logging on for the first time.  **NOTE: If Windows XP has been reinstalled over another copy of the operating system, additional Default User profile folders will be created in the Documents and Settings folder. Typically, the new profile is called Default User.WINDOWS or Default User.COMPUTERNAME. Prior copies of the Default User folder, although still existing, will not be used. Unlike the All Users profile, Default User does not have an associated environment variable, Therefore, the currently-used profile should be specified in this template entry if different than Default User. To determine the Default User profile currently being used, see the HKLM\Software\Microsoft\ Windows NT\ CurrentVersion\ProfileList\ DefaultUserProfile registry key value.**	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\io.sys Empty file that serves as a placeholder for DOS applications that use it to determine where the system partition is.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\msdos.sys Empty file that serves as a placeholder for DOS applications that use it to determine where the system partition is.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\ntbootdd.sys Copy of the SCSI device driver. Used when using SCSI or Signature syntax in boot.ini.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\ntdetect.com **c:\ntdetect.com** Hardware detector during Windows XP boot.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\ntldr **c:\ntldr** Windows XP operating system loader.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\System Volume Information Accessible only by SYSTEM.	Ignore		Ignore
%SystemRoot% Folder in which the Windows XP operating system is installed. For a new installation of Windows XP, by default this is called WINDOWS. Upgrades to Windows XP will maintain the older system root folder name, usually winnt if they were upgraded from Windows NT 4.0 or 2000 and WINDOWS if they were upgraded from Windows 9x.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subfolders and files only) Full Control Read, Execute	Replace
%SystemRoot%\$NtServicePackUninstall$ Contains older versions of system files necessary to back off a service pack.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\CSC Contains all offline files requested by any user on the computer. CSC means “client side caching”.	Administrators	Full Control	Replace
%SystemRoot%\Debug Contains various log files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subfolders and files only) Full Control Read, Execute	Propagate
%SystemRoot%\Debug\UserMode Contains logs for group policy application to users.	Administrators SYSTEM Users Users	Full Control Full Control Traverse folder, List folder, Create files (This folder only) Write data, Append data (Files only)	Propagate
%SystemRoot%\Debug\UserMode **userenv.log** Policy application log file.	Administrators SYSTEM Users	Full Control Full Control Write data, Append data	Replace
%SystemRoot%\Installer	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\Offline Web Pages Folder containing web pages that have been downloaded for off-line viewing.	Ignore		Ignore
%SystemRoot%\Prefetch Contains data files related to the speed at which applications start.	Administrators Administrators SYSTEM	Full Control (This folder only Read, Execute (Files only) Full Control (Files only)	Replace
%SystemRoot%\regedit.exe Registry editing tool.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Registration Folder containing Component Load Balancing (CLB) registration files read by COM+ applications.	Administrators SYSTEM Users	Full Control (This folder and files) Full Control (This folder and files) Read (This folder and files)	Replace
%SystemRoot%\Registration\CRMLog	Administrators CREATOR OWNER SYSTEM Users Users	Full Control Full Control (Subfolders and files only) Full Control Traverse folder, List folder, Read attributes, Read extended attributes, Create files, Read permissions (This folder only) Read data, Read attributes, Read extended attributes, Write data, Append data, Write attributes, Write extended attributes, Delete, Read permissions (Files only)	Replace
%SystemRoot%\repair Backup files of SAM database and other important registry and system files to be used during a system repair. Updated if NTBACKUP is used when the option to back up system state files is enabled.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\security Contains security templates and analysis databases.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (Subfolders and files only) Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\system32 Contains core operating system files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subfolders and files only) Full Control Read, Execute	Replace
%SystemRoot%\system32\arp.exe Displays and modifies the IP to MAC address translation tables of the address resolution protocol (ARP).	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\at.exe Schedules programs to run at a specified date and time.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\ciadv.msc Microsoft common console for Indexing Service.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\Com\comexp.msc Microsoft common console for Component Services.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\compmgmt.msc Microsoft common console for Computer Management.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\config Contains registry hive files and event logs.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\devmgmt.msc Microsoft common console for Device Management.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\dfrg.msc Microsoft common console for Disk Defragmenter.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\diskmgmt.msc Microsoft common console for Disk Management.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\dllcache Contains copies of protected system files. These copies are used by the System File Checker to repair corrupted or modified system files.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (Subfolders and files only) Full Control	Replace
%SystemRoot%\system32\eventvwr.msc Microsoft common console for Event Viewer.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\fsmgmt.msc Microsoft common console for Shared Folders.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\gpedit.msc Microsoft common console for Group Policy.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\Group Policy Folder containing local Group Policy Objects.	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\system32\ias Contains databases for the Internet Authentication Service.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
%SystemRoot%\system32\lusrmgr.msc Microsoft common console for Local Users and Groups.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\MSDTC Contains files for MS Distributed Transaction Coordinator, which is required for Microsoft Transaction Server.	Administrators NETWORK SERVICE SYSTEM	Full Control Read, Write, Execute Full Control	Propagate
%SystemRoot%\system32\nbtstat.exe Displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\netsh.exe Command-line network configuration tool.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\netstat.exe Displays protocol statistics and current TCP/IP connections.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\nslookup.exe Displays DNS information.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\Ntbackup.exe File system backup program.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\NTMSData Default location for the Removable Storage database.	Administrators SYSTEM	Full Control Full Control	Propagate
%SystemRoot%\system32\ntmsmgr.msc Microsoft common console for Removable Storage.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\ntmsoprq.msc Microsoft common console for Removable Storage Operator Requests.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\perfmon.msc Microsoft common console for Performance Monitor.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\rcp.exe Program used to execute remote procedure calls.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\reg.exe Command-line tool for editing and querying the registry.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\regedt32.exe Pointer to regedit.exe. In previous versions of Windows NT (including Windows 2000) this was an additional registry editing tool.	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\system32\regini.exe Command-line tool for editing and querying the registry.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\rexec.exe Program used to execute remote calls.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\route.exe Program used to manipulate network routing tables.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\rsh.exe Program used to execute a remote shell.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\RSoP.msc Microsoft common console for Resultant Set of Policy.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\secedit.exe Security configuration and analysis tool.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\secpol.msc Microsoft common console for Local Security Policy.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\services.msc Microsoft common console for Services.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\Setup Contains optional component manager files.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemRoot%\system32\spool\Printers Printer spool.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subfolders and files only) Full Control Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (This folder and subfolders)	Replace
%SystemRoot%\system32\systeminfo.exe Program that queries for basic system information.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\tftp.exe Uses the Trivial File Transfer Protocol service to transfer files to and from a remote computer without authentication.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\system32\wmimgmt.msc Microsoft common console for Windows Management Instrumentation.	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\Tasks Folder containing jobs scheduled by Task Scheduler	Ignore		Ignore
%SystemRoot%\Temp Folder containing temporary files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subfolders and files only) Full Control Traverse folder, Create files, Create folders (This folder and subfolders)	Replace

Table 14 Recommended Folder and File Permissions

Chapter

11

Security Configuration and Analysis

Once the appropriate security templates have been modified, security analysis and configuration can be performed via the Security Configuration and Analysis snap-in or command line operations. This procedure should be conducted when applying a security configuration to a local system. For instructions on importing security templates into Group Policy, see **Chapter 12**.

WARNING: Applying a secure configuration to a Windows XP 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 → All Programs → Administrative Tools**.

NOTE: More than one snap-in can be loaded into the MMC at one time. For example, 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 10**.

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

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

- Click **Open**

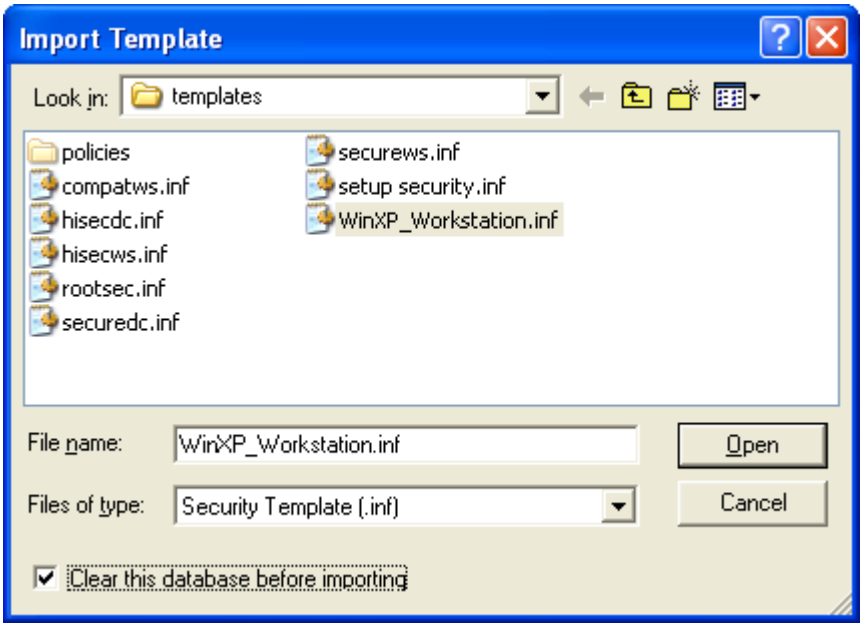


Figure 10 Configuration File Selection

Secedit Command Line Options

`Secedit.exe`, introduced in Chapter 2, is useful for performing security analyses and configurations via the command line and batch and/or scheduled programs. The command line syntax for secedit when used for system analysis or configuration is:

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

Table 15 explains the parameter syntax for `secedit.exe` options.

Parameter	Description
/analyze	Performs an analysis
/configure	Performs a configuration
/cfg filename	Path to a configuration file that will be appended to the database prior to performing the analysis
/db filename	Path to the database that secedit will perform the analysis against. If this parameter is not specified, the last configuration/analysis database is used. If there is no previous database, %SystemRoot%\Security\Database\secedit.sdb is used.  **NOTE: It is recommended that a new database be created for each analysis and configuration coupling.**
/log LogPath	Path to log file for the process. If not provided, progress information is output to the console.  **NOTE: Log information is appended to the specified log file. User must specify a new file name if a new log file is to be created.**
/verbose	Specify detailed progress information
/quiet	Suppress screen and log output
/overwrite	Overwrite the named database with the given configuration information.  **NOTE: Configuration files can be appended to or overwrite database information that has been previously created. Appending is the default. Specify the /overwrite option to overwrite the current database.**  **WARNING: To avoid confusion and accidental combining of configurations, it is recommended that this option be included every time a new analysis or configuration is performed.**

Parameter	Description
/areas Areas	Only relevant when using the /configure switch. Specifies the security areas to be processed. The following areas are available: SECURITYPOLICY - Local policy and domain policy for the system, including account policies, audit policies, etc. GROUP_MGMT - Restricted Group settings USER_RIGHTS - User rights assignments DSOBJECTS - Security on directory objects REGKEYS - Security permissions on local registry keys FILESTORE - Security permissions on local file system SERVICES - Security configuration for all defined services  **NOTE: If the /areas switch is not used, the default is all security areas. If used, each area name should be separated by a space.**

Table 15 Secedit Command Line Parameters

NOTE: The secedit /refreshpolicy option (used to force a group policy update) that was available in Windows NT and Windows 2000 no longer exists in Windows XP. This command has been replaced by the gpupdate.exe command. See Chapter 12 for more details on gpupdate.

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 command prompt window:

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

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

Performing a Security Analysis via the GUI

Figure 11 shows a sample result of a security analysis via the Security Configuration and Analysis snap-in. The following steps should be followed to perform a security analysis via the GUI:

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

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

- Click **OK**

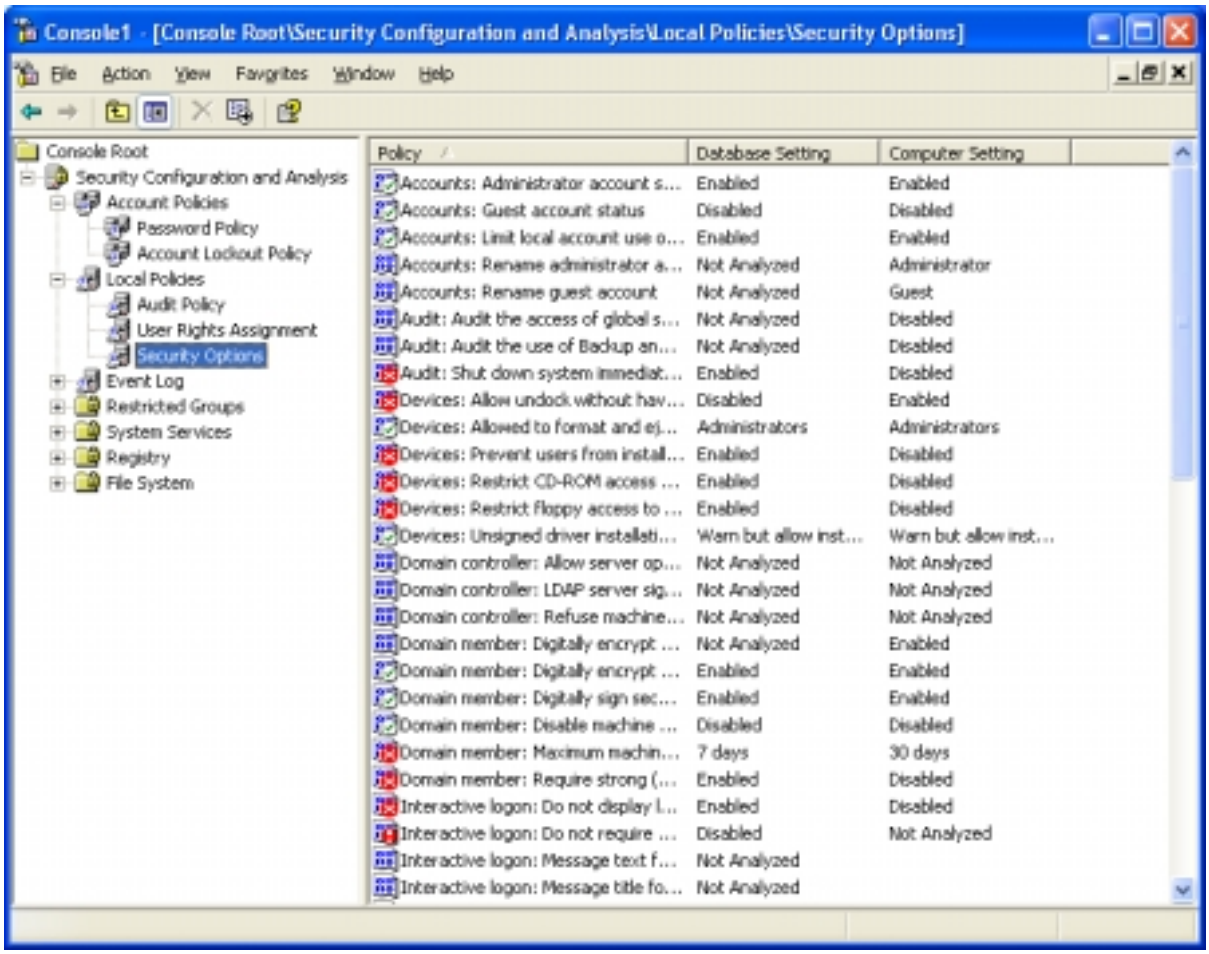


Figure 11 Results of a Security Analysis

Configuring a System

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

Configuring a System via the Command Line

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

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

WARNING: Failure to enter a new database name each time a configuration is made or specify the /overwrite option may result in unpredictable behavior by 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 "WinXP_workstation.inf" /db newdb.sdb /log logfile.txt /overwrite /areas REGKEYS FILESTORE`

This example will import the `WinXP_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

12

Applying Windows XP Group Policy in a Windows 2000 Domain

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

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

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

Overview

Windows XP Group Policy introduces many new options previously not included in Windows 2000. However, Windows 2000 domain controllers are still able to push group policy to Windows XP clients via Active Directory.

In order to take advantage of all the new Windows XP settings and features, the GPO must be edited on a Windows XP machine. An administrator can, however, perform subsequent GPO management (e.g. linking the GPO to domains or OUs) from the Windows 2000 domain controller. If a GPO is applied to a container containing both Windows XP and Windows 2000 systems, the Windows 2000 systems will ignore the Windows XP-specific settings, only configuring those options the Windows 2000 clients understand. Windows XP machines will correctly apply all settings. Review the *Guide to Securing Microsoft Windows 2000 Group Policy* prior to applying any GPOs on a Windows 2000 domain. Also, see the Microsoft article on "Upgrading Windows 2000 Group Policy for Windows XP" at http://support.microsoft.com/support/kb/articles/Q307/9/00.asp.

Security Settings Extension

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

The Security Settings extension is located under **Computer Configuration\Windows Settings\Security Settings** within a GPO and can be accessed via the Group Policy MMC snap-in. Security Settings are computer, not user, specific and include all areas present in the security templates (e.g. Account Policies, Local Policy, etc.), with the addition of Public Key Policies and IP Security Policies on Active Directory.

Creating a Window XP GPO

A Windows XP GPO must be edited on a Windows XP machine. To open and/or create a GPO, perform the following steps **from a Windows XP system already joined to a domain**:

- Run the Microsoft Management Console (`mmc.exe`)
- Select **Console → Add/Remove Snap-in**
- Click **Add**
- Select **Group Policy**
- Click **Add**
- A **Select Group Policy Object** window will appear. Under the **Group Policy Object** section, by default **Local Computer** will be listed. To change the GPO to edit, click the **Browse** button
- Within the domain, navigate to the container to which the GPO will apply. Once the container is displayed, either select an already-existing GPO or click on the second icon at the top of the window to create a new GPO, then select this GPO
- Click **OK**
- Click **Close**
- Click **OK**

Importing a Security Template into a GPO

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

- In the Group Policy snap-in, navigate to the **Computer Configuration\Windows Settings\Security Settings** node
- Expand the **Security Settings** node before importing a template. **Figure 12** shows the expanded **Security Settings** extension.

WARNING: Due to a bug in the MMC, failure to expand the Security Settings node prior to importing a template will result in an error in loading the template.

- Right-click **Security Settings**
- Select **Import Policy** from the pull-down menu

- The **Import Policy From** window will initially display all template files in the `%SystemRoot%\security\templates` folder. Select a template from this folder or browse to find the appropriate template
- Click **Open**
- The settings in the selected template file will now be imported into the **Security Settings** node. You may view and modify these settings by navigating down through the **Security Settings** tree

WARNING: In order for a new GPO to apply correctly, you must register a modification to it. Simply importing a template into a new GPO isn't seen as a change despite the fact that closing the GPO in the Group Policy snap-in, then opening it again at a later time will show that the imported security settings have been retained. The GPO will be considered empty and not applied when group policies are refreshed. To register a change, edit anything in the GPO after importing the security template, even if you change a setting, then change it back again.

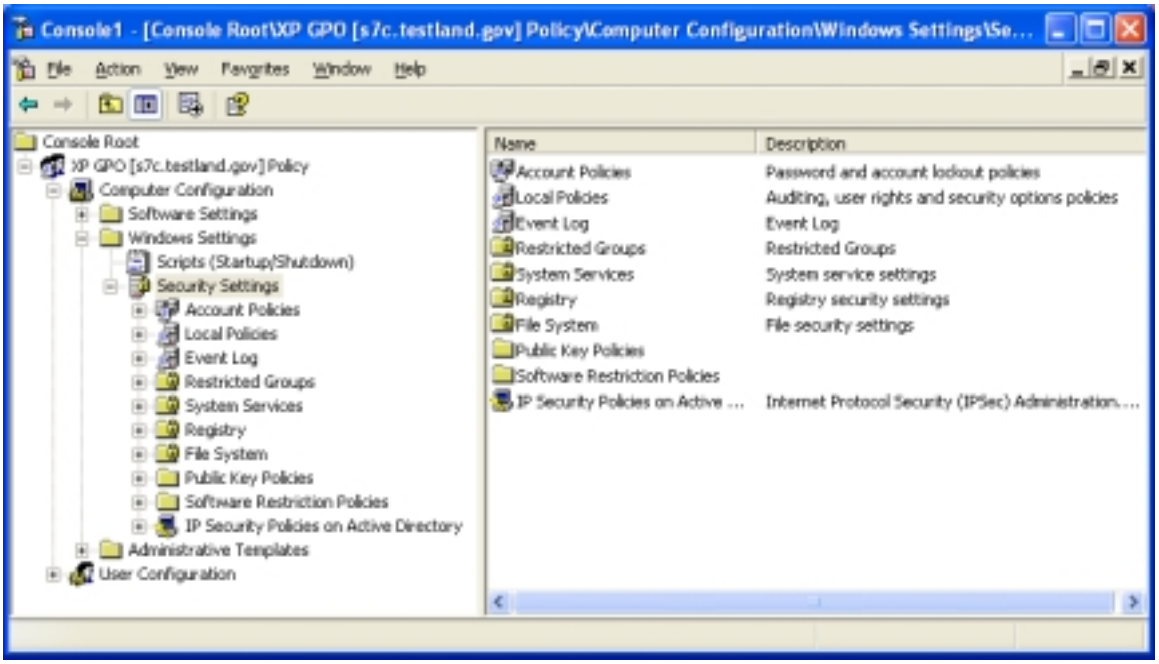


Figure 12 Security Settings extension in a GPO

Managing a Windows XP GPO from a Windows 2000 Domain Controller

As stated earlier, once a Windows XP GPO has been edited on a Windows XP machine, subsequent GPO management (e.g. linking the GPO to domains or Organizational Units) can be performed from a Windows 2000 domain controller.

When trying to view a Windows XP GPO via a Windows 2000 domain controller, navigating down to the **Computer Configuration\Windows Settings\Security Settings** section may result in a "Windows cannot open template file" message in the right pane. This will occur if any Windows XP-unique groups and/or users (e.g. LOCAL SERVICE, NETWORK SERVICE) are listed in any file or registry permissions configured in Security Settings. Even though the security settings cannot be viewed via Windows 2000, the GPO will still be applied correctly.

Local Group Policy Object

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

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

The LGPO does not have the full number of settings available with Active Directory Group Policy. For example, under the Security Settings node, only Account Policies and Local Policies are available. Thus, while a security template can be imported into the local policy, only the settings available to local policy will actually be imported. Additional settings, such as registry and file permissions, can be applied locally via Security Configuration and Analysis.

Forcing a Group Policy Update

Group Policy is periodically updated via Active Directory. The default setting updates workstation policy every 90 minutes.

To force a Group Policy refresh on a local machine, use the `gpupdate.exe` command-line tool. Typing `gpupdate /?` will give a complete listing of command line options. As an example, to force an update of the computer configuration portion of Group Policy, type:

```
Gpupdate /target:computer /force
```

Viewing the Resultant Set of Policy

Multiple GPOs can be applied to domain objects depending on which containers the objects are in. For example, a GPO set at the domain level will apply to all domain computers, and GPOs for different Organizational Units (OUs) will then be applied to objects in that OU. Manually determining what GPOs were applied and in what order can be a daunting task, especially in a complex domain structure. This makes troubleshooting Group Policy problems difficult. However, Windows XP offers two tools, Resultant Set of Policy (RSoP) and gpresult.exe, to show how GPOs were applied to an object.

RSoP Snap-in

RSoP.msc is an MMC snap-in that displays the aggregate settings of all policies applied to the local computer. To open the snap-in, type `RSoP.msc` from the command line or add the Resultant Set of Policy snap-in while in the MMC. **Figure 13** shows the RSoP snap-in.

For each group policy setting, RSoP shows the **Computer Setting** (how the computer is currently configured) and the **Source GPO** (which GPO ultimately set that current configuration). For more information on RSoP, see http://www.microsoft.com/technet/prodtechnet/winxppro/proddocs/RSPintro.asp.

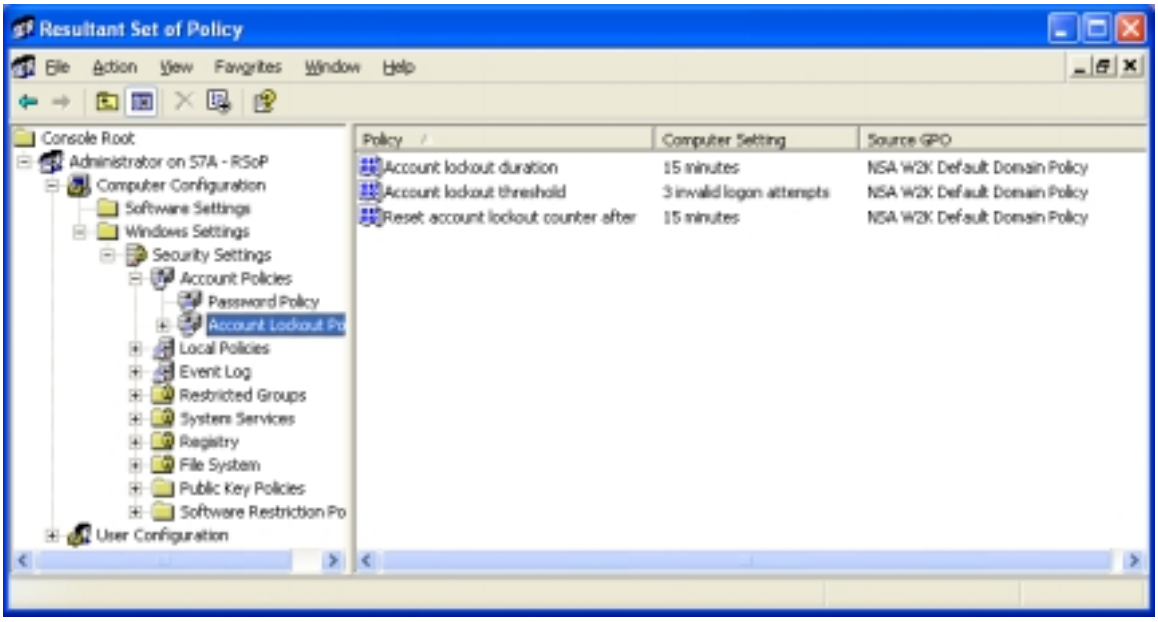


Figure 13 RSoP snap-in

Gpresult.exe

`Gpresult.exe` is a command-line tool that gives statistics on when Group Policy was last applied to the computer, what GPOs were applied and in what order, and any GPOs that were not applied because of filtering. Gpresult can also collect information about a remote system.

To view all the command-line options for gpresult, at the command line type:

```
gpresult /?
```

Known Issues

This section addresses several known issues involving the interoperability of Windows XP Professional within a Windows 2000 domain.

RestrictAnonymous Setting and "User must change password at next logon"

Windows XP does not by default grant the anonymous user (null connection) the same privileges as the Everyone group as is the case in Windows NT and Windows 2000. This may lead to potential problems when a user account in a Windows 2000 domain has the **User must change password at next logon** option selected and the RestrictAnonymous registry key on the Windows 2000 domain controller is set so that the anonymous user has no permissions unless explicitly given (registry value = 2) as is recommended in the NSA Windows 2000 security guide.

Whereas from a Windows 2000 Professional client a user has no problems logging on and changing his password when prompted, from a Windows XP client, the user is presented with a "You do not have permission to change password" error after entering a new password. The only solution is backing off the RestrictAnonymous security setting on the Windows 2000 domain controller to either 0 or 1. Note that relaxing the Windows

2000 setting opens up the domain controller to numerous information-gathering tactics that could be used by an attacker. Even if the registry key is set = 1, there are several tools that can circumvent this setting and still enumerate user account information. The security risks in this case must be carefully weighed against any potential benefit of forcing users to change their passwords on next logon from Windows XP clients.

Chapter

13

Remote Assistance/Desktop Configuration

Like all remote-control technology, Remote Assistance and Remote Desktop have security implications that must be considered prior to using them. For the highest level of security, it is not recommended that remote-control technology be used on operational networks. However, it is understood that this technology can provide operational benefits to customers. This section addresses security recommendations that can be implemented to improve the security of the remote desktop and/or remote assistance capabilities if it is desired to use this technology.

Remote Assistance

Remote Assistance (RA) is a capability that allows a user, referred to as a novice, to request assistance from another person, referred to as the expert. Using this technology the expert may view the novice's computer screen and send them messages or, if the novice's computer settings allow it, the expert has the ability to take control of the novice's system and simultaneously interact directly with the desktop. The novice is prompted to allow or deny the initial connection in view-only mode, and prompted again if the expert attempts to take control of the system. To use RA, both the novice and the expert must be running Windows XP.

RA can be initiated via a user request, known as Solicited Remote Assistance, or by the expert offering assistance to the novice, known as Remote Assistance Offers. The HelpAssistant account is used for RA actions. The account is created as part of the default installation, randomly assigned a complex password, and then disabled. When an RA invitation is opened a "novice" ticket is created on the user's local machine, port 3389 is opened to allow access to terminal services, and the HelpAssistant account is enabled. The expert then connects to the novice's machine using the credentials of the HelpAssistant account. Once all tickets are either closed or expire, the HelpAssistant account is again disabled and port 3389 is closed.

NOTE: Terminal Services is also used for the Remote Desktop Connection capability so port 3389 may remain open if Remote Desktop is enabled on that machine.

Solicited Remote Assistance

A user can send a remote assistance invitation via e-mail, via Windows Messenger, or can save it as a file. Currently there is no way to limit who a novice can request assistance from; the invitation can be sent to virtually anyone who has physical connectivity to the user's network. When a Solicited RA invitation is answered, the novice is presented with the username of the expert. However, the only way to

ensure that the person is who they say they are is through the use of a password. The novice is prompted to provide a password for the session when they generate the invitation although it is not required by the system. The password is not contained within the invitation and must be provided to the expert via another means. However, password complexity, password policy, and account lockout policy rules are not applied to Solicited RA passwords.

Invitations sent through MSN Messenger are sent as clear text XML formatted messages. Invitations sent through e-mail or saved as a file are MsRcIncident files which are also clear text XML formatted messages. It is therefore possible to read these messages to obtain data on who is requesting assistance, the machine's IP address, the port in use by Terminal Services, and if the novice implemented a password.

For these reasons, it is not recommended to use Solicited RA requests on any network where security is of concern.

Remote Assistance Offers

RA Offers are viewed as the more secure way to provide assistance to novice users. RA Offers are only available between two machines in the same domain or trusted domains, and the list of users who are allowed to offer such assistance is configurable. When using this capability, an expert cannot connect to a user's system unannounced or control it without explicit permission from the user. The user is still given the opportunity to accept or deny the connection.

In order to use the Remote Assistance capability, the following changes must be made to the User Rights section of the provided security configuration template.

User Rights	Recommended Settings
Allow logon through Terminal Services Determines which users or groups have the right to log on as a Terminal Services client. This right is needed for Remote Desktop users. If Remote Assistance is being used, only administrators using this new feature should have this right. **Note: It is not necessary to add any users or groups to this setting to allow RA offers.**	<No one>
Deny logon through Terminal Services Determines which users and groups are prohibited from logging on as a Terminal Services client. This right is used for Remote Desktop users.	<No one>

Additionally, to permit the use of Remote Assistance Offers, the following group policy settings must also be set:

- Open a GPO in the Group Policy snap-in via the MMC or access a linked GPO through a container's **Properties → Group Policy** tab.
- If accessing through the **Group Policy** tab, highlight the desired GPO and click the **Edit** button to access the Group Policy snap-in

- Navigate down to the **Computer Configuration\Administrative Templates\System\Remote Assistance** node.
- Double-click on the **Solicited Remote Assistance** setting in the right pane.
- Click the **Enabled** radio button to allow users to request remote assistance.
- Select the "**Allow helpers to only view the computer**" option from the pull down menu.
- Set the **Maximum ticket time (value)** to 0 and the **Maximum ticket time (units)** to minutes.
- Apply the setting and close this dialog box.

NOTE: It is necessary to enable Solicited Remote Assistance in order for Remote Assistance Offers to function. However, setting the maximum ticket time to 0 will prevent users from using the Solicited Remote Assistance capability

- Double-click on the **Offer Remote Assistance** setting in the right pane.
- Click the **Enabled** radio button if you plan to allow experts to offer remote assistance to this machine.
- Select the "**Allow helpers to only view the computer**" option from the pull down menu.

WARNING: It is recommended that you never allow users the ability to give another person remotely control of their computer. Although the user can watch their actions and take back control at any time, it can only take a second to compromise a machine or make it inoperable.

- Click the **Helpers: Show…** button and provide a list of users who can provide assistance to this machine, such as administrators or help desk personnel. It is recommended that this capability be limited to only those users who absolutely require this capability. Users should be listed using the format:

  <Domain Name>\<User Name> or

  <Domain Name>\<Group Name>

Remote Desktop Connections

Remote Desktop (RD) is a limited implementation of Terminal Services that is available on Window XP Professional. It allows a user to connect from a remote system to the client and use the resources of the client as if they were physically at that computer. RD is disabled by default on Windows XP Professional systems.

RD connections are established using the RD client software. This software is installed by default on XP systems and clients for Microsoft Windows 2000, NT, Windows 98 and Windows 95 are included with Windows XP. There is also an ActiveX based client known as the Remote Desktop Web Connection (RDWC) that can be installed on any IIS web server. Using RDWC, any computer that has a browser capable of running ActiveX controls can connect to the web page, download the ActiveX client, and then establish a RD connection even if they do not have the

Terminal Services client installed on their computer. The RDWC is installed by default when IIS is installed on XP Professional systems.

When RD is enabled, port 3389 is opened to allow access to terminal services. All administrators (local and domain) and groups/users listed as members of the "Remote Desktop Users" group can access the machine remotely. When the connection is established, the client computer is locked using the credentials that were used to establish the connection. If a user is currently logged on to the system when another user attempts to connect, the remote user is given the option to disconnect the local user from their session and log them out, but only AFTER the remote user has already successfully authenticated, and only if s/he is an Administrator.

RD uses the standard Windows authentication mechanisms therefore password policy and account lockout policy apply to the RD capability. All accounts used for RD connections must have passwords set.

NOTE: It is possible to lockout the default administrator account through remote desktop connections and prevent it from logging in remotely. However, the account can still be used to log in locally.

In order to use the Remote Desktop capability, the following changes must be made to the User Rights section of the provided security template file.

User Rights	Recommended Settings
Allow logon through Terminal Services Determines which users or groups have the right to log on as a Terminal Services client. This right is needed for Remote Desktop users. If Remote Assistance is being used, only administrators using this new feature should have this right.	Administrators, Remote Desktop Users
Deny logon through Terminal Services Determines which users and groups are prohibited from logging on as a Terminal Services client. This right is used for Remote Desktop users.	<No one>

To enable a computer to accept Remote Desktop Connections, perform the following functions:

- Right click on **My Computer** and select **Properties** to open the System Properties dialog box.
- Select the **Remote** tab from the dialog box.
- Check the **Allow users to connect remotely to this computer** checkbox.
- Click the **Select Remote Users…** button to open the **Remote Desktop Users** dialog box.
- Add users or groups based on your local policy.

NOTE: This process will add the selected users and groups to the local 'Remote Desktop Users' group. Users and groups can also be added directly using local Computer Management.

Group Policy - Administrative Templates

Terminal Services

In addition to the settings outlined above, it is recommended that the following guidance be applied to the Terminal Services either as part of a Group Policy Object (GPO) or through local computer configuration.

These recommendations apply to the Terminal Services extension located under **Computer Configuration\Administrative Templates\Windows Components\Terminal Services** within a GPO and can be accessed via the Group Policy MMC snap-in. Terminal Services settings that also appear under **User Configuration** are overridden by these **Computer Configuration** settings.

Terminal Services Policy Option	Recommended Settings
Limit users to one remote session Limits user to one remote session. By default, Terminal Server allows an unlimited number of simultaneous active or disconnected sessions for each remote user.	Enabled
Limit number of connections This setting limits the number of simultaneous connections allowed to the Terminal Server.	TS Maximum Connections Allowed = 1
Do not allow new client connections When this setting is disabled, the Terminal Server will accept new client connections to the limit set in "Limit number of connections" setting. If this setting is set to enabled, the Remote Desktop feature is effectively disabled, with the exception that users will be able to reconnect to disconnected sessions.	Not configured
Do not allow local administrator to customize permissions Disables the administrator rights to customize security permissions in the Terminal Services Configuration tool. Security settings should be configured at the domain level, not by someone with local administrator rights on the system.	Enabled
Remote control settings To use the remote desktop remote capabilities, this setting must be enabled. It is recommended that only "View Session with user's permission" be selected unless it is absolutely essential that the user exercise full control over another user's session.	Enabled = "View Session with user's permission"
Start a program on connection This setting is used to specify a program that will run automatically when a user logs on to a Terminal Server, overriding Start Program settings by the server administrator or user.	Disabled
Do not allow clipboard redirection Prevents the user from cutting and pasting information using the Windows clipboard between the applications running on the client computer itself and the applications running from within the user's Terminal Services session.	Enabled
Do not allow smart card device redirection Prevents the mapping of smart card devices in a Terminal Services session. If this setting is enabled, users cannot use a smart card device to log on to a Terminal Services session.	Disabled
Allow audio redirection Allows users to play server audio on the local computer, or vice versa, during a Terminal Services session.	Disabled
Do not allow COM port redirection Prevents the user from accessing devices that require a serial (COM) port mapping from within the user's Terminal Services session.	Enabled
Do not allow client printer redirection Prevents users from routing printing jobs from the server to a printer attached to the local computer.	Enabled
Do not allow LPT port redirection Prevents the user from accessing devices that require a parallel (LPT) port mapping from within the user's Terminal Services session.	Enabled
Do not allow drive redirection Disables the mapping of client drives in the Terminal Services session.	Enabled
Do not set default client printer to be default printer in a session When enabled, the default printer that the user has set up on the client computer will not be the default printer from within the Terminal Services session. The default printer is that which is specified at the server.	Enabled

Terminal Services Policy Option	Recommended Settings
Always prompt client for password upon connection Requires users to provide a password to establish a Terminal Services session with the server. Prevents the use of saved credentials to connect to the server.	Enabled
Set client connection encryption level Sets the encryption parameters for all communications between the TS client and server. There are two choices: "Client Compatible" and "High Level". Client compatible encrypts data at the maximum key strength supported by the client. High level encrypts data using a strong 128-bit key.  **NOTE: A user's computer must be running the 128-bit TS client software in order to establish a session with a server that is using the high level. Clients that do not support this level of encryption cannot connect.**	Enabled = "High level"
Do not use temp folders per session Allows the creation of temporary folders for each session the server is supporting. Creating separate folders reduces the risk of data being accessed inappropriately.	Disabled
Do not delete temp folder upon exit The server will delete the temporary folder created to support a user's session when the session is closed. Deleting the folders reduces the risk of data being accessed inappropriately.  **Note: The folders are not deleted when a session is disconnected, but only when the session is closed by logging off from that session.**	Disabled
Set time limit for disconnected sessions Limits how long a disconnected session can exist before it is closed. When a session is in a disconnected state, the programs/processes that the user had running on the server will continue to run even though the communications with the client have been lost.	Enabled = "10 minutes"
Set time limit for active sessions Limits how long a user can maintain an active session with the server. If set to "never", no limit is set on how long an active session can exist.	Enabled = "Never"
Set time limit for idle sessions Limits how long an idle session is kept open and not disconnected. An idle session may indicate that the user has stepped away from their computer, presenting someone else with the opportunity to use their session if their computer is not locked.	Enabled = "15 minutes"
Allow reconnection from original client only This setting only applies to Citrix ICA clients and is ignored for Windows clients.	Not applicable
Terminate session when time limits are reached This setting determines if timed-out sessions are disconnected or closed by the server. When enabled, all sessions are closed when time-out limits are reached.	Enabled

Table 16 Terminal Services Policy Options

Network Configuration Recommendations

Remote Assistance and Remote Desktop both use terminal services to provide the remote user access to the local system. Terminal services opens port 3389 on the Windows XP system when these capabilities are utilized. It is highly recommended that remote connections be limited to systems within the local intranet and that port 3389 be blocked at the perimeter firewall or filtering router. Both inbound and outbound connections on this port must be blocked to prevent external access. If only inbound connections are blocked, it is still possible for remote assistance connections to be established through an external messenger server using Windows Messenger. These connections are established by both users initiating outbound connections to the messenger server therefore connections in both directions must be blocked.

If RA or RD connections from outside the local LAN are required, it is suggested that filtering be implemented on the firewall or router to permit only the specific external IP addresses access to the internal systems. All other addresses should be denied access on port 3389. For a higher level of protection, set up a VPN and require extremely strong multi-factor authentication for the very few users who are permitted to dial into to this VPN. It is generally also a good idea to only allow specific IPs to connect to this VPN server.

Chapter

14

Internet Connection Firewall Configuration

The Internet Connection Firewall (ICF) provides a basic level of protection to a computer from external connections. It uses stateful packet inspection to deny external packets from reaching the client unless they are in response to a client-initiated request. All other packets are dropped in the default configuration setting.

This chapter gives a brief overview of security settings available with the ICF.

Recommended Usage

Internet Connection Firewall is not intended or flexible enough to use in a network setting. The ICF would not normally be run where the client is part of a protected network, or where the client computer is providing a service. Some examples of services include: file and print sharing, web servers, and ftp servers. In these cases, a dedicated firewall should be used to provide the customized level of protection needed.

There are some situations where the use of the ICF does provide additional amounts of protection for the client computer. These occur when the computer is directly connected to Internet or external networks. Laptops that are connected to a DSL or cable modem, or connected to a different network while traveling, would benefit from the ICF.

Features

ICF protects the client computer in three different ways: stateful packet inspection, protection from port scans, and security logging. This section briefly describes each of these features.

Stateful packet inspection

The ICF uses stateful packet inspection, which keeps a table of all connections initiated by the client computer and compares all incoming packets. If the incoming packet is in response to a client-initiated request, it is allowed. Unless a filter has been implemented to allow unsolicited traffic, all other traffic is blocked.

Protection from port scans

When the default configuration is used, the computer will be invisible to most port scanners. If the configuration is changed to allow external connections, only those ports that have been opened via the advanced settings tables will be detected by a port scan.

Many port scanners will perform an ICMP ping to see if a host exists before executing a port scan. By default, pings will also be dropped, and the ICF-protected computer may be skipped even if some ports are in actuality open.

Security Logging

The ICF can be configured to log connection attempts. You can choose to log successful connections, dropped packets, or both. There are no other options for what information is written to the log file.

What it doesn't provide

The ICF only provides packet filtering in the incoming direction. You cannot use it to restrict the types of data transmitted from the local machine. This also means that the ICF cannot restrict destinations to which the local machine can connect.

The ICF settings that allow for external connections to the local computer do not provide any restrictions on who may access those services. It will not allow you to grant access to, or deny access from specific computers, users, or networks. If a service is enabled, it grants access from all. If it is not enabled, it is denied to all. However, you can use IP Filtering to obtain more granular control over both inbound and outbound connections.

Enabling the ICF

The following conditions must be met before you can enable the ICF:

- You must have Administrator privileges.
- The ICF must not be denied in the group policy.

WARNING: Enabling Internet Connection Firewall with default settings can disable the ability to share files and printers. ICF also can disable the ability to browse My Network Places along with other "network" functions. See Microsoft Q298804 at http://support.microsoft.com/support/kb/articles/Q298/8/04.asp for more information.

The ICF must be enabled and configured on each interface on which it is to run. If you used the **Set up a home or small office network** wizard either from the **Network Tasks** panel or from the **Create a new connection wizard**, the firewall may have been enabled by default. This wizard will enable the ICF under the two options in the wizard:

- **This computer connects directly or through a network hub. Other computers on my network also connect to the Internet directly or through a hub.**
- **This computer connects directly to the internet. I do not have a network yet.**

If the network interface was set up any other way, or if the ICF is not enabled, it can be enabled by performing the following actions:

- **Control Panel → Network**
- Right-click on the connection interface and select **Properties** from the pull-down menu
- Click the **Advanced** tab

- Click on **Protect my computer and network by limiting or preventing access to this computer from the Internet.** See Figure 14**.** This will enable the ICF using the default configuration.

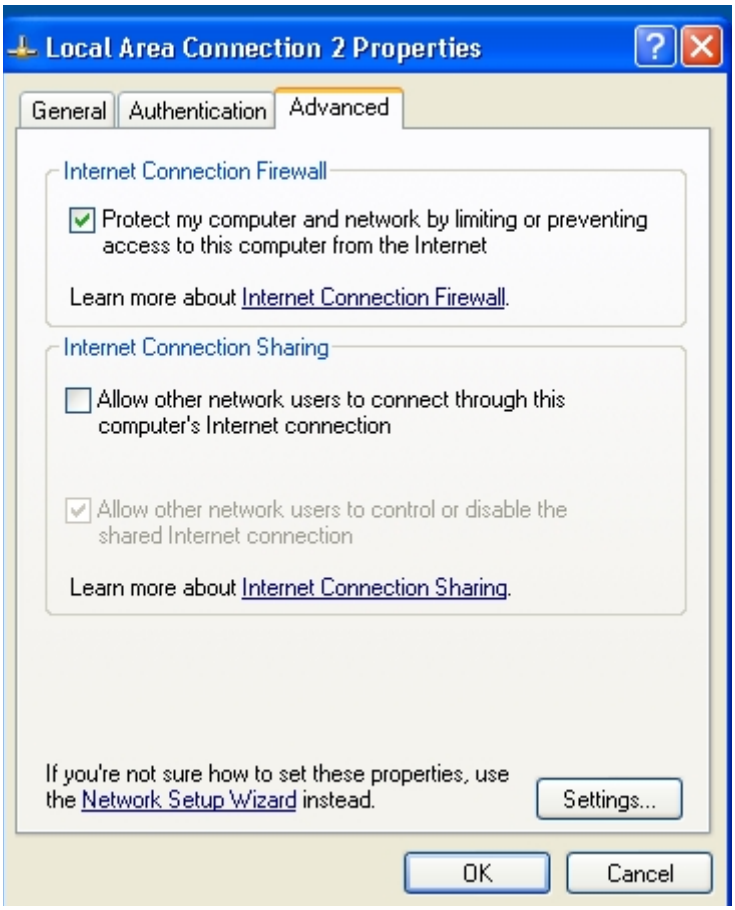


Figure 14 Enabling ICF

- If you wish to customize the firewall settings, click **Settings**. This will bring up an interface with three tabs: **Services**, **Security Logging**, and **ICMP**.

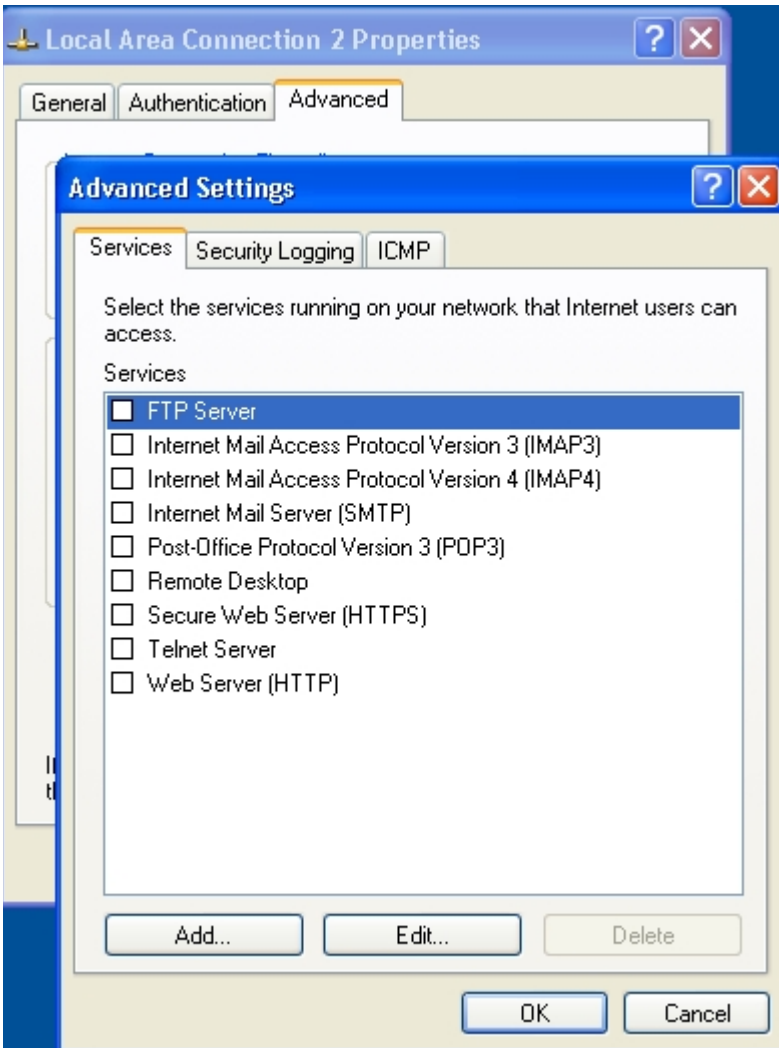


Figure 15 Services tab

The **Services** tab in **Figure 15** shows the default options available for common services. Select any of the services and a window will pop up allowing you to indicate the name or address of the computer on which that service is running. Unless you are using the computer as a gateway to other computers, that entry should reflect the name of the computer on which the ICF is running.

You can add additional services by clicking the **Add** tab and filling in the information for that service. For example, to add a web server on port 8080, the entry may look like **Figure 16**.

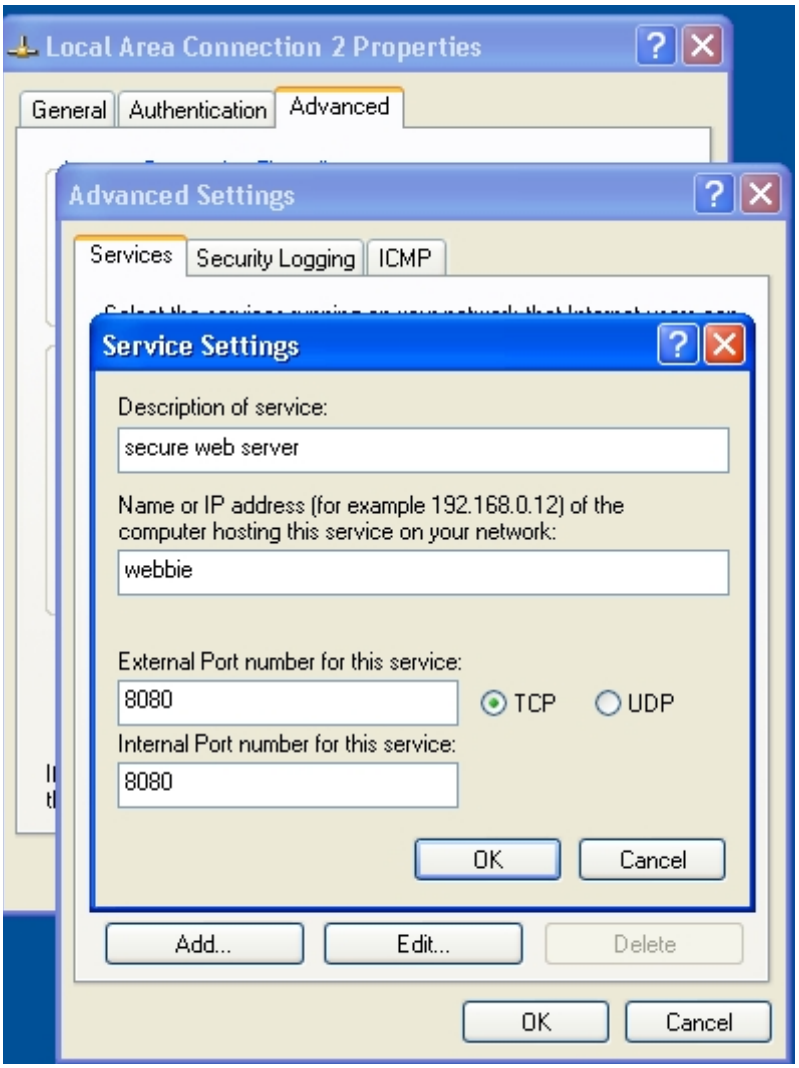


Figure 16 Example service setting

NOTE: If you are using DHCP to get the network address, you should use the machine name rather than the IP address on these forms since there is no guarantee that the IP address will always be the same.

The **Security Logging** tab will allow you to set up a log of ICF activity. You can choose to log dropped packets, successful connections, or both. You also have the choice of the location and maximum size of the log file. If the log file exceeds the maximum size, the oldest entries are dropped from the file. There is no way to automatically archive the log file. **Figure 17** shows the security logging options.

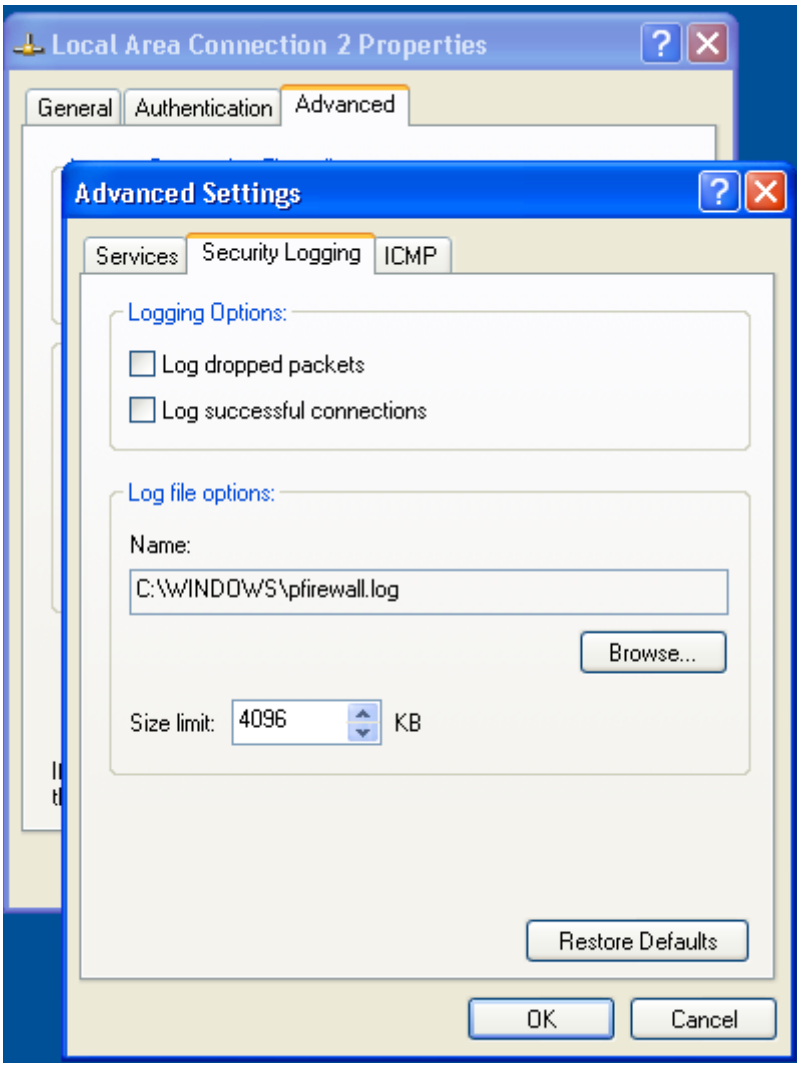


Figure 17 Security Logging tab

The **ICMP** tab will allow you to select various types of ICMP messages to allow. Unlike the TCP/UDP services, the ICMP section is broken into inbound and outbound packets. ICMP packets can be used to gather information about your network. It is recommended not to enable any of these messages unless absolutely necessary. **Figure 18** shows the ICMP options.

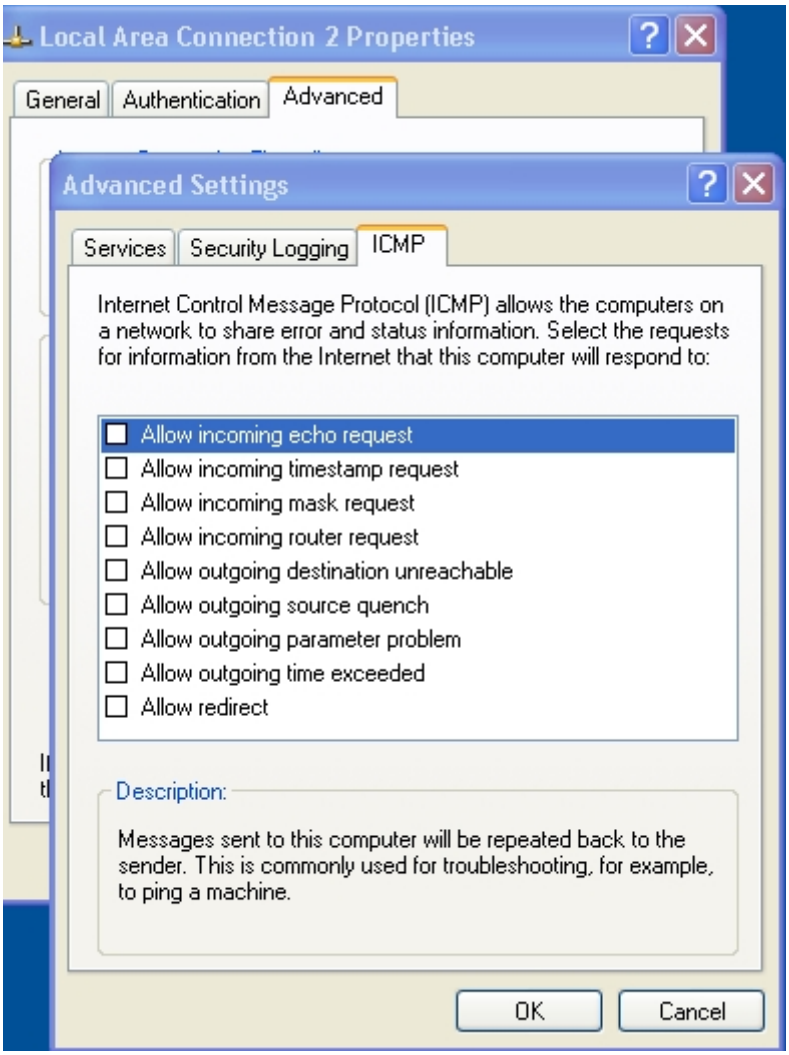


Figure 18 ICMP tab

Summary

The Internet Connection Firewall provides a basic level of protection to a computer. This protection is limited to new inbound connections, as there is no restriction on any connections initiated from the local machine or replies to a locally initiated connection. The default configuration will block all external connections to local services and will provide some protection against port scanning. Individual services can be allowed through the ICF by opening the associated port, but there is no selectivity. Traffic is either allowed or denied; you cannot filter based on content or address. If the computer is supporting these services, it should be located behind a more robust firewall than the ICF can provide.

The ICF is useful in limited situations, such as when a computer is not part of a network and is connected directly to the Internet, such as when traveling dialing into the organizational Remote Access Server. Note that in environments that use IPSec, ICF must be disabled. Otherwise, the client will be unable to negotiate the IPSec policy and will not be able to make any network connections.

This Page Intentionally Left Blank

Chapter

15

Additional Security Settings

Aside from the security options set via security templates, several other security-related settings should be configured. This chapter addresses these settings.

Administrator Accounts Recommendations

Due to their power, administrator accounts must be especially safeguarded in a Windows environment. This section discusses several additional recommendations related to accounts with administrative privileges.

Additional Administrator Accounts

During Windows XP installation, if the user has chosen to install XP as a stand-alone machine as opposed to a domain member, the user is asked "Who will use this computer?" and prompted to enter at least one user account. He will not be able to proceed with the installation until at least one account is entered. Any accounts entered here will automatically be assigned blank passwords and become members of the Administrators group. Thus, even if only one user is entered, there will be two administrators on the machine: the built in Administrator account and the user entered. Windows XP in a stand-alone mode requires this extra administrator account because it is not recommended to log on locally with the built-in administrator. However, in a domain environment, the extra administrator account poses a potential security risk. In Windows XP, local users with blank passwords cannot logon via a network connection, but they can log on locally. Therefore, in a domain environment, it is recommended to remove the extra user account created during installation and ensure that a good, complex password is set on the built-in Administrator account. If the extra administrator account is needed, ensure that the account has a strong password

To remove a user account:

- Select **Control Panel → User Accounts**
- Click on the account(s) to delete
- Click **Delete the account**

User accounts may alternately be removed by performing the following steps:

- Select **Start → All Programs → Administrative Tools→ Computer Management**
- Expand the **Local Users and Groups** node
- Double-click **Users**
- In the right-hand pane, right-click on the user to delete
- Select **Delete** from the pull-down menu

Use of Administrator Accounts and the RunAs Command

Administrators should have two accounts: one with administrative privileges and one normal user account. System administrators should use their administrator account credentials only when necessary and use their regular user account for most daily tasks. Administrators should never browse the Internet with their administrator accounts since malicious web code will run under the context of the logged-on user.

When performing tasks that require administrator privileges, the `runas` command can be used. This command will allow an unprivileged user to run a program as another user. Typing `runas /?` at the command prompt will provide a list of options for the command. Use the following syntax:

`runas /user:`*domain_name*`\`*administrator_account program_name*

The `runas` command can also be launched via a menu item shortcut by performing the following steps:

- From the **Start** menu, navigate to the desired application
- While holding down the SHIFT key, right-click on the application
- Select **Run As** from the pull-down menu
- Click the option **The following user**
- Type or select **User name**
- Type the **Password**
- Click **OK**

NOTE: The RunAs feature requires that the Secondary Logon service on Windows XP or the RunAs service on Windows 2000 be running. These services are started by default.

See the Microsoft Knowledge Base article Q294676 at http://support.microsoft.com/support/kb/articles/Q294/6/76.asp for more information on use of the `runas` command.

Shared Resource Permissions

Windows shares are a means by which files, folders, printers, and other resources can be published for network users to remotely access. Regular users cannot create shares on their local machines; only Administrators and Power Users have this ability and must have at least Read permission on the folder to do so. Any users that are granted the **Create Permanent Shared Objects** user right also can create shares. Since shares may contain important data and are a window into the local system, care must be taken to ensure proper security settings on shared resources.

The following share permissions can be granted or denied to users or groups:

- Full Control
- Change

- Read

Share permissions are granted independent of NTFS permissions. However, share permissions act aggregately with NTFS permissions. When accessing a remote share, the more restrictive permissions of the two apply. For example, if a user accesses a share remotely and has Full Control over a shared folder, but only NTFS Read access to that folder on the local file system, he will only have Read access to the share.

The default permissions on a share give the Everyone group Full Control; therefore, you must explicitly edit security permissions on shared resources to limit share access.. This means that your NTFS permissions will be solely used to determine what access remote users have to the share. If for some reason users accessing the share remotely should have less permission than the same users accessing the directory locally you can use share permissions to further restrict their access. Keep in mind, however, that restricting access to users on shares has no effect if they are logged on locally or via terminal services. For that reason, it is recommended to set good NTFS permissions.

NOTE: When Simple File Sharing is disabled (as is the case when a Windows XP machine is joined to a domain), Windows XP does not allow sharing of the Documents and Settings, Program Files, and %SystemRoot% folders as well as any folders below %SystemRoot%.

Setting Share Permissions

To create a share and set security permissions:

- In explorer, right mouse-click on the folder that is to be shared.
- Select the **Sharing and Security…** menu option
- Click the **Share this folder** radio button.
- Specify the **Share Name**.
- Click the **Permissions** button.
- Add, remove, or edit the users and/or groups in the access control list for the share.

NOTE: If you have Simple File Sharing turned on, this dialog will be entirely different. With simple file sharing, all network users authenticate as the Guest user, regardless of the credentials they enter.

Share Security Recommendations

When creating shares and share permissions, adhere to the following criteria when possible:

- Ensure that the Everyone group is not given permissions on any shares.
- Use the Authenticated Users or Users groups in place of the Everyone group.
- Give users and/or groups the minimum amount of permissions needed on a share.
- To protect highly sensitive shares not for general use, hide shares by placing a $ after the share name when creating a share. Users can still connect to hidden shares, but must explicitly enter the full path to the share (i.e. the share will not be visible in Network Neighborhood).

Deleting POSIX Registry Keys

As stated earlier in this guide, the POSIX subsystem is no longer included in Windows XP. However, two POSIX registry key values still exist. In fact, one key, HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems\Posix is set to %SystemRoot%\system32\psxss.exe, a file that doesn't even exist in Windows XP. Therefore, it is recommended that the registry key values be removed by performing the following steps:

- In the registry editor, `regedit`, navigate to the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Subsystems** registry key
- In the right-hand pane, select the **Optional** value.
- From the **Edit** menu, select **Delete**
- In the dialog box asking **"Are you sure you want to delete this value?"** click the **Yes** button
- Repeat this process for the **Posix** registry key value, also under the **Subsystems** registry key

Additional Group Policy Settings

This section recommends several security settings that can be applied via Group Policy. Group Policy can be applied to locally to a Windows XP machine regardless of whether or not it is a member of an Active Directory domain. Of course, Group Policy can also be applied to Windows XP workstations from a Windows 2000 domain controller. To access a GPO:

- Open a GPO in the Group Policy snap-in via the MMC or access a linked GPO through a container's **Properties → Group Policy** tab.
- If accessing through the **Group Policy** tab, highlight the desired GPO and click the **Edit** button to access the Group Policy snap-in

Disabling Remote Assistance/Desktop

Like all remote-control technology, Remote Assistance and Remote Desktop have security implications associated with their use. It is recommended that remote-control technology not be used on operational networks where the highest level of security is desired.

To disable the use of Remote Assistance, the following group policy settings must be set:

- Navigate down to the **Computer Configuration\Administrative Templates\System\Remote Assistance** node.
- Double-click on the **Solicited Remote Assistance** setting in the right pane.
- Click the **Disabled** radio button to disallow users to request remote assistance.
- Apply the setting and close this dialog box.
- Double-click on the **Offer Remote Assistance** setting in the right pane

- Click the **Disabled** radio button to disallow experts to offer remote assistance to this machine.
- Apply the setting and close this dialog box.

NOTE: The settings in group policy override any settings on the System Properties/Remote tab and will prevent users from using these capabilities even though the items may be selected under System Properties.

To disable a computer from accepting Remote Desktop Connections, perform the following functions:

- Right click on **My Computer** and select **Properties** to open the System Properties dialog box.
- Select the **Remote** tab from the dialog box.
- Ensure the **Allow users to connect remotely to this computer** checkbox is unchecked.
- Click the **Select Remote Users…** button to open the **Remote Desktop Users** dialog box.
- Remove all users and groups from the Remote Desktop Users group.

Network Initialization

By default, Windows XP does not wait for the network to be fully initialized prior to user logon. Instead, cached credentials are used to log on existing users, resulting in shorter logon times. Group Policy is then applied in the background.

This behavior results in certain policy extensions, such as Software Installation and Folder Redirection, taking up to two logons to be successfully applied. These extensions require that no users be logged on and must be processed in the foreground before users are using the computer. Also, user policy changes such as adding a profile path or logon script may also take up to two logons to be detected.

A problem occurs with respect to password expiration notices not being displayed to users logging onto Windows XP clients in a Windows 2000 or Windows NT 4.0 domain. If the user is logged on with cached credentials before Group Policy is applied, the policy indicating when a password expiration warning should be displayed won't be processed until after the user logs on. Therefore, the user's password will eventually expire with the user having had received no warning.

This guide recommends not allowing user credentials to be cached (the **Interactive logon: Number of previous logons to cache** security option set equal to 0). Therefore, cached user credentials should never be used during logon to a domain, forcing the network to fully initialize. However, if the cached logons count is set to anything other than 0, problems could ensue. See Microsoft Knowledge Base article Q313194 at http://support.microsoft.com/support/kb/articles/Q313/19/4.asp for more information on the password expiration issue on Windows XP.

In general, it is good practice to ensure that all computer-related group policy changes are applied prior to users logging on so that the user can operate under the correct security context. Therefore, the following group policy setting is recommended:

- Navigate down to the **Computer Configuration\Administrative Templates\System\Logon** option
- In the right pane, double-click **Always wait for the network at computer startup and logon**
- Click the **Enabled** radio button
- Click **OK**

Disabling Media Autoplay

Autoplay reads from a drive as soon as it is inserted. By default, Windows XP 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. To disable autoplay on all devices, perform the following steps:

- Navigate down to the **Computer Configuration\Administrative Templates\System** option
- In the right pane, double-click **Turn off Autoplay**
- Click the **Enabled** radio button
- In the **Turn off autoplay on:** pull-down menu, choose **All drives**
- Click **OK**

Blocking NetBIOS and SMB Ports at the Network Perimeter

Within a Windows environment, NetBIOS defines a software interface and a naming convention. NetBIOS over TCP/IP (NetBT) provides the NetBIOS programming interface over the TCP/IP protocol. Windows 2000 and Windows XP use NetBT to communicate with Windows NT and older versions of Windows (e.g. Windows 9x). However, when communicating with other Windows 2000 or Windows XP systems, Windows XP uses direct hosting. Direct hosting makes use of DNS, vice NetBIOS, for name resolution, and uses TCP port 445 instead of TCP port 139. The Server Message Block service used for network resource sharing is now run directly over TCP/IP without using NetBIOS as a “middle man.”

Communications via the Windows NetBIOS and SMB ports (ports 135-139 and 445) can provide much information about the Windows systems and allow a gateway for attacks. Therefore, it is important to disallow systems outside the network perimeter from connecting to internal systems via these ports.

It is recommended that outbound and inbound traffic to ports 135, 137, 138, 139, and 445 be blocked at the network perimeter router and/or firewall. A number of attacks as well as further compromise is made significantly harder if outbound SMB traffic is blocked.

Chapter

16

Modifications for Windows XP in a Windows NT Domain

Windows XP Professional may be used as a client in a Windows NT 4.0 domain. However, several modifications from the recommendations in this guide must be made for Windows XP to successfully function in such an environment. This chapter describes known issues when adding a Windows XP client to a domain containing Windows NT 4.0 domain controllers.

Lack of GroupPolicy

Windows NT 4.0 does not support Active Directory, and, hence, does not support the application of Group Policy. However, security settings can be locally set on a Windows XP machine either through the Security Configuration and Analysis tool described earlier in this document and/or via Local Group Policy.

NTLM and LanManager Settings

In Chapter 5, the security option Network security: LAN Manager authentication level is recommended to be: Send NTLMv2 response only\refuse LM and NTLM. However, when authenticating to an NT Domain for the first time from an XP Client, this option should be set to Send LM & NTLM – use NTLMv2 Session Security if Negotiated. This must be done for each new XP client.

- **Start → Run → gpedit.msc**
- In the left pane, navigate to **Computer Configuration\Windows Settings\Security Settings\Local Policy\Security Options**
- In the right pane, double-click **Network Security: LAN Manager Authentication Level**
- Select **Send LM & NTLM – use NTLMv2 Session Security if Negotiated**
- Click **OK**
- Close the Group Policy window

Once initial authentication has been completed it is recommended that this setting be returned to Send NTLMv2 response only\refuse LM and NTLM.

Strong Session Key

In Chapter 5, the security option **Domain member: Require strong (Windows 2000 or later) session key** is recommended to be enabled. However, in a Windows NT domain, this option must be set to **Disabled**.

- **Start → Run → gpedit.msc**
- In the left pane, navigate to **Computer Configuration\Windows Settings\Security Settings\Local Policy\Security Options**
- In the right pane, double-click **Domain Member: Require strong (Windows 2000 or later) session key**
- Select **Disabled**
- Click **OK**
- Close the Group Policy window

Autoenrollment

By default, Windows XP attempts automatic public key certificate enrollment. This autoenrollment feature requires Active Directory. In a Windows NT 4.0 domain, there is no Active Directory, so autoenrollment does not work and will record a failure periodically in the event log.

To disable Autoenrollment, edit the Windows XP system's Local Group Policy.

- **Start → Run → gpedit.msc**
- In the left pane, navigate to **Computer Configuration\Windows Settings\Security Settings\Public Key Policies**
- In the right pane, double-click **Autoenrollment Settings**
- Click **Do not enroll certificates automatically**
- Click **OK**
- Close the Group Policy window

See Microsoft Knowledge Base Article Q310461 at http://support.microsoft.com/support/kb/articles/Q310/46/1.asp for more information on this issue.

Appendix

A

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 XP 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.

Appendix

B

References

Bartock, Paul, et. al., *Guide to Securing Microsoft Windows NT Networks version 4.1*, National Security Agency, September 2000.

DiMaria, Vincent, et.al., *Guide to Securing Microsoft Windows 2000 Terminal Services*, National Security Agency, July 2, 2001.

Haney, Julie, *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset*, National Security Agency, January 2002.

MacDonald, Dave, Warren Barkley, "Microsoft Windows 2000 TCP/IP Implementation Details," white paper, http://secinf.net/info/nt/2000ip/tcpipimp.html.

McGovern, Owen, Julie Haney, *Guide to Securing Microsoft Windows 2000 File and Disk Resources*, DISA and National Security Agency, May 2002.

Microsoft Technet, http://www.microsoft.com/technet.

Microsoft Windows XP Professional Resource Kit Documentation, Microsoft Press, 2001.

"No Password Expiration Notice Is Presented During the Logon Process," KB Article Q313194, http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313194, Microsoft, March 2002.

"Problems When the Autoenrollment Feature Cannot Reach an Active Directory Domain Controller," KB Article Q310461, http://support.microsoft.com/default.aspx?scid=kb;en-us;Q310461,

Microsoft, March 2002.

Schultze, Eric, “Windows XP Security: Everything you’ve always wanted to know…and a little bit more,” as presented at InfoSec World 2002 conference.

“Upgrading Windows 2000 Group Policy for Windows XP,” Microsoft KB article http://support.microsoft.com/default.aspx?scid=kb;en=us;Q307900, Microsoft, November 2001.