Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Taking the Confusion Out of Security Templates

This paper will address how security templates are constructed using the Security Templates Snap-in to the Microsoft Management Console (MMC). The primary focus of the examples will deal with Windows 2000 Professional. A security template is a versatile tool to assist in creating a baseline security configuration for a system. The settings used in a template need to be thoroughly researched and tested to comply with company security policies. The Security Template that is created can then be applied using the Security ...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Title: Taking the Confusion Out of Security Templates
Name: Robert Aitken
Date: February 27, 2003
Practical: GSEC Version 1.4b option1

Abstract

This paper will address how security templates are constructed using the Security Templates Snap-in to the Microsoft Management Console (MMC). The primary focus of the examples will deal with Windows 2000 Professional. A security template is a versatile tool to assist in creating a baseline security configuration for a system. The settings used in a template need to be thoroughly researched and tested to comply with company security policies. The Security Template that is created can then be applied using the Security Configuration and Analysis Snap-in within the MMC, or by using the Secedit.exe command-line tool.

Why create a security template

There are many opinions on what is the best security solution. I would not dream of telling you what the best solution is for your environment. The consensus among most security professionals has always been Defense in Depth, which means that security for a system or network should contain many different countermeasures working together to prevent compromise to the three major areas of protection (confidentiality, integrity, and availability). Confidentiality means we don't want unauthorized people to view our data. Integrity means we want to make sure our data is correct and has not been altered. Availability means that those people who are authorized to access our resources are able to do so. Now the Security Template gives us the opportunity to incorporate many security features into a single file that can be applied in different ways. Some of these security features include configuring auditing and permissions on the file system and registry, password policy, access and use of system services, values in the registry used by the operating system to manage security.

The security template you create can make applying many security features to your system much simpler than trying to set them individually. You can create one template to use on many different systems. There may also be the need to create many different templates to be used in conjunction with each other. We are all aware that there is not just one solution that will work for all possible environments. I want to make sure you challenge convention and not blindly accept what might be considered a best practice. It is generally considered a best practice to have at least eight characters in a password for authentication. These eight characters are to be made up of both upper and lower case alphabetic characters and also include numbers and special characters. There are also rules about how these characters are to be put together. The characters should not be repeated more than twice. They should not form dictionary words,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

or be related to the user name. These are good principles everyone should understand, but then they should be improved and customized for your specific environment. Nobody would ever say you should just have the minimum level of security. Everyone should be working on a level of security that at least meets the level suggested by the best practices, but do not forget you still need to meet your operational requirements. Please do not forget to TEST each and every setting thoroughly on a test machine before applying it to a production system. You will need to keep in mind that as you start to collect a larger number of security settings that these will need to be tested to see that the settings do not conflict with each other. Vulnerability checking tools should be run to make sure your specific configuration is not ignoring known vulnerabilities. If you fail to educate all those responsible for the system, which includes administrators and users you will be opening yourself up to potential problems.

The unsigned driver setting located in the security options section of the template is a great example of the need to educate users. If you have this setting set in the registry. A regular user may not realize the severity of the Graphical User Interface (GUI) window that just popped up informing the user an unsigned driver was just installed. Most users see pop-up windows all the time, especially while interacting with web pages and advertisements on the Internet. These users are accustomed to closing most pop-up windows sometimes without even reading them. It might be a good idea if you let everyone know what this specific GUI means. Having an established security policy on what they are supposed to do, if they do see it. Screaming across a room filled with people who are busy doing important work might be a little distracting. It might make the person responsible for the compromise aware of the fact that you know something is wrong with the system. Instructions to write down the time and events that caused the GUI window to appear can help with an investigation later. You might also want to make sure that they stay logged on, but lock the screen before leaving the station to inform an administrator. If the GUI window or other windows are closed, it could really hamper your ability to determine what caused the window to appear in the first place. Keep in mind that Microsoft has not signed every driver they distribute to the public so be aware that false positives happen. You need to know what to look for to determine what action to take next. It might be a little hazardous to your career prospects to shut down production systems and call in the FBI to find out you have a freshly installed unsigned printer driver.

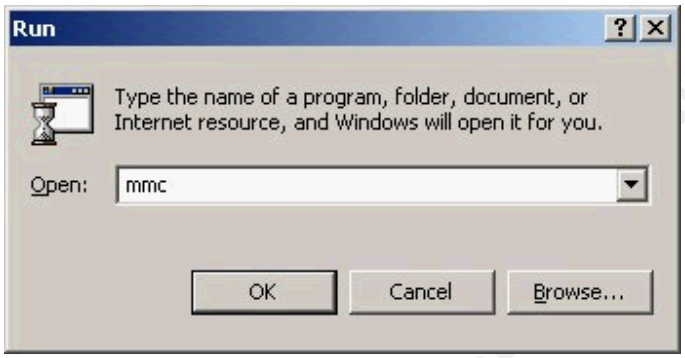
These are all good reasons to have well written and intuitive security policies that management supports and users understand. It is important to have all users of your systems agree in writing to read and follow your company's security policies. Please keep all this information in mind while analyzing the security template settings for your specific environment. It will assist you in making your Security Template consistent with security policies and understandable from a user's point of view.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Creating a Security Template

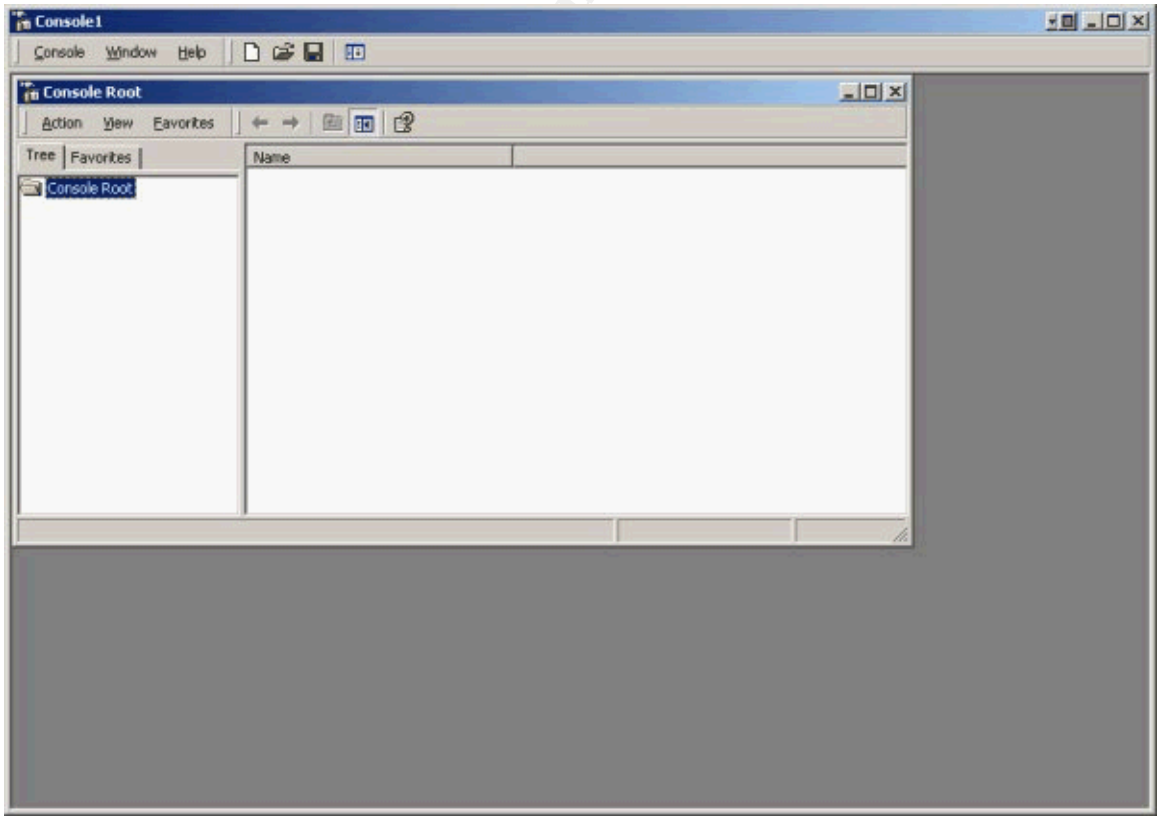
Launch Microsoft Management Console (MMC)

1. Click the 'Start' button select 'Run…' and type 'mmc' in the 'Open:' text box



2. Click the 'OK' button

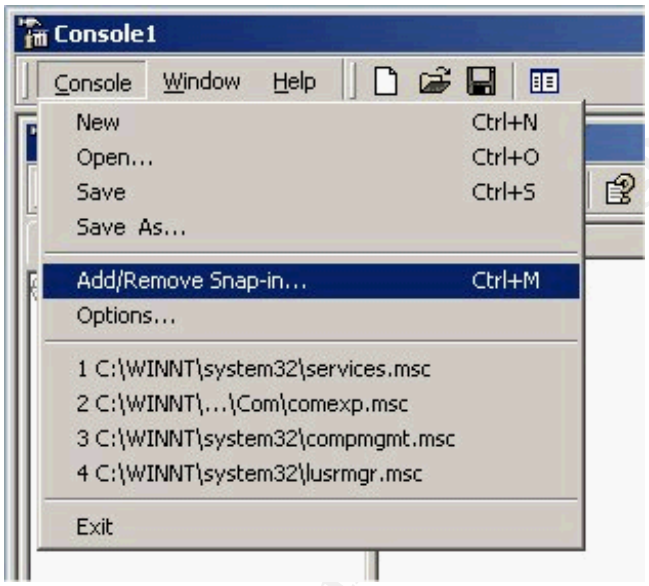
3. A GUI should be display titled 'Console1' which contains a smaller window titled 'Console Root'



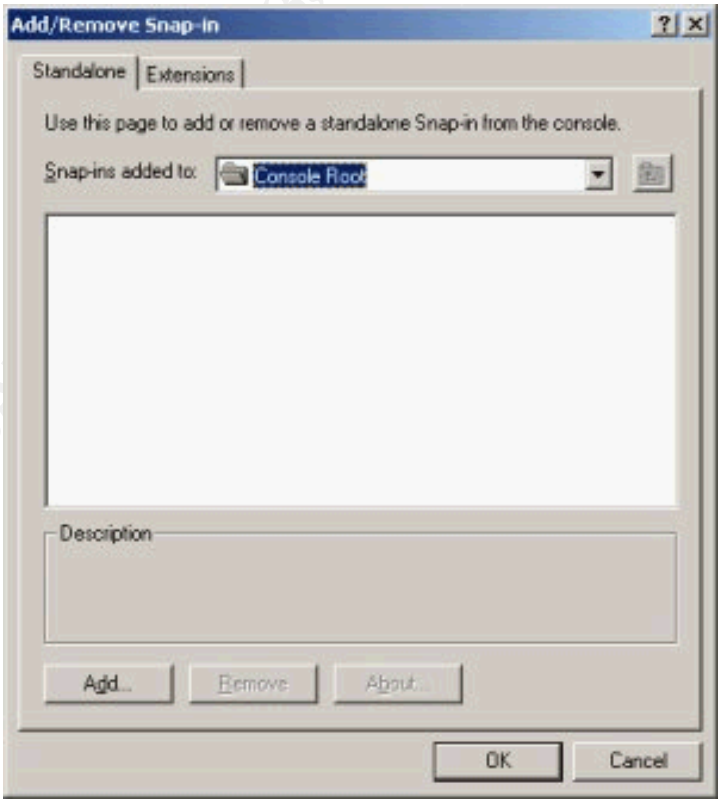
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Loading the Security Templates Snap-in to the MMC

1. Click on the 'Console' menu option
2. Select 'Add/Remove Snap-in…' from the drop-down menu options or use the shortcut key sequence 'Ctrl+M'

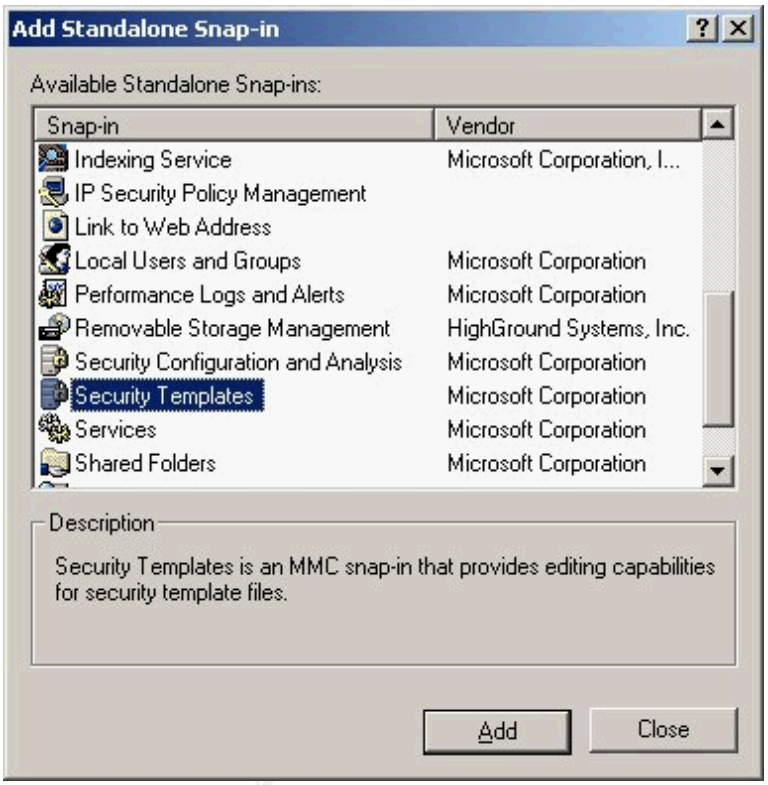


3. Another GUI window titled 'Add/Remove Snap-in' will appear



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4. Click the 'Add…' button
5. Another GUI window titled 'Add Standalone Snap-in' will be displayed
6. From the 'Available Standalone Snap-ins:' scroll box select 'Security Templates'



7. Click the 'Add' button, then click the 'Close' button
8. The 'Security Templates' Snap-in should now appear in the first GUI titled 'Add/Remove Snap-in'
9. From the GUI titled 'Add/Remove Snap-in' click the 'OK' button

<u>Creating a new security template</u>

The 'Security Templates' Snap-in should now appear in the window titled 'Console Root' with a '+' sign in front of it

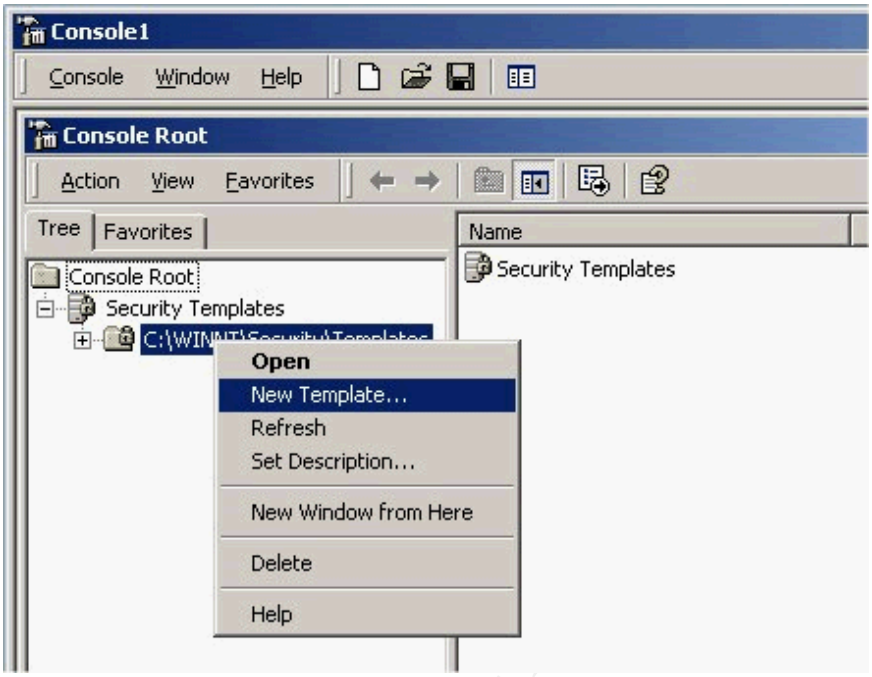
Click the '+' sign or double-click the 'Security Templates' Snap-in

A small folder icon with a lock labeled 'C:\WINNT\Security\Templates' with a '+' sign in front of it should appear under the 'Security Templates' Snap-in

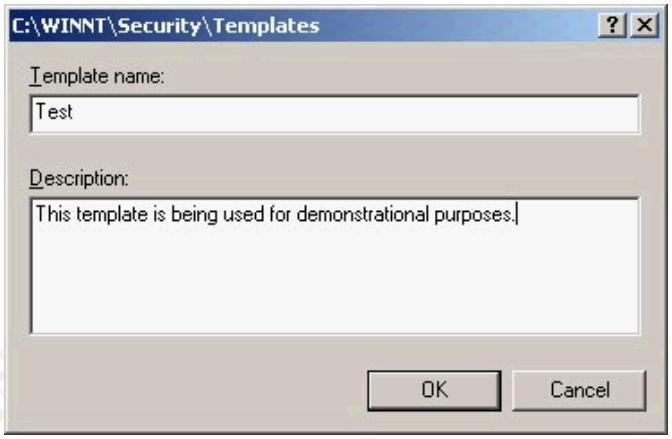
Right-click either on the folder icon or the label 'C:\WINNT\Security\Templates'

From the menu select 'New Template…'

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



In the text box labeled 'Template name:' enter a name for your template (i.e. Test). Filling in the 'Description:' text box with information about this particular Security Template is a nice way to give additional information to users.



Click the 'OK' button

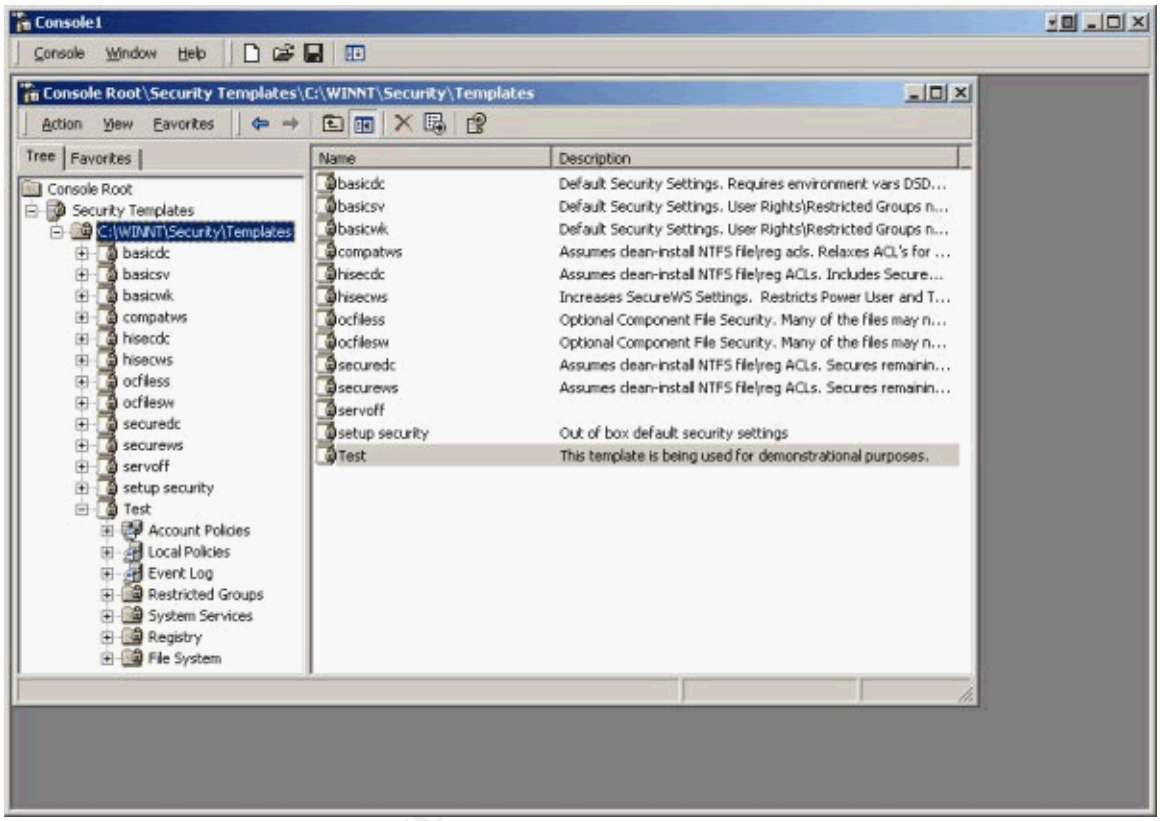
Click on the '+' sign in front of the folder icon labeled 'C:\WINNT\Security\Templates'

There should be a list of notepad like icons with locks on them and '+' signs in front of them. These are the default templates that are installed with Windows 2000 plus the one just created. The default templates are already configured with the appropriate settings for a specific level of security and the type of operating system (workstation, server, or domain controller). Using the default

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

templates or customizing one is a valid alternative to creating a new template. This decision should be made after considering the needs of your specific environment.

Click on the '+' sign in front of the one we just created (i.e. Test).



Configuring the sections within a security template

There should be a list of the different sections that make up a Security Template:

- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System

Account Policies section

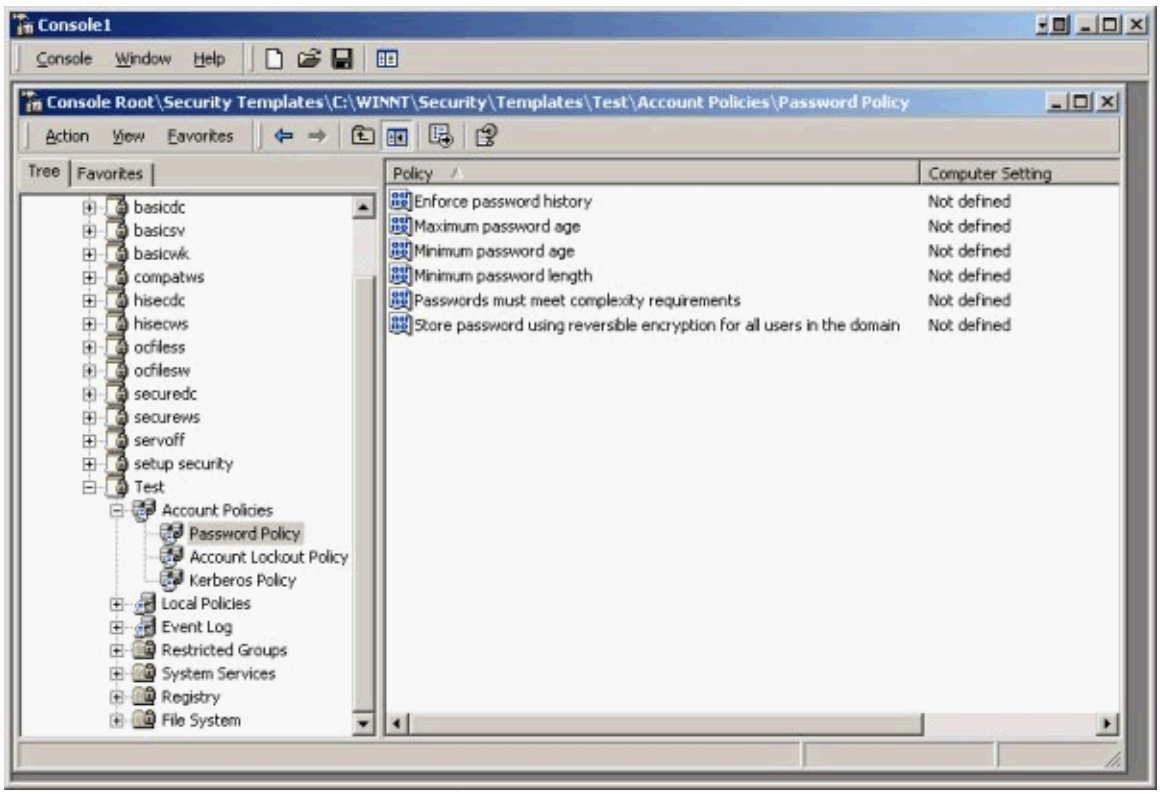
The first section is Account Policies. Click on the '+' sign in front of 'Account Policies' to reveal 3 subsections:

- Password Policy

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Account Lockout Policy
- Kerberos Policy

Clicking on the 'Password Policy' reveals in the right windowpane a list of policies and what the 'Computer Setting' is for each 'Policy'



The Password Policies are:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Passwords must meet complexity requirements
- Store password using reversible encryption for all users in the domain

The 'Computer Setting' for each of these policies is currently set to 'Not defined'.

To set a 'Policy' double-click on the policy you wish to set in the right windowpane. A gray box labeled 'Template Security Policy Setting' should appear with the 'Policy' selected displayed. We will use 'Enforce password history' as an example.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Place a checkmark in the box by 'Define this policy setting in the template' by clicking in the box.

The grayed out 'passwords remembered' feature should now be accessible. The value is set by using the up and down arrow buttons, or the value can be edited manually.

To determine what value to use is not an easy task. The first thing you need to do is understand what 'Enforce password history' means. The following Microsoft Corporation reference URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/500.asp has the explanation for this setting:

> Enforce password history
>
> Description:
> Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This policy enables administrators to enhance security by ensuring that old passwords are not reused continually.
To maintain the effectiveness of the password history, do not allow passwords to be changed immediately when you configure the Minimum password age.

The maximum setting of 24 passwords remembered is the setting used in the Secure (securews) and High Secure (hisecws) default templates for workstations. This setting should not cause any operational problems for most environments, so it will be the value I use for the 'Test' example. The 'Minimum password age' setting should not be set to 0 (zero), otherwise users could change their passwords 24 times to defeat the value of the 'Enforce password history' feature.

If you are not sure what the value of a setting should be, research the information at the following Microsoft Corporation URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/615.asp. You will be able to navigate to each specific 'Policy' for a description of what it means and the acceptable values to set. It is your responsibility to make an informed decision on each setting used in your template. I recommend that you document what each policy means and how you determined the value for that setting. You will be using that information later to make sure your templates are in agreement with your company's security policies. You do not want your template to be in violation of security policies. You want your template to assist you in enforcing security policies.

The 'Account Policies' 'Password Policy' section should look similar to the following example when completed.

Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

The possibility exists that you may not wish to set a specific value. The 'Computer Setting' should be left as 'Not defined' for that situation.

You may want to periodically save your template. Right-click on the name of the template in the example 'Test', and select 'Save'. It may be important to note at this time that all these templates are saved with a '.inf' file extension, and are stored in the %SystemRoot%\security\templates directory (%SystemRoot% is usually defined as C:\WINNT). If you are modifying one of the default templates, you may wish to select the 'Save as' option and give it a new name to prevent

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

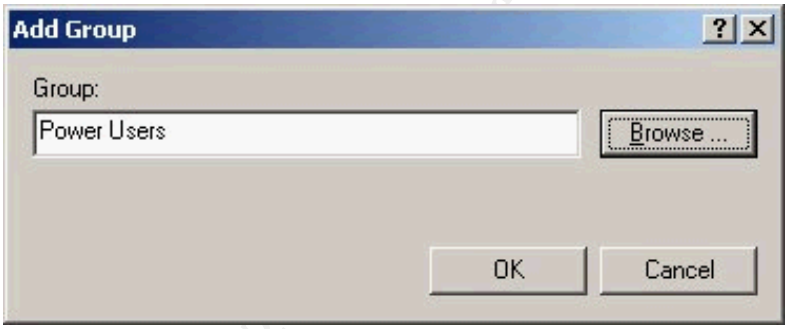
you from overwriting the default template. The template files can be viewed with Notepad.exe, but keep in mind they are Unicode.

Local Policies and Event Log sections

The Local Policies and Event Log sections should both be fully researched and configured in the same way as the 'Account Policies' section.

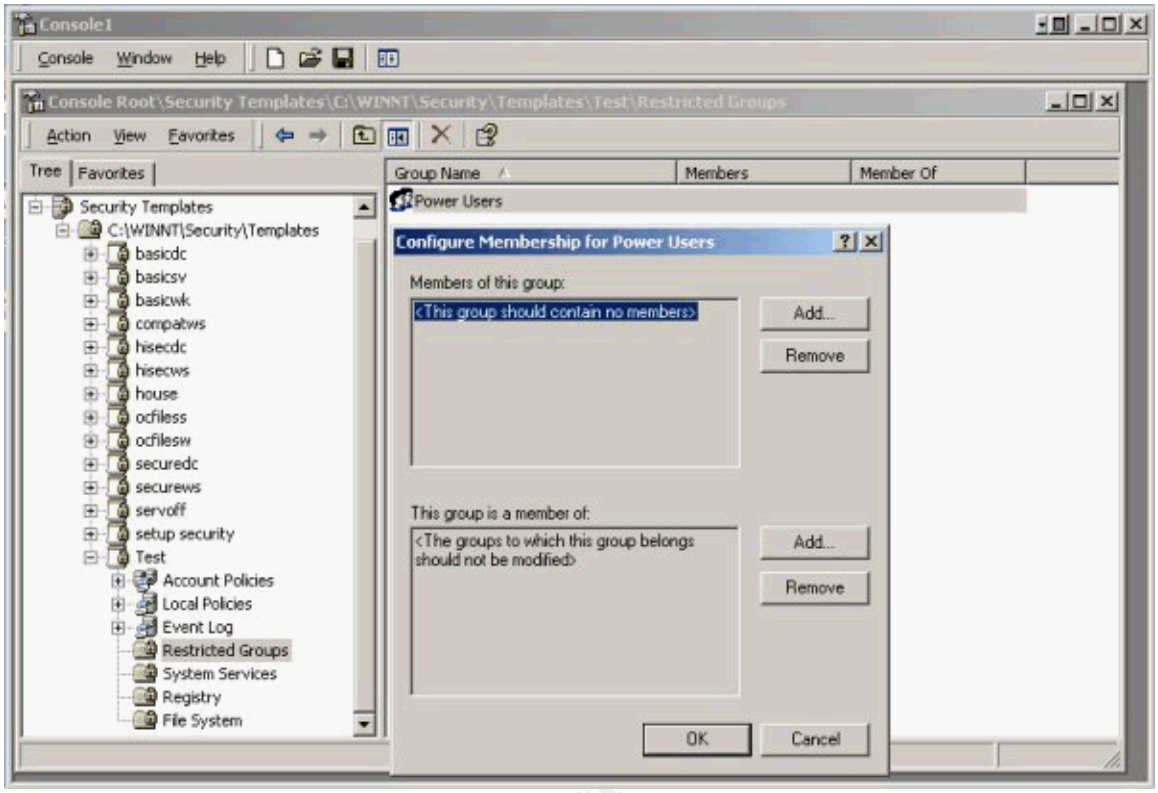
Restricted Groups section

The Restricted Groups section of the Security Template is used to restrict access to sensitive groups. This is designed to prevent users from elevating their privileges to those of groups that are restricted. Users and groups that are authorized to be in a restricted group are added to appropriate access lists. In order to set a restricted group right-click on 'Restricted Groups' and select 'Add Group…' from the list. Then click the 'Browse' button and select a group you want to restrict (i.e. Power Users) and click the 'OK' button.



Double-click on the 'Power Users' 'Group Name' in the right windowpane, and a GUI titled 'Configure Membership for Power Users' will be displayed.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Click the 'Add…' button next to the 'Members of this group:' to add a user to the 'Restricted Group', or the 'Add…' button next to the 'This group is a member of:' to add a group to the 'Restricted Group'. Repeat the process as needed to add additional users or groups to the 'Restricted Group'. Then click the 'OK' button.

<u>System Services section</u>

The 'System Services' section of the Security Template is used to set the startup mode for many system services, and set permissions for the users that will be authorized to start, stop, or pause these services.

Researching what a service does is an important step in deciding how to configure that service through a security template. The following Microsoft Corporation URL: http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp is a "Glossary of Windows 2000 Services". Another source of information one should view to determine how to configure system services is the 'Services' Administrative Tool.

- Click 'Start', click 'Settings', click 'Control Panel', double-click 'Administrative Tools', double-click 'Services'.

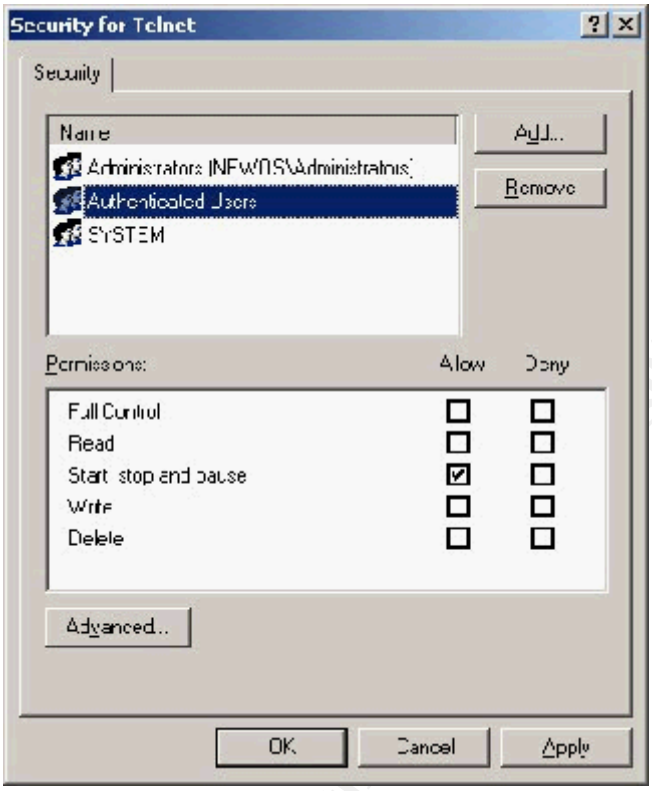
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Services Administrative Tool will give a listing of the Windows 2000 system services and any additional services installed by other software. Each service is listed with a 'Description', 'Status', 'Startup Type', and 'Log On As' field.

In order to set a startup mode on a system service, click on the 'System Services' line under our 'Test' template. A list of system services will appear in the right windowpane. Double-click on the service you wish to set (i.e. Telnet).

Place a checkmark in the box by 'Define this policy setting in the template' by clicking in the box. Select the desired startup mode (Automatic, Manual, or Disabled). This may cause another GUI window titled 'Security for Telnet' to be displayed. This GUI is used to set permissions for authorized users of the service.

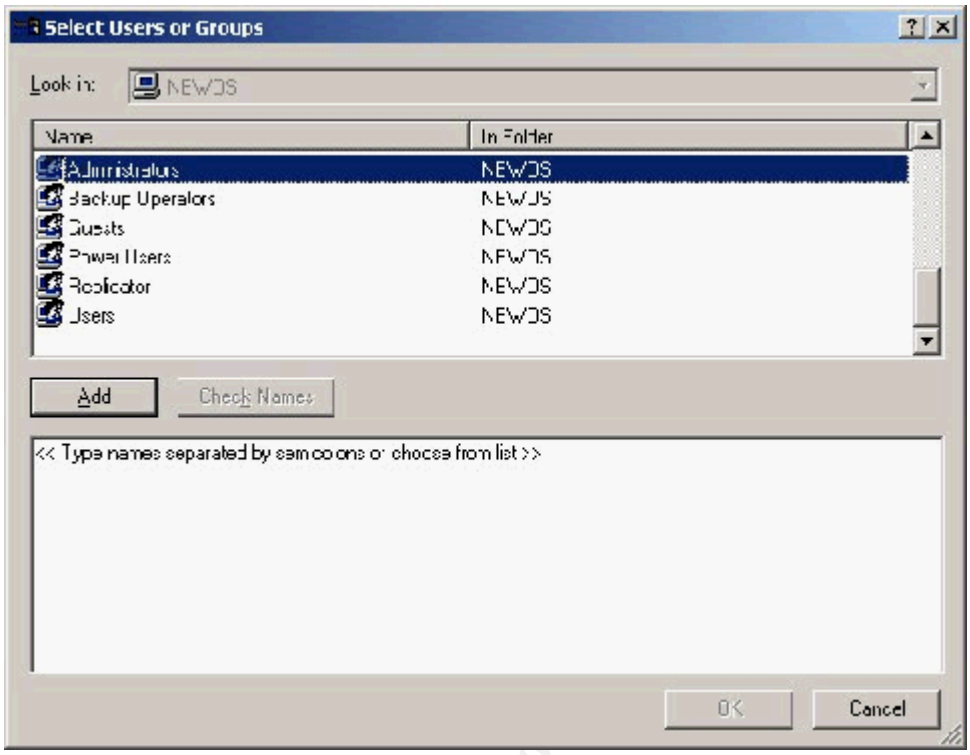
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



What users are allowed to access the service and the level of control each user will have will depend on the operational environment. It is always a good idea to practice the policy of least privilege. Only allow those users who need a service access to it, and restrict their level of access to the lowest level to accomplish their work tasks. To remove a user from the list, highlight the 'Name' of the user and click the 'Remove' button.

To add a user click the 'Add…' button and select the desired user from the GUI titled 'Select Users or Groups' by highlighting the name of the user or group then click the 'Add' button and then click the 'OK' button.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

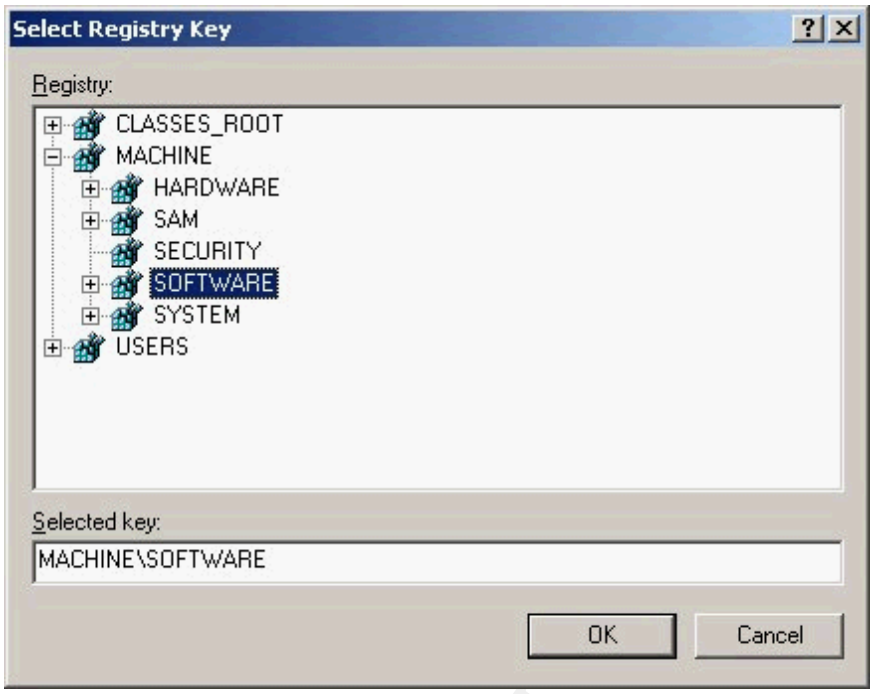


From the GUI titled 'Security for Telnet' click the 'Apply' button and then the 'OK' button. From the GUI titled 'Template Security Policy Setting' click the 'OK' button.

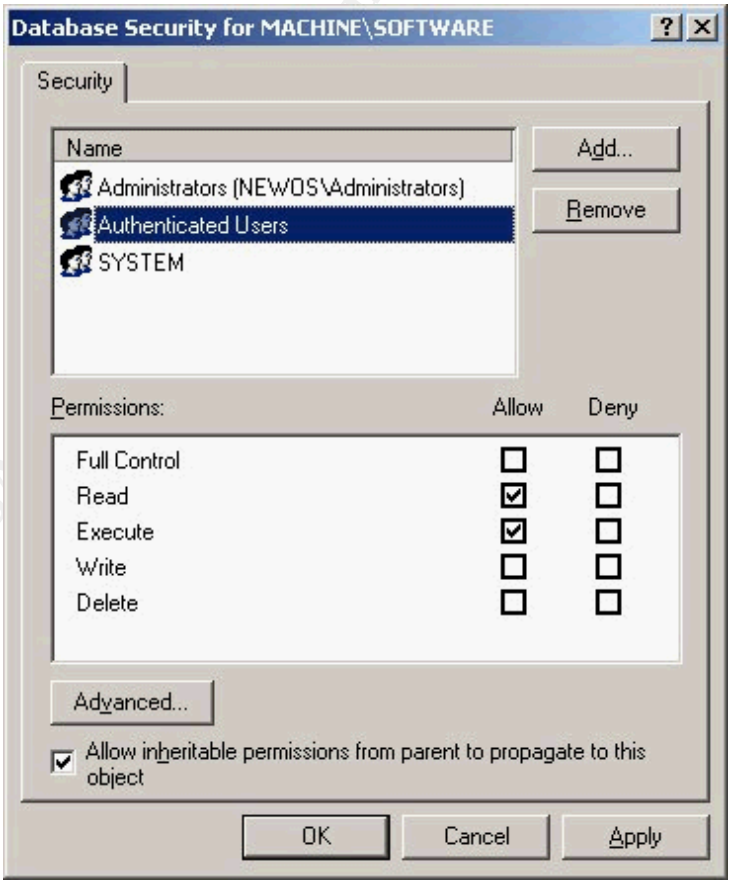
Registry section

The 'Registry' section of the Security Template is used to restrict access to specified registry keys to authorized users and groups. In order to set a registry key right-click on 'Registry' and select 'Add Key…' from the list. Then navigate to the key you wish to set permissions on in the GUI titled 'Select Registry Key' (i.e. MACHINE\SOFTWARE) and click the 'OK' button.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

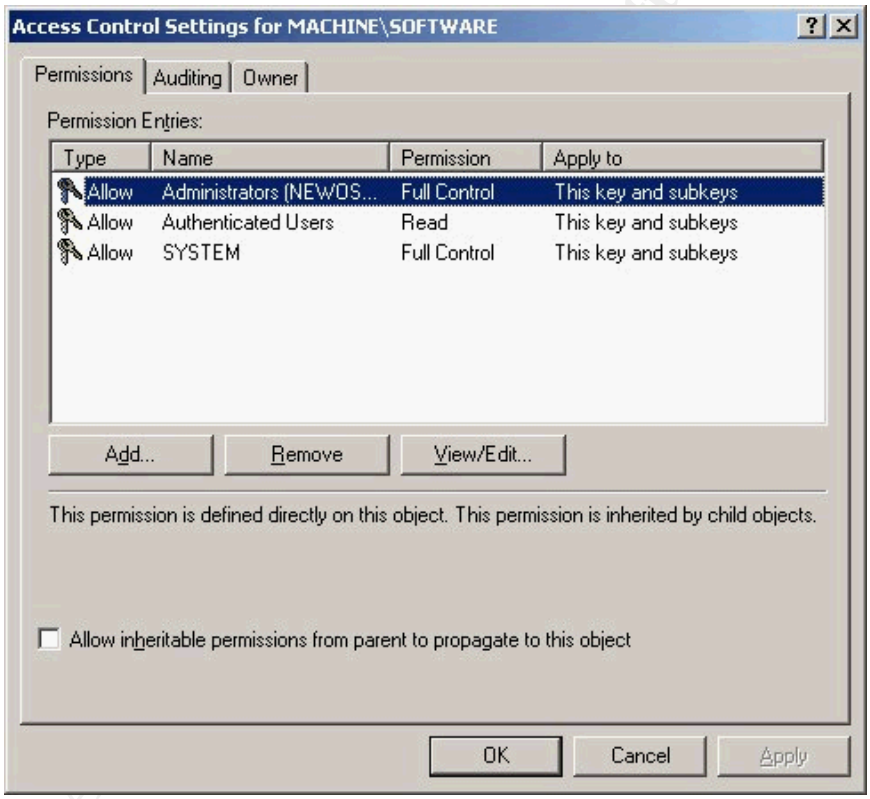


The permissions GUI titled 'Database Security for MACHINE\SOFTWARE' should appear.



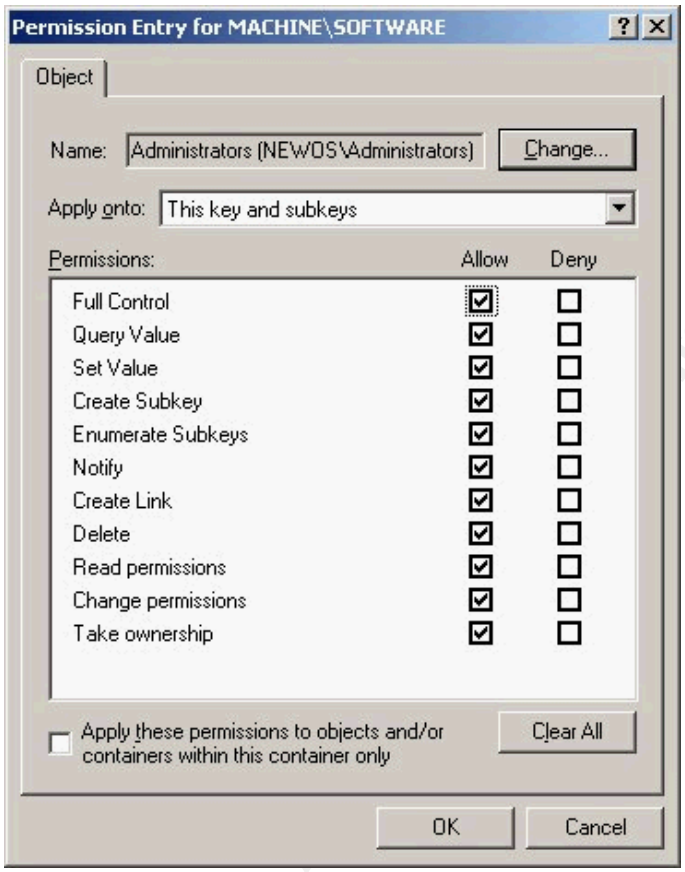
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Permissions are an extremely important factor to evaluate and test before applying them to a system. If permissions are set incorrectly, it could prevent the system from operating properly. It may even cause the system to stop working permanently. This could result in having to reinstall the operating system. The 'Allow inheritable permissions from parent to propagate to this object' feature is checked in the GUI titled 'Database Security for MACHINE\SOFTWARE'. This means that permissions on this key are being inherited from the key above it (i.e. MACHINE). In order to prevent this from happening remove the checkmark from the box by clicking on it. It may be beneficial to see a more detailed view of the permissions that are set. Click on the 'Advanced…' button for a more granular look at setting permissions. A GUI window titled 'Access Control Settings for MACHINE\SOFTWARE' will be displayed.



To set permissions for a specific user or group highlight the choice and click 'View/Edit…' button and the GUI window titled 'Permission Entry for MACHINE\SOFTWARE' should be displayed.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

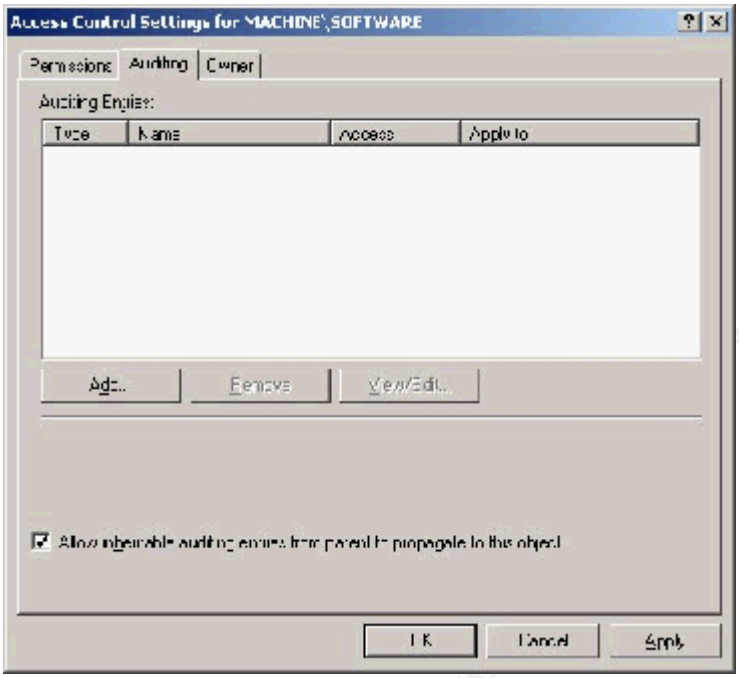


The 'Apply onto:' is an important part of how permissions get set. It determines if the permissions will be set on 'This key only', 'This key and subkeys', or 'Subkeys only'. Cascading of permissions is when the permission on the parent key as passed on to subkeys. This allows large numbers of permissions to be set at once. This is a wonderful feature, but can have unforeseen results. You may need to investigate what the current permissions are before making any change. The list of possible permissions to either allow or deny are:

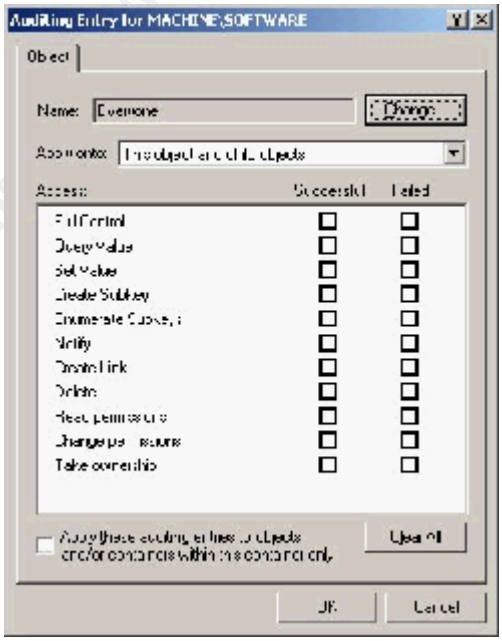
- Full Control
- Query Value
- Set Value
- Create Subkey
- Enumerate Subkeys
- Notify
- Create Link
- Delete
- Read permissions
- Change permissions
- Take ownership

When you clicked that 'Advanced…' button, you hopefully noticed another tab beside the 'Permissions' tab labeled 'Auditing'.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Auditing should be preformed on important registry keys as part of any security template. For permissions it is a good idea to specify single users and groups, but for auditing the 'Everyone' group is an effective setting. It helps prevent the possibility of forgetting to audit a specific group or user. Click the 'Add…' button to get the 'Select User or Group' GUI, select 'Everyone'. Another GUI window should appear titled 'Auditing Entry for MACHINE\SOFTWARE'.



You will be auditing the success and failure of users and groups to use their specified permissions. After setting the events you wish to audit and permissions

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

for your users and groups a GUI window should appear titled 'Template Security Policy Setting'

There are three potential settings for this GUI:

1. Configure this key then, Propagate inheritable permissions to all subkeys
2. Configure this key then, Replace existing permissions on all subkeys with inheritable permissions
3. Do not allow permissions on this key to be replaced

Option 1 - will just add the permissions you set to the key and all inheritable subkeys without removing any permissions currently set.

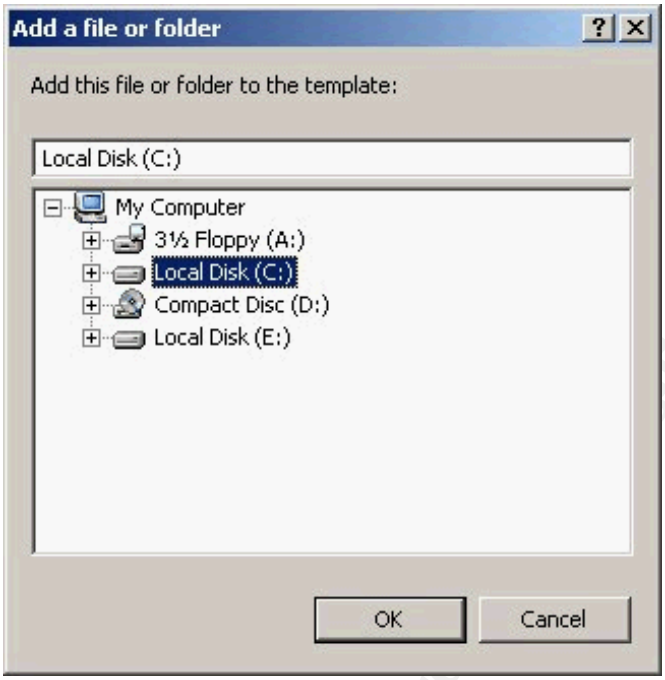
Option 2 - will replace the permissions you set to the key and all inheritable subkeys. This option can cause unforeseen errors if not applied properly. Be very careful and test thoroughly before using this setting.

Option 3 – will prevent permissions from being changed on this key.

<u>File System section</u>

The 'File System' section is very similar to the procedures outlined in the Registry section. The major difference is instead of keys you will be dealing with files and directories. To set the 'File System' right-click on it and click 'Add File…' A GUI window titled 'Add a file or folder' will appear. Navigate to the desired file or folder (i.e. Local Disk (C:)) and click 'OK'.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Determine the permissions and auditing just like you did with the registry section keeping in mind the process is the same, but the specific permissions are different. Permissions for files and folders are:

- Full Control
- Traverse Folder / Execute File
- List folder / Read data
- Read attributes
- Read extended attributes
- Create files / Write data
- Create folders / Append data
- Write attributes
- Write extended attributes
- Delete subfolders and files
- Delete
- Read permissions
- Change permissions
- Take ownership

Sample Test.inf

The information below is what our security template looks like when saved as Test.inf in the %SystemRoot%\security\templates directory. The file values are not easily translated back to the to the security template, but with a little effort and the right web pages it can be done. I have included an Appendix A that

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

maps the settings seen in the Microsoft Management Console (MMC) with the Security Template Snap-in to what the Template headings and values are in the '.inf' file. The Restricted Groups, System Services, Registry, and File System are not included in the Appendix. Please use the references 1-5 for Security Descriptor information related to file and registry permissions and auditing. I will try to explain in more detail the entry we created for 'File Security' in the next section.

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=This template is being used for demonstrational purposes.
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
ClearTextPassword = 0
[Registry Values]
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Registry Keys]
"MACHINE\SOFTWARE",2,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;
SY)S:AR(AU;OICISAFA;SDWDWO;;;WD)(AU;OICIFA;KA;;;WD)"
[File Security]
"%SystemDrive%\",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;O
ICIIO;FA;;;CO)(A;OICI;FA;;;SY)S:AR(AU;OICISAFA;SDWDWO;;;WD)(AU;
OICIFA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
[Service General Setting]
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;R
PWPDTRC;;;AU)(A;;RPWPDTRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;SY)"
```

<u>How to translate a File Security entry</u>

[File Security]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"%SystemDrive%\",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)S:AR(AU;OICISAFA;SDWDWO;;;WD)(AU;OICIFA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

The [File Security] heading is equal to the File System section of the security template from the MMC.

%SystemDrive%\ translates to C:\
The '2' means to replace all permissions
The 'D:' means these are the folder permissions (DACL)
The 'P' means do not inherit permissions from the parent
The 'AR' means SDDL_AUTO_INHERIT_REQ flag is set, which I think means all files or folders created under this directory will inherit permissions from this directory. See *"Security Descriptor Definition Language (SDDL)"*. The U. S. Department of Energy (DOE). URL: http://www.ciac.org/ciacNT/SCM/SDDL.html for more information
The '(A;OICI;FA;;;BA)' means
- 'A' access allowed
- 'OI' files (object inherit)
- 'CI' subfolders (container inherit)
- 'FA' full access or full control
- 'BA' Built-in Administrators
- In summary: Administrators have full control to this folder by default and all files and subfolders

The (A;OICI;0x1200a9;;;AU) means the same as the administrators, except the 'AU' is for Authenticated Users and the '0x1200a9' is the permission Read and Execute
The (A;OICIIO;FA;;;CO) means the same as the administrators, except the 'CO' is for Creator Owner and the 'OICIIO' translates to files and subfolders only
The (A;OICI;FA;;;SY) means the same as the administrators, except the 'SY' is for System
The 'S' means these are the auditing permissions (SACL)
The (AU;OICISAFA;SDWDWO;;;WD)
- 'AU' means audit
- 'SA' means successful access
- 'FA' means failed access
- 'SD' audit delete permission
- 'WD' audit change permissions permission
- 'WO' audit write owner permission
- 'WD' the second time means Everyone group

The (AU;OICIFA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) is an audit listing for failed access on all the other permissions not listed in first entry

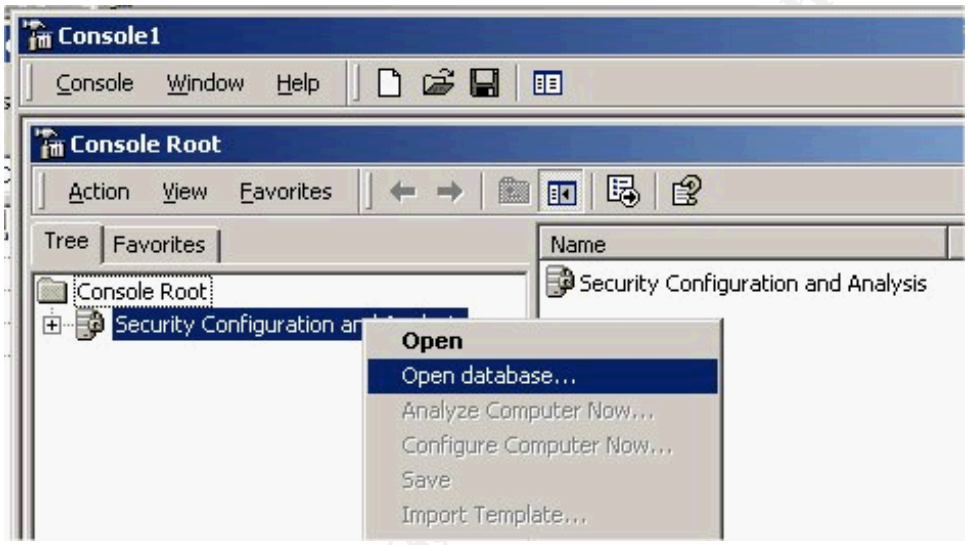
Research the references 1-5 listed below for more technical detail.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

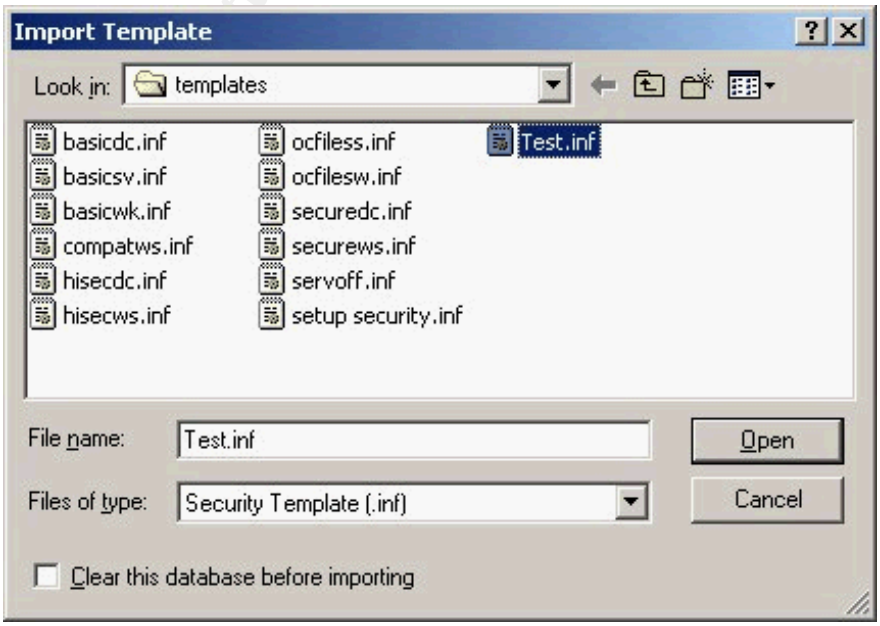
Applying the Security Template to the system

Security Configuration and Analysis Snap-in

Launch the MMC and add the 'Security Configuration and Analysis' Snap-in like we did when we created our security template. Right-click on 'Security Configuration and Analysis' and select 'Open database…'.



Type 'Test.sdb' for the File name in the GUI window that appears titled 'Open database'. Then click the 'Open' button. Another GUI window titled 'Import Template' should appear.



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Select the 'Test.inf' file and click the 'Open' button. Right-click on 'Security Configuration and Analysis' and select 'Analyze Computer Now…' from the list. You will be asked to specify a path for the error log file. Just accept the default location by clicking the 'OK' button. The Analysis will show the differences between our database setting and the current computer setting. If there are no problems with the settings we are changing, we can configure the computer. Right-click on 'Security Configuration and Analysis' and select 'Configure Computer Now…' from the list. You will be asked to specify a path for the error log file. Just accept the default location by clicking the 'OK' button.

Secedit.exe command-line tool

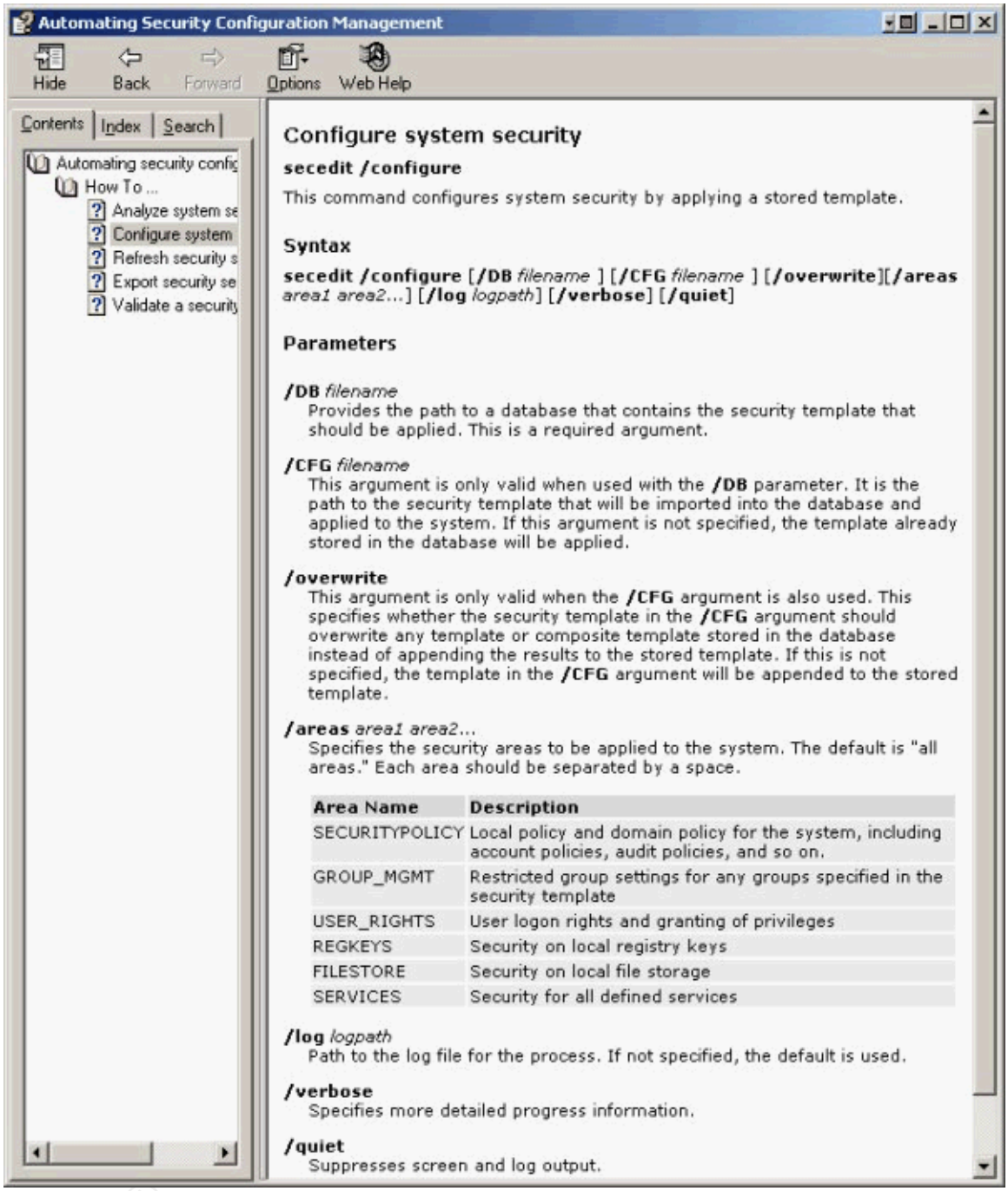
From a command-line type the following to apply the Test.inf security template:

```
secedit.exe /configure /db %SystemRoot%\Security\database\Test.sdb /cfg
    %SystemRoot%\security\templates\Test.inf /log
    %SystemRoot\security\logs\Test.txt /verbose /overwrite
```

This should all be typed in as one continuous line.

A 'Help' GUI on the secedit.exe command-line tool can be displayed by bringing up a command window or from the Start->Run box by typing the line 'secedit.exe /?' without the quotation marks at the prompt.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Summary

The information covered by this paper is intended to provide a good understanding of how security templates are constructed. I hope the message is understood that all settings must be thoroughly researched and tested before being applied to an operational system. This tool can help enforce security policies and save time. The security template should be continually reviewed as system requirements and security needs change.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

1. *"Security Descriptor Definition Language (SDDL)"*. The U. S. Department of Energy (DOE). URL: http://www.ciac.org/ciacNT/SCM/SDDL.html
2. *"SID Strings"*. Microsoft Corporation. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/sid_strings.asp
3. *"Security Descriptor String Format"*. Microsoft Corporation. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/security_descriptor_string_format.asp
4. *"ACE Strings"*. Microsoft Corporation. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/ace_strings.asp
5. *"Bug in SCM for NT 4.0 (2 of 2) - Long"*. Raymond P. Galloni (rpgallon@MITRE.ORG) Tue. Aug. 24, 1999 – 09:45:59 EDT. URL: http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=ind9908&L=ntbugtraq&F=P&S=&P=6074
6. *"Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set"*. Network Security Evaluations and Tools Division of the Systems and Network Attack Center. Author: Julie M. Haney Updated: July 22, 2002. Version 1.1.1. URL: http://nsa1.www.conxion.com/win2k/guides/w2k-3.pdf
7. *"Microsoft Security Configuration Manager for Windows NT 4.0"*. Microsoft Corporation. URL: http://www.microsoft.com/ntserver/docs/scm-nt4.doc
8. *"Security Setting Descriptions"*. Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/615.asp
9. *"Center for Internet Security Benchmarks and Scoring Tool for Windows 2000 and Windows NT"*. The Center for Internet Security. URL: http://www.cisecurity.org/bench_win2000.html
10. *"HOW TO: Apply Predefined Security Templates in Windows 2000"*. Microsoft Corporation. URL: http://support.microsoft.com/?kbid=309689
11. *"Group Policy and Security"*. Windows & .NET MAGAZINE. Author: Robert McIntosh InstantDoc #9169 July 24, 2000. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=9169
12. *"Chapter 4 - Windows 2000 Common Criteria Security Configuration Templates"*. Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGc4.asp
13. *"Enforce password history"*. Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/500.asp
14. *"Glossary of Windows 2000 Services"*. Microsoft Corporation. Date: July 31, 2001. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A

Mapping the MMC security template settings to the template .inf file

MMC Policy	Template Section	Template Value
Password Policy		
Enforce password history	[System Access]	PasswordHistorySize
Maximum password age	[System Access]	MaximumPasswordAge
Minimum password age	[System Access]	MinimumPasswordAge
Minimum password length	[System Access]	MinimumPasswordLength
Passwords must meet complexity requirements	[System Access]	PasswordComplexity
Store password using reversible encryption for all users in the domain	[System Access]	ClearTextPassword
Account Lockout Policy		
Account lockout duration	[System Access]	LockoutDuration
Account lockout threshold	[System Access]	LockoutBadCount
Reset account lockout counter after	[System Access]	ResetLockoutCount
Kerberos Policy		

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Enforce user logon restrictions	[Kerberos Policy]	MaxTicketAge
Maximum lifetime for service ticket	[Kerberos Policy]	MaxRenewAge
Maximum lifetime for user ticket	[Kerberos Policy]	MaxServiceAge
Maximum lifetime for user ticket renewal	[Kerberos Policy]	MaxClockSkew
Maximum tolerance for computer clock synchronization	[Kerberos Policy]	TicketValidateClient

Audit Policy

Audit account logon events	[Event Audit]	AuditAccountLogon
Audit account management	[Event Audit]	AuditAccountManage
Audit directory service access	[Event Audit]	AuditDSAccess
Audit logon events	[Event Audit]	AuditLogonEvents
Audit object access	[Event Audit]	AuditObjectAccess
Audit policy change	[Event Audit]	AuditPolicyChange
Audit privilege use	[Event Audit]	AuditPrivilegeUse
Audit process tracking	[Event Audit]	AuditProcessTracking
Audit system events	[Event Audit]	AuditSystemEvents

User Rights Assignment

Access this computer from the	[Privilege Rights]	SeNetworkLogonRight

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

network		
Act as part of the operating system	[Privilege Rights]	SeTcbPrivilege
Add workstations to domain	[Privilege Rights]	SeMachineAccountPrivilege
Back up files and directories	[Privilege Rights]	SeBackupPrivilege
Bypass traverse checking	[Privilege Rights]	SeChangeNotifyPrivilege
Change the system time	[Privilege Rights]	SeSystemtimePrivilege
Create a pagefile	[Privilege Rights]	SeCreatePagefilePrivilege
Create a token object	[Privilege Rights]	SeCreateTokenPrivilege
Create permanent shared objects	[Privilege Rights]	SeCreatePermanentPrivilege
Debug programs	[Privilege Rights]	SeDebugPrivilege
Deny access to this computer from the network	[Privilege Rights]	SeDenyNetworkLogonRight
Deny logon as a batch job	[Privilege Rights]	SeDenyBatchLogonRight
Deny logon as a service	[Privilege Rights]	SeDenyServiceLogonRight
Deny logon locally	[Privilege Rights]	SeDenyInteractiveLogonRight
Enable computer and user accounts to be trusted for delegation	[Privilege Rights]	SeEnableDelegationPrivilege
Force shutdown from a remote	[Privilege Rights]	SeRemoteShutdownPrivilege

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

system		
Generate security audits	[Privilege Rights]	SeAuditPrivilege
Increase quotas	[Privilege Rights]	SeIncreaseQuotaPrivilege
Increase scheduling priority	[Privilege Rights]	SeIncreaseBasePriorityPrivilege
Load and unload device drivers	[Privilege Rights]	SeLoadDriverPrivilege
Lock pages in memory	[Privilege Rights]	SeLockMemoryPrivilege
Log on as a batch job	[Privilege Rights]	SeBatchLogonRight
Log on as a service	[Privilege Rights]	SeServiceLogonRight
Log on locally	[Privilege Rights]	SeInteractiveLogonRight
Manage auditing and security log	[Privilege Rights]	SeSecurityPrivilege
Modify firmware environment values	[Privilege Rights]	SeSystemEnvironmentPrivilege
Profile single process	[Privilege Rights]	SeProfileSingleProcessPrivilege
Profile system performance	[Privilege Rights]	SeSystemProfilePrivilege
Remove computer from docking station	[Privilege Rights]	SeUndockPrivilege
Replace a process level token	[Privilege Rights]	SeAssignPrimaryTokenPrivilege
Restore files and directories	[Privilege Rights]	SeRestorePrivilege
Shut down the system	[Privilege Rights]	SeShutdownPrivilege
Synchronize directory	[Privilege Rights]	SeSyncAgentPrivilege

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

service data		
Take ownership of files or other objects	[Privilege Rights]	SeTakeOwnershipPrivilege

Security Options

Additional restrictions for anonymous connections	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous
Allow server operators to schedule tasks (domain controllers only)	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl
Allow system to be shut down without having to log on	[Registry Values]	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon
Allowed to eject removable NTFS media	[Registry Values]	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD
Amount of idle time required before disconnecting session	[Registry Values]	MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect
Audit the access of global system objects	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects
Audit use of Backup and Restore privilege	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing
Automatically log off users when logon time expires	[System Access]	ForceLogoffWhenHourExpire

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Automatically log off users when logon time expires (local)	[Registry Values]	MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\EnableForcedLogOff
Clear virtual memory pagefile when system shuts down	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown
Digitally sign client communicatio n (always)	[Registry Values]	MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\RequireSecuritySignature
Digitally sign client communicatio n (when possible)	[Registry Values]	MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\EnableSecuritySignature
Digitally sign server communicatio n (always)	[Registry Values]	MACHINE\System\CurrentControlSet\Services\Lanman Workstation\Parameters\RequireSecuritySignature
Digitally sign server communicatio n (when possible)	[Registry Values]	MACHINE\System\CurrentControlSet\Services\Lanman Workstation\Parameters\EnableSecuritySignature
Disable CTRL+ALT+D EL requirement for logon	[Registry Values]	MACHINE\Software\Microsoft\Windows\CurrentVersion \Policies\System\DisableCAD
Do not display last user name in logon screen	[Registry Values]	MACHINE\Software\Microsoft\Windows\CurrentVersion \Policies\System\DontDisplayLastUserName
LAN Manager Authentication Level	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Lsa\LmC ompatibilityLevel
Message text for users attempting to log on	[Registry Values]	MACHINE\Software\Microsoft\Windows\CurrentVersion \Policies\System\LegalNoticeText
Message title for users attempting to	[Registry Values]	MACHINE\Software\Microsoft\Windows\CurrentVersion \Policies\System\LegalNoticeCaption

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

attempting to log on		
Number of previous logons to cache (in case domain controller is not available)	[Registry Values]	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount
Prevent system maintenance of computer account password	[Registry Values]	MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange
Prevent users from installing printer drivers	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers
Prompt user to change password before expiration	[Registry Values]	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning
Recovery Console: Allow automatic administrative logon	[Registry Values]	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel
Recovery Console: Allow floppy copy and access to all drives and all folders	[Registry Values]	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand
Rename administrator account	[System Access]	NewAdministratorName
Rename guest account	[System Access]	NewGuestName
Restrict CD-ROM access to locally logged-on user only	[Registry Values]	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Restrict floppy access to locally logged-on user only	[Registry Values]	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies
Secure channel: Digitally encrypt or sign secure channel data (always)	[Registry Values]	MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal
Secure channel: Digitally encrypt secure channel data (when possible)	[Registry Values]	MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel
Secure channel: Digitally sign secure channel data (when possible)	[Registry Values]	MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel
Secure channel: Require strong (Windows 2000 or later) session key	[Registry Values]	MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey
Secure system partition (for RISC platforms only)	[System Access]	SecureSystemPartition
Send unencrypted password to connect to third-party SMB servers	[Registry Values]	MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Shut down system immediately if unable to log security audits	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail
Smart card removal behavior	[Registry Values]	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption
Strengthen default permissions of global system objects (e.g. Symbolic Links)	[Registry Values]	MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode
Unsigned driver installation behavior	[Registry Values]	MACHINE\Software\Microsoft\Driver Signing\Policy
Unsigned non-driver installation behavior	[Registry Values]	MACHINE\Software\Microsoft\Non-Driver Signing\Policy

Settings for Event Logs

Maximum application log size	[Application Log]	MaximumLogSize
Maximum security log size	[Security Log]	MaximumLogSize
Maximum system log size	[System Log]	MaximumLogSize
Restrict guest access to application log	[Application Log]	RestrictGuestAccess
Restrict guest access to security log	[Security Log]	RestrictGuestAccess
Restrict guest access to system log	[System Log]	RestrictGuestAccess

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Retain application log	[Application Log]	RetentionDays
Retain security log	[Security Log]	RetentionDays
Retain system log	[System Log]	RetentionDays
Retention method for application log	[Application Log]	AuditLogRetentionPeriod
Retention method for security log	[Security Log]	AuditLogRetentionPeriod
Retention method for system log	[System Log]	AuditLogRetentionPeriod
Shut down the computer when the security audit log is full	[Event Audit]	CrashOnAuditFull

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**