Global Information Assurance Certification Paper

SANS Practical Assignment

"Securing Windows 2000 with Security Templates"

(Option 2)

Securing Windows Certification (GCWN)

Ver 3.1 (April 2002)

Submitted by: Patricia Shirer

May 16, 2003

TABLE OF CONTENTS

I. INTRODUCTION:

The Role of Group Policy

Group Policy is a key management feature of Windows 2000 Server Operating System (OS) which provides for centralized security configuration and management of Windows 2000 servers and clients in a domain environment. It is no news to system administartors that both Windows NT and Windows 2000 are notoriously full of vulnerabilities that can place an organization at risk. While in Windows NT most of the security settings were done manually using registry edits, Windows 2000 has policy based security settings which can be defined in the Local Security Policy or assigned by Group Policy. This can prove to be an invaluable tool to administrators trying to secure their Windows 2000 environments. Used in conjuction with a solid cabling infrastructure, a secure routing policy and business policies defining acceptable use, the desired level of security can be achieved.

Using Group Policy, specific options can be set to manage registry-based policy settings, security settings, software installation, scripts, folder redirection, remote installation, and Internet Explorer maintenance. It is similar, but much more powerful than System Policy in Windows NT, as shown in the table below. These settings contained in Group Policy objects (GPO) can be associated with Active Directory (AD) containers, such as sites, domains, and organizational units (OUs). Each computer and user placed in these containers receives these settings when the computer starts and the user logs in. In this way, an administrator is assured that anyone accessing the network will have sufficient rights while minimizing vulnerabilities inherent in the Windows OS.

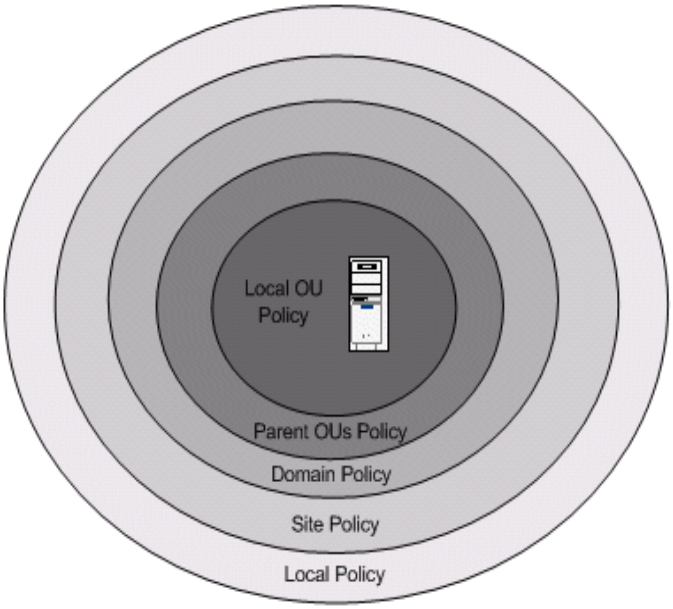
The following table lists the components of Group Policy[1].

Component	Description
Administrative Templates	Registry based policy, known as System Policy in Windows NT® Server 4.0.
Security Settings	Security settings for domains, computers and users.
Software Installation	Assign or publish applications.
Internet Explorer Maintenance	Administer Internet Explorer after deployment.
Scripts	User logon/logoff and computer startup/shutdown.
Folder Redirection	The ability to re-direct folders and files to the network.

[1] Microsoft Technet "Chapter 3, Managing Security with Windows 2000 Group Policy" March 2003

Granular Application of Settings

Usually, security is based on the role of the server, workstation or user involved. For example, a web server would require different security settings than a domain controller, terminal server or member server. Group Policy objects applied to servers at the domain and organization unit can provide this security at a granular level. Policies can be created and applied in a "layered" manner so that incrementally each server, workstation and user has just the right protection. This is done by configuring multiple "templates" and applying them in a specific order to achieve the desired affect. It is very important to understand how these policies are applied. [2]



First is the local security policy, followed by GPO's for the site, domain, parent OU and child OU. These settings are applied sequentially and accumulate. In case of a conflict in the settings, the later policy overides the previous setting.

Microsoft Management Console

In Windows 2000, security policies can be applied directly via the command line using Secedit, or by using the GUI provided in the Microsoft Management Console (MMC). Tools, called "snap-ins", can be imported into the MMC. There are two snap-ins for administering Group Policy: the Security Templates and the Security Configution and Analysis Tool. These tools allow an administrator to create/edit security configuration files, perform security analysis, graphically review the analysis results and apply the configurations to a system(s).

Due to the powerful nature of Group Policies, Microsoft recommends several "Best Practices" to ensure a successful implemenation:

- Simplify. Users and computers will be placed in the same organizational unit. Block

[2] National Security Agency "Microsoft Windows 2000 Network Architecture Guide." March 5, 2003

Inheritance and No Override will not be used, unless there is no other alternative. We will avoid creating multiple GPOs with conflicting policies that apply to the same users or computers.

- Document. Group Policies will be diagramed as well as documented in writing.
- Test. A test server on a test network will be setup to make sure new policies are working properly. [3]

Templates and Checklists

Templates are files containing security settings. To help administators, Microsoft developed sample templates for automating and enforcing a consistent security policy across the organization. They reside in the %SystemRoot%\Inf folder. These templates contain settings for domains, various server roles and workstations that can be customized and imported into Group Policies or applied directly using Secedit.exe. This allows the Administrator centralized control over the security needs of the organization and is a major time saving tool! Some of the templates provided include: [4]

Role	Description	Security Template
Windows 2000 Domain Controller and Workstations	The Basic templates specify default security settings for all security areas, with the exception of user rights and group membership.	BasicDC.inf, BasicWS.inf
Windows 2000 Domain Controller and Workstations	The Secure templates provide increased security for areas of the operating system that are not covered by permissions, including: increased security settings for the account policy, auditing, and for some well-known security-relevant registry keys. Access Control Lists (ACLs) are not modified by this template, because the assumption is that default Windows 2000 security settings are in effect.	SecureDC.inf, SecureWS.inf
Windows 2000 Domain Controller and Workstations	The Highly Secure templates are provided for Windows 2000-based computers that operate in native Windows 2000 environments only. Requires that all network communications be digitally signed and encrypted at a level that can only be provided by Windows 2000. Computers configured with this template cannot communicate with downlevel Windows clients.	HisedDC.inf, HisecWS.inf

Out of the box, the templates actually applied are called Setup_Security.inf and DC_Security.inf if the server is a Domain Controller. These templates can be life savers if something goes wrong when building and applying advanced settings to Domain Controllers and Servers. Thorough testing in a non-production environment is strongly recommended.

[3] National Security Agency "Guide to Securing Microsoft Windows 2000 Group Policy", March 5, 2003

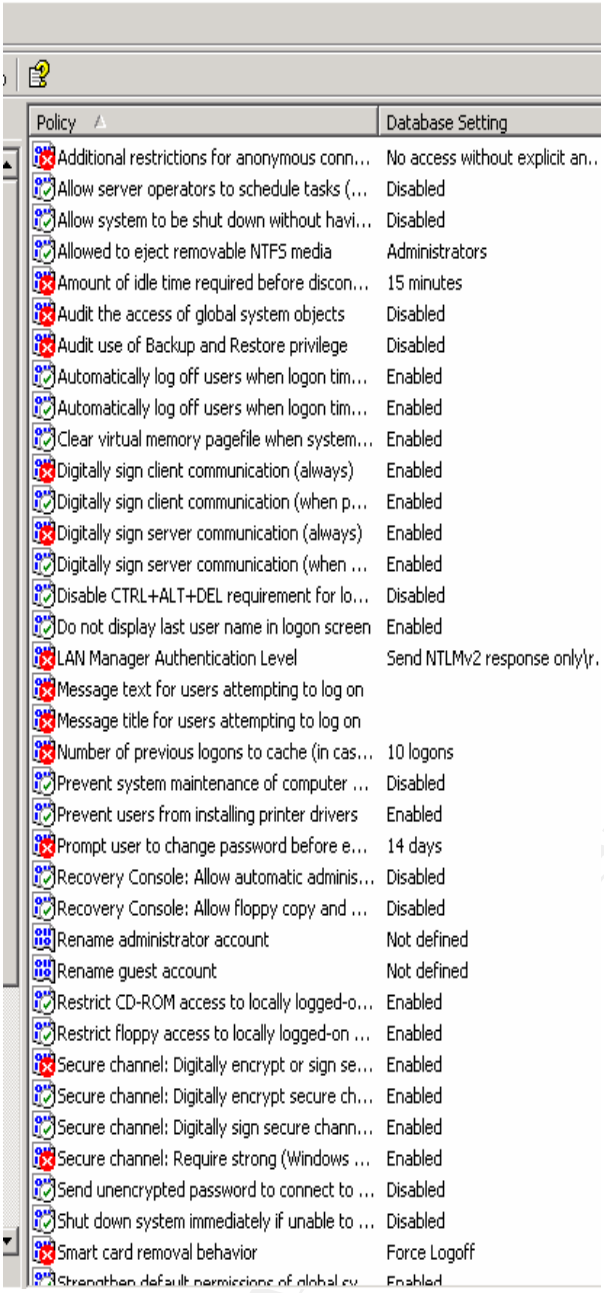
[4] Microsoft Technet #Q309689 "HOW TO: Apply Predefined Security Templates in Windows 2000", October 26, 2002

The National Secrutiy Agency (NSA) and National Institue have also developed and distributed configuration templates for Microsoft Windows 2000 OS. These templates reflect the cooperation and input of other government agencies and industry partners who provided their expertise and extensive technical review. The templates available from NSA for Windows 2000 are: [5]

Roles	Description	Security Template
Windows 2000 Domain Controller, Servers and Workstations	Default	W2K_DC.inf, W2K_Server.inf and W2K_Workstation.inf
Windows 2000 Member Servers	Enhanced security settings for Domain Controllers, Member Servers and Workstations	W2K_Server.inf
Windows 2000 Professional	Enhanced settings for workstations.	W2K_Workstation.inf
Windows 2000 Domain	Enhanced account policy settings to be applied in a Domain-level Group Policy Object	W2K_Domain.inf

The National Institute of Standards and Technology (NIST) has also developed templates in conjuction with the NSA, DISA, CIS, and SANS. The NSA and NIST templates offer a much higher degree of security than currently offered in Microsoft templates. Specifically, the Microsoft templates do not try to define File System, Registry, Kerberos or User Rights Assignment. The following screen shows some of the default settings of Microsofts hisecdc.inf policy.

[5] National Security Agency "Guide to Securing Microsoft Windows 2000 Group Policy." March 5, 2003



Policy	Database Setting
Additional restrictions for anonymous conn...	No access without explicit an...
Allow server operators to schedule tasks (...	Disabled
Allow system to be shut down without havi...	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before discon...	15 minutes
Audit the access of global system objects	Disabled
Audit use of Backup and Restore privilege	Disabled
Automatically log off users when logon tim...	Enabled
Automatically log off users when logon tim...	Enabled
Clear virtual memory pagefile when system...	Enabled
Digitally sign client communication (always)	Enabled
Digitally sign client communication (when p...	Enabled
Digitally sign server communication (always)	Enabled
Digitally sign server communication (when ...	Enabled
Disable CTRL+ALT+DEL requirement for lo...	Disabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\r.
Message text for users attempting to log on	
Message title for users attempting to log on	
Number of previous logons to cache (in cas...	10 logons
Prevent system maintenance of computer ...	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before e...	14 days
Recovery Console: Allow automatic adminis...	Disabled
Recovery Console: Allow floppy copy and ...	Disabled
Rename administrator account	Not defined
Rename guest account	Not defined
Restrict CD-ROM access to locally logged-o...	Enabled
Restrict floppy access to locally logged-on ...	Enabled
Secure channel: Digitally encrypt or sign se...	Enabled
Secure channel: Digitally encrypt secure ch...	Enabled
Secure channel: Digitally sign secure chann...	Enabled
Secure channel: Require strong (Windows ...	Enabled
Send unencrypted password to connect to ...	Disabled
Shut down system immediately if unable to ...	Disabled
Smart card removal behavior	Force Logoff
Strengthen default permissions of global sy...	Enabled

Policy	Database Setting
Access this computer from the network	Not defined
Act as part of the operating system	Not defined
Add workstations to domain	Not defined
Back up files and directories	Not defined
Bypass traverse checking	Not defined
Change the system time	Not defined
Create a pagefile	Not defined
Create a token object	Not defined
Create permanent shared objects	Not defined
Debug programs	Not defined
Deny access to this computer from the network	Not defined
Deny logon as a batch job	Not defined
Deny logon as a service	Not defined
Deny logon locally	Not defined
Enable computer and user accounts to be trusted for delegation	Not defined
Force shutdown from a remote system	Not defined
Generate security audits	Not defined
Increase quotas	Not defined
Increase scheduling priority	Not defined
Load and unload device drivers	Not defined
Lock pages in memory	Not defined
Log on as a batch job	Not defined
Log on as a service	Not defined
Log on locally	Not defined
Manage auditing and security log	Not defined
Modify firmware environment values	Not defined
Profile single process	Not defined
Profile system performance	Not defined
Remove computer from docking station	Not defined
Replace a process level token	Not defined
Restore files and directories	Not defined
Shut down the system	Not defined
Synchronize directory service data	Not defined
Take ownership of files or other objects	Not defined

Therefore, the NSA templates will be used here bacause:

- of the broadness and depth of the security applied
- the school is directed by law to provide a safe computing environment for students
- these templates are derived from a culmination of input from corporate, government and security specialists.
- they include extensive file system, registry and user rights.

Recommended Checklist

A server can be returned to it's original configuration by reapplying Microsoft's Setup_Security.inf and DC_Security.inf. However, this is not an absolute. Great care should always be taken when applying templates because a misconfiguration can render a system unusable. Here is a list of guidelines recommended by the NSA when applying templates: [6]

- Understand the warnings and problems that can occur. The templates make changes to the server's registry and file system. Starting in a test environment is highly recommended.
- Make a backup of the system.
- Apply the latest service packs and desired critical updates for your server software.
- Review the templates thoroughly and determine which best suits the requirements of your organization. Pay special attention to warnings about certain settings that could adversley affect your network.
- Make copies of the templates and use them for modification and application to your systems. Keep the original templates intact.
- If using the templates provided by NSA, there are several new security options available. To access them, you will need to download the sceregvl.inf file to your %SystemRoot%\inf folder and run "refgvr32 scecli.dll". (Make sure to make a backup copy of sceregvl.inf.)
- Some important security options are not set by default, but deserve your consideration: rename the Guest and Administrator accounts, and logon banners.

II. DESCRIPTION:

Existing Network Design and Security

An all boys high school had a network of aging Windows NT 4.0 Servers on three separate domains (student, faculty and administation) and two separate cable plants (student & faculty/admin). Separate networks were created to meet the growing needs of each area. Yet, due to the lack of centralized standards, there was no forethought or regard given to sharing resources or elimating redundancies. The only consensus between the administrators of these networks was to ensure security of sensitive data by keeping the students off the faculty/admin networks. Thus, the separate cable plants were used.

[6] National Security Agency "Guide to Securing Microsoft Windows 2000 Group Policy." March 5, 2003

The faculty network consisted of one Windows NT 4.0 Server (PDC) on a cable plant that linked 40 Windows NT workstations in teacher offices. It was used primarily to store data in personal folders, share printers and access a program called "Grade Book". There were no groups, login scripts or security policies being utilized. Teachers were not required to change their passwords.

The administration network had 3 Windows NT Servers on a cable plant with 35 PCs running Windows 9x. The PDC was mainly used for file and print sharing, one BDC ran the MAS 90 accounting system and another BDC ran an Oracle database. A custom application was created in Oracle for tracking Student and Alumi information including grades, progress reports, attendance, donations and giving histories. In order to give the faculty access to enter data, a cable was run to link the two networks and a two way trust was setup between the Admin & Faculty domains. Groups and login scripts were utilized to limit access to sensitive financial data.

The student domain contained three Windows NT servers, one PDC and two BDCs. The cable plant connected over 300 PCs in classrooms, running Windows NT, 2000 and several Windows 9x. This network was used by the students to store homework and classroom assignments. Each student had an NTFS secured personal folder where they were allowed to save 10MB of data. Disk quotas were handled a product called "Quota Manager" by NTP Software. There were several applications installed on the network server for science and chemistry classes that were accessed by the students using a mapped drive provided via their personal profile. A student policy had been created using NT's System Policy, that limited desktop access and capabilities and provided default paths for MS Office applications. There were no login scripts, no groups and the servers were administered by four teachers who had all been given full administrator rights.

Eventually, teachers requested accounts to access the student network so they could place assignments, quizes and tests in students folders. The faculty network was not linked to the student network so teachers had to carry data on diskette to the classroom, login in with an account on the student domain, and copy files to the student's folders. The teachers each had an NTFS secured folder and full rights to all the student folders.

Security Requirements and Goals

The President of the school demands a high level of external and internal security for the network. In this environment, it will be important to provide a high level of security at the desktop as well as at the server against these security risks:

- External risks from hackers and alumni. Data to protect = alumni records, alumni giving history and financial data.
- Internal risks from student hackers. Data to protect = grades, progress reports, attendance, student records, homework assignments, tests and exams.

The school's internet access is provided by the School District who provide firewall and content filtering for all network traffic. This should reduce the risk of external attacks.

Internally, sensitive data must be protected from students, several of whom have MSCE certification! Dispite a strict computer policy that forbids sharing of account and password information, there have been several instances of students accessing other students files and, in one case hacking the Administrator password.

Plan for the Student Network

To achieve this level of internal security, the following issues need to be addressed:

Security Goals	Security Solution
Ensure security of Administration and Faculty data on a single cable plant with Students to reduce costs and allow centralized management	Install Cisco switches and concentrators and implement VLANs; implement NTFS file auditing on Faculty and Administration folders.
Allow secure remote access for Faculty to Student grades, progress reports	Install Cisco VPN concentrator and require DES3 encryption
Reduce the number of serverrs to support	Consolidate number of servers to two
Higher level of authentication	Configure **NSA** templates to NTLM authentication (will need to retire Windows NT and 9x clients), and cached credetials
More detailed auditing of system with alert notification of possible intrusion, tampering or problems	Configure **NSA** Auditing Policies and Event Log settings; use 3rd party tools from GFI, SolarWinds and APC
Have fewer system administrators and restrict access to secure areas	Configure **NSA** Restricted Group settings; keep all equipment behind locked doors.
Tighter server security by protecting available services, file system and registry security	Configure **NSA** System Service, File System and Registry Policy settings
Prevent students from using too much space on server hard disks; could prevent large downloads	Configure **NSA** Administrative Template settings for System, Quota Policies
Lockdown Student desktops; only run approved apps; limit disk space; no rights to install software or drivers.	Configure **NSA** Student Workstation Policies.

The problems caused by having separate cable plants outweigh the security benefit they offer. The same level of security can be achieved using a single cable plant and implementing VLANs, virtual local area networks. A new cable plant has been designed and installed using Cisco 3548 Ethernet Switches. The switches are centrallized in two stacks, one in the school and one in the administration building. VLANs will be configured to keep Student PCs from accessing Faculty and Admin data. This can be done on a port by port basis and will eliminate the need to have separate cable plants. A Cisco VPN concentrator will be configured to allow teachers using PCs on Student VLANs to have access to resources in the Faculty/Admin network via a secure tunnel using DES3 encryption. In the future, the VPN concentrator will allow teachers and administrators access to vital information from outside the school via high speed internet connections.

A decision has been made to replace the three small Windows NT servers that have been in service for four years. These servers were all clone PCs, there was no service contract and no standards were applied across the network. There was one PDC and two BDC's. The plan is to buy a new server, install Windows 2000 Server and retire the Windows NT servers. The new server will provide home directories for students, printer access, DNS and WINS services. A new domain will be created and a one way trust

will be setup temporarilly to copy data from the old domain servers. One of the retired NT servers will be re-conditioned and installed with Windows 2000 Server to act as a member server for Active Directory replication, WINS and DNS services. This will provide a level of redundancy until other servers are added to the network in the future.

The new server is a Dell PowerEdge 2600 server with the following configuration: RAID 5 utilizing four 36GB 15k drives, 1.5GB memory, 2 Penitum 4 1.4Ghz processors, a 40/80GB DLT tape drive, redundant power supplies and redundant 1000MB ethernet cards. The Operating System is Windows 2000 Server with Service Pack 3 and all critical updates applied. Computer Associates Etrust InoculateIT 6.0 is installed on the server and workstations. The server is configured to check for updates via the internet every eight hours. The workstations are configured in groups to to check the server for updates every eight hours, and are staggered to reduce the amount of traffic generated during an update. ArcServeIT 2000 is used for tape backup management

The Dell server and Cisco switches will be located in a locked room that has a climate controlled environment. The only people with access will be the two teachers who have been assigned to support the network and their hired computer consultant. An APC 1500 watt Smart-UPS is connected to the server, and APC 700 watt Smart-UPS's with environmentatl monitors are connected to the switches. A Windows 2000 workstation has been setup with APC's Enterprise manager is configured to alert administrators via email when power is lost, or if temperatures or moisture levels fall out of the desired range. It is also running GFI's LanGuard System Event Log Monitor (SELM) and is configured to alert administrators to suspicious activity in the Event Logs. GFI's LanGuard System Integrity Monitor (SIM) is used to monitor and alert administrators to changes in key system folders and files. Finally, SolarWind's Network Monitor is being used to monitor the server, switches and internet routers and send alerts when services are interrupted.

As you can see in the table above, the NSA's security templates will play a large role in helping secure the network as prescribed by the users and environment. These templates will be used to secure the Domain, Domain Controllers and Workstations. Password, Auditing, User Rights, Event Logs, System Services, Registry and File System permissions will be configured at both levels to ensure the highest level of security possible. For the purpose of this paper, I will focus on the internal security applied to Domain Controller of the Student network.

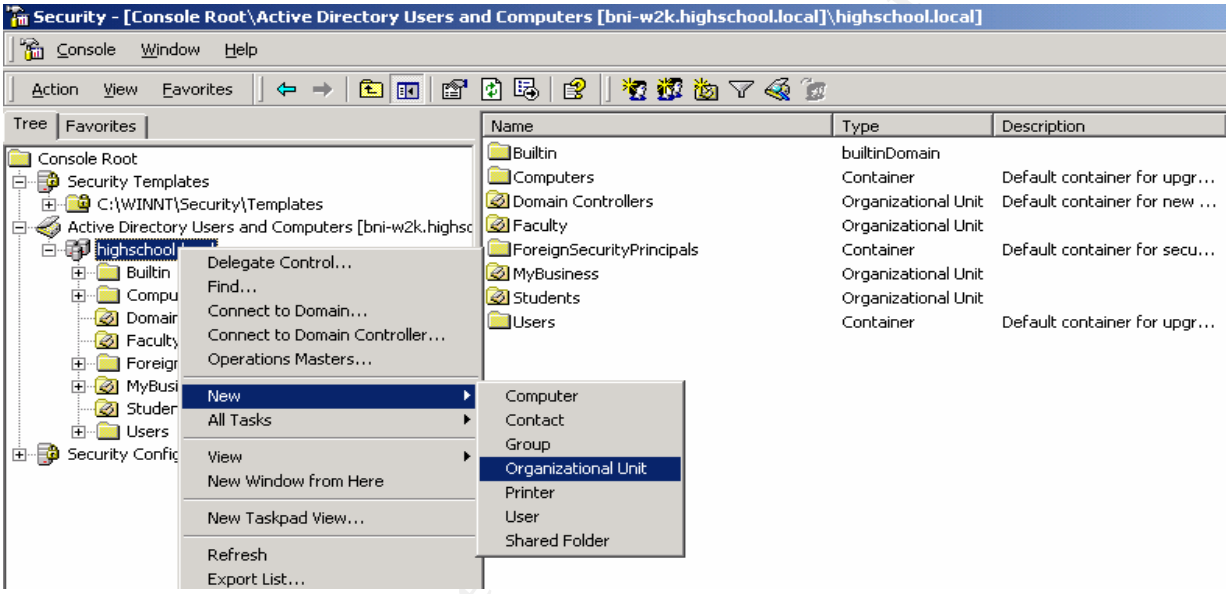
III. SECURITY SETTINGS:

Define the Active Directory Organization Structure

Group Policies using templates provided by the NSA will be used to secure the server and workstations. Since this server will also be the domain controller, the NSA's w2k_domain and w2k_DC templates will be applied. Microsoft's Default Domain Policy

will be left in place, but the local server policy will not be used. A new domain policy and domain controller policy will be configured and applied. Organizational Units will be created for Student and Faculty users and computer accounts. NT System Policies will be configured to provide security for the remaining Windows NT workstation and 9x clients. To create the organization's structure in Active Directory:

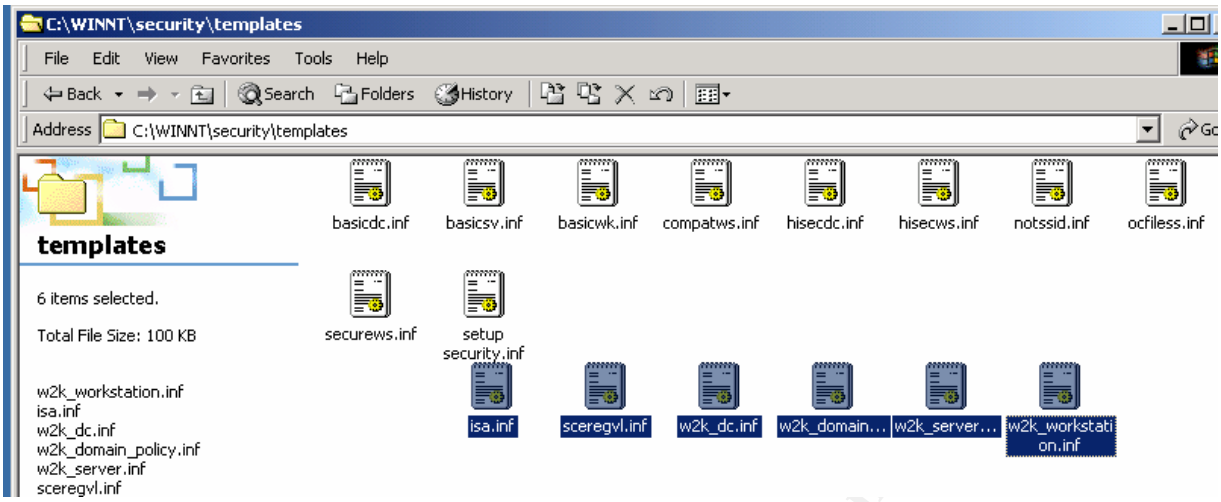
1) Click on **Start**, **Programs**, **Administrator Tools**, and click on **Active Directory Users and Computers**.
2) Right click on the domain name, select **New**, and select **Organizational Unit**.
3) Type **Students** and click **OK**.
4) Repeat step 2 and type **Faculty**.



Loading and Reviewing the Templates

The NSA's templates are available for download from their website http://www.nsa.gov/snac/index.html.

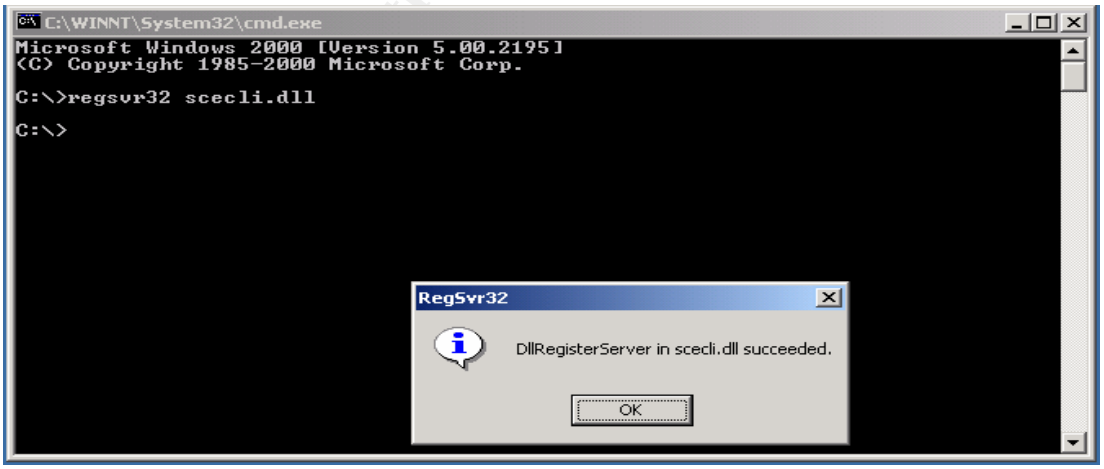
1. If you have a highspeed connection, download the Windows 2000 Guides "Zipped Archive" which contains the entire offering of templates.
2. Extract the files and place them in the %SystemRoot%\security\templates folder.

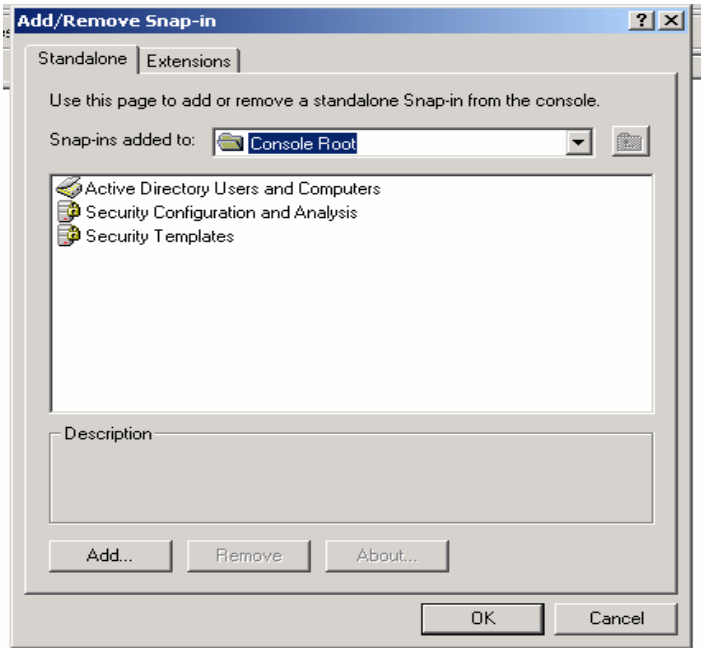


3. Make backup copies of the templates and leave the originals unmodified.
4. Review the "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set" and "Guide to Securing Microsoft Windows 2000 Group Policy". These excellent documents explain all the available security settings in the NSA templates and provide step by step directions on how to apply the templates using Group Policy.

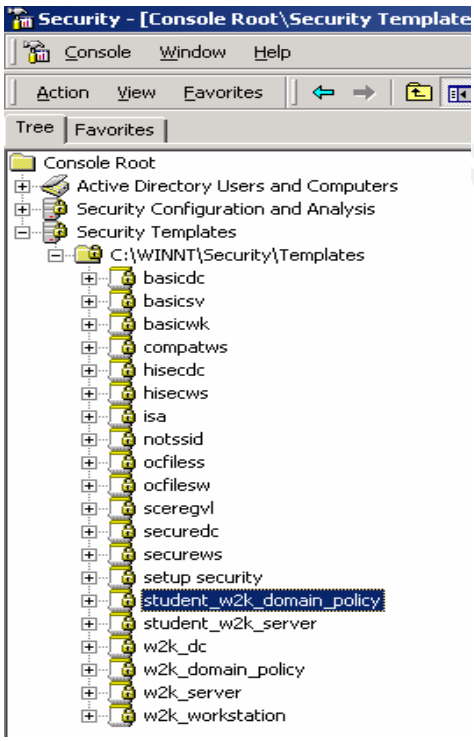
The templates provided by NSA include several new security options that are not available in Microsoft's templates. To access them you will need to:

5. In the %SystemRoot%\inf folder, rename sceregvl.inf to **sceregvl.old**
6. Copy the **sceregvl.inf** file you downloaded from the NSA to your %SystemRoot%\inf folder.
7. Click **Start**, **Run** and enter "**regsvr32 scecli.dll**" on the run line.





8. Then, open the MMC by clicking **Start**, **Run** and typing "**mmc**". Once the console loads, we will add the Security Template snap-ins.
9. Click on **Console**, **Add/Remove snap-ins**, then select **Add** to get a list of snap-ins.
10. Select **Security Templates**.
11. Select **Security Configuration and Analysis**.
12. Select **Active Directory Users and Computers**, and then close each open dialog. We will use these later when applying the Template to an Active Directory OU.



13. Once back in the MMC, click on "Secruity Templates" and the "C:\WINNT\Security\Templates" folder to get a list of the available templates.
14. Open the w2k domain policy.inf file by double-clicking the file name. Right Click on the template name, select **Save As** and give the template a new name (ex: "highschool_w2k_domain_policy.inf")
15. Do the same for the w2kDC.inf template and **Save As** "highschool_w2k_DC.inf".
16. Right Click on C:\WINNT\Security\Templates, and select **Refresh**. The new templates will appear in the list.

Now we are ready to begin reviewing and configuring the security options by opening each folder.

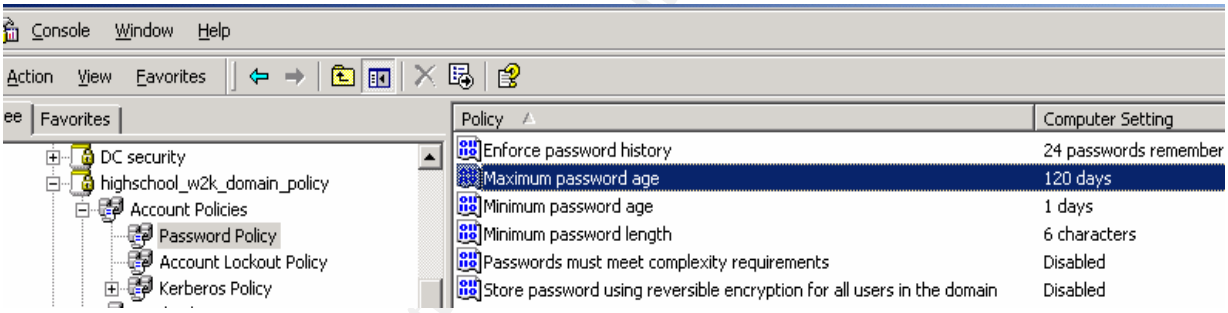
Account Policies

Account Policies are applied at the domain level only. These settings include password and lockout that will be applied to all servers in the domain using the "highschool_w2k_domain_policy. As a best practice, we will keep the settings for the domain controller in "highschool_w2k_dc.inf. Both templates will be applied to this server using the Domain Controllers Organizational Unit.

Password Policy

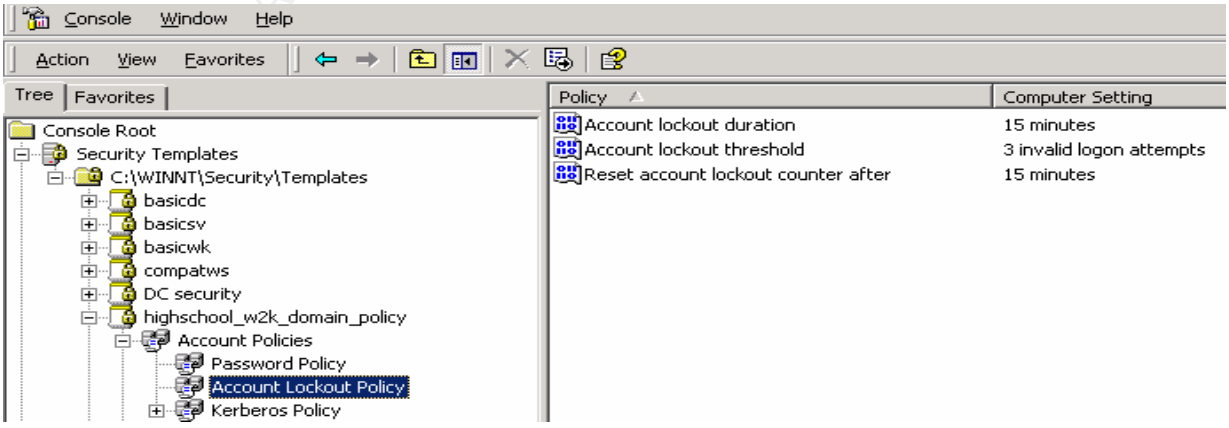
The domain based password settings chosen by the NSA do not suit the school environment where the year is divided in two semesters and children are the users. User names are based on the "Student ID" uniquely assigned by the administration to each student. The security template changes required are:

- "Maximum password age" will be extended to cover the length of a semester = 120 days.
- "Minimum password length" will be 6
- "Passwords must meet complexity requirements" will be disabled to reduce problems with students forgetting passwords.



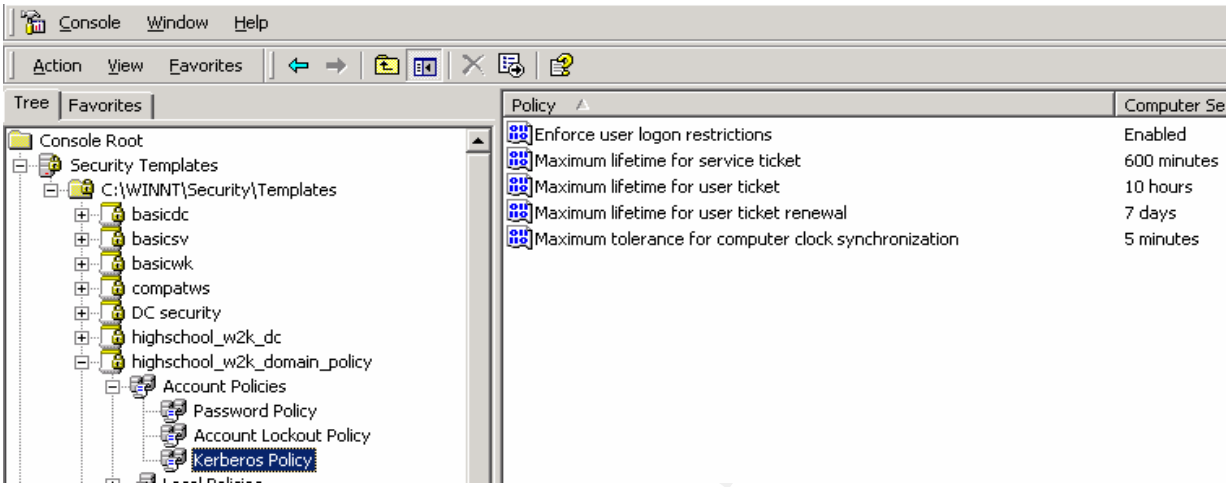
Lockout Policy

These policies are important in slowing down possible dictionary attacks. The NSA recommended settings will be used.



Kerberos Policy

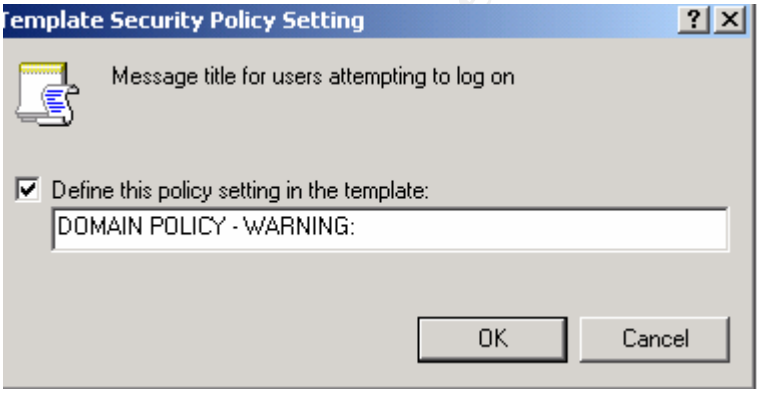
Kerberos policies only apply to domain controllers. The NSA recommended settings will be used.



Security Options

An additional setting will be made to help distinguish this policy from other over-lapping policies like the "highschool_w2k_dc policy". I will add a simple label to the logon text box to help distinguish which policy is in place.

- "Message text for users logging on" will be: **DOMAIN POLICY - WARNING:**



This concludes the configuration of the "highschool_domain_policy.inf" template. The rest of the settings will be configured in the "highschool_w2k_DC.inf" template.

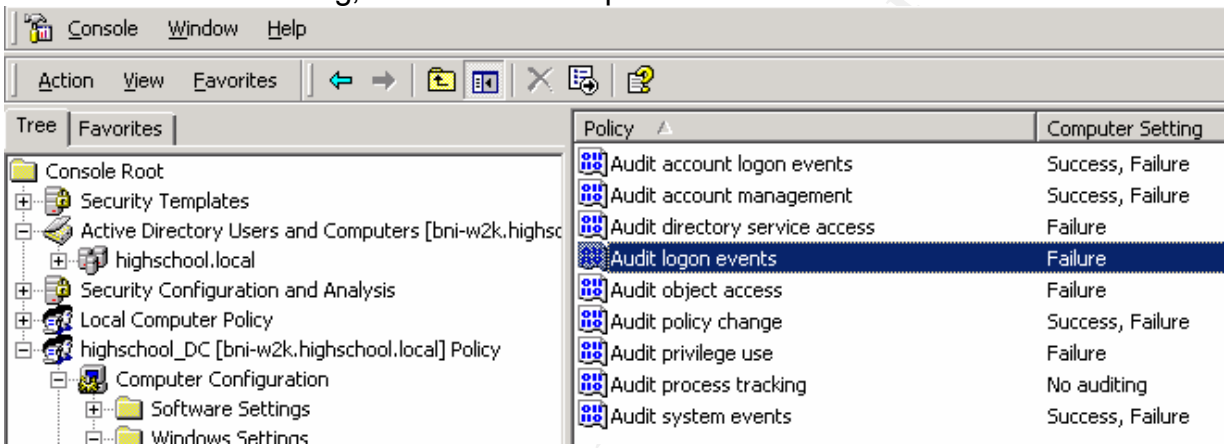
8. Right-click on the "highschool_w2k_domain_policy" and select **Save** to save the new settings.

Local Policies

Local Policies can be customized depending on the type of server or workstation. This server will be a file and print server, but it's also the domain controller. Therefore the NSA's w2k_dc policy will be used. Double-click to open the highschool_w2k_dc.inf to expand the available options and begin configuring the desired settings.

Audit Policy

Auditting is an extremely important tool to administrators for day to day maintenance of the domain, and when watching for evidence of hacking. By default, Windows 2000 does not enable auditing, but the NSA template makes extensive use of it.

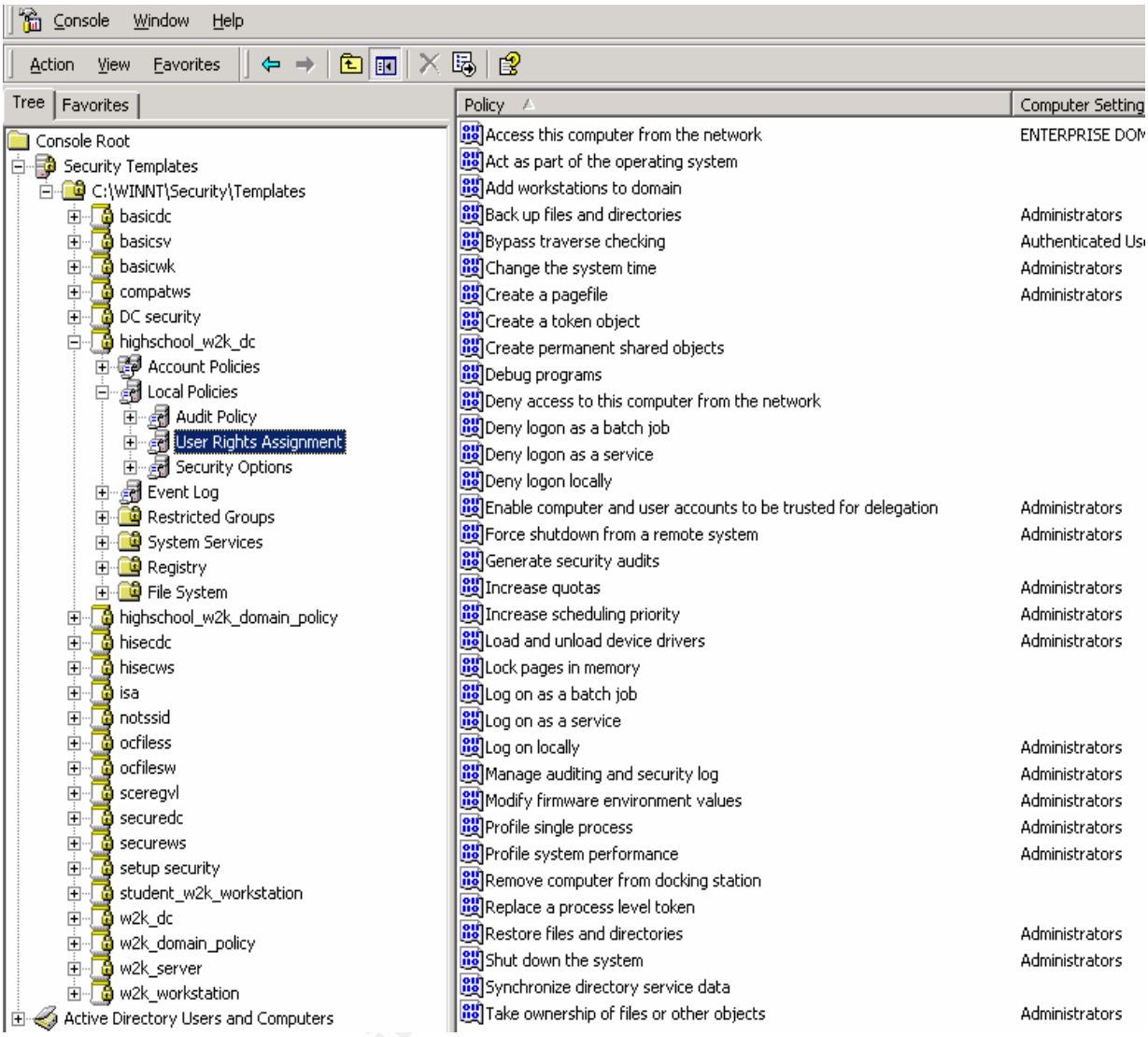


A few modifications will be made:

- "Audit logon events" will be changed to **Failures** only, due to the number of students and the frequency which they login and out of the network. There are about 300 students who access the network each hour following the class schedule of the day.
- "Audit directory service access" will be set to **Failure** to monitor failed access to Active Directory objects.
- "Audit object access" will be **Failure** only based on logon frequency and log size.

User Rights Assignment

Using this area of the template, you can provide or remove rights by user and or group name. The NSA's settings here are more than adequate to secure the domain servers in this organization. By using the "domain controller" template as opposed to the "member server" template, we gain the added security of the group Users being replaced by Authenticated Users.

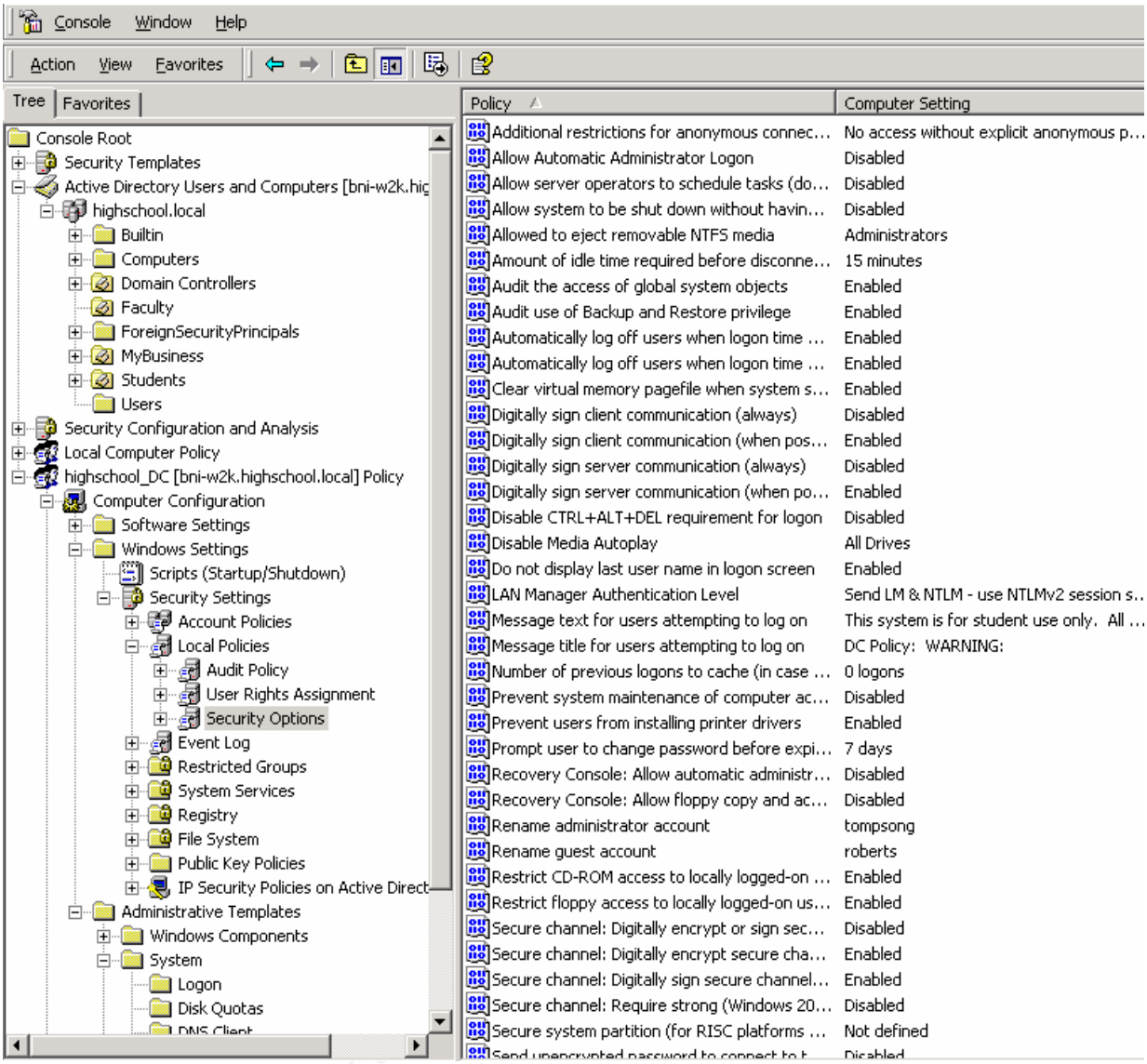


Security Options

Most of these settings will be used with the exception of the following changes:

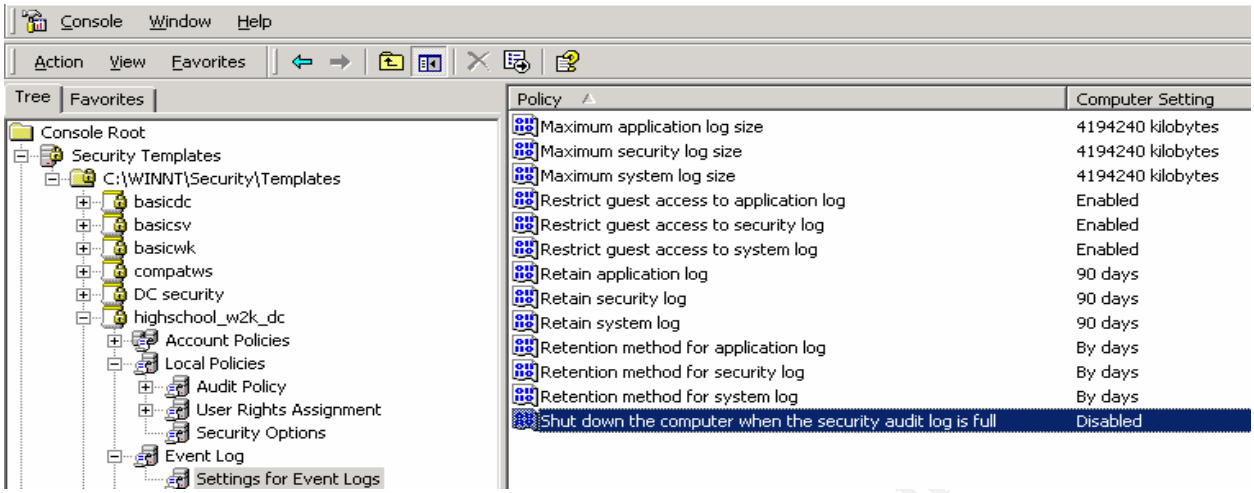
- "Amount of idle time required before disconnecting session" will be **15 minutes** to reduce the risk of a student gaining access to the file server.
- "Automatically log off users when logon time expires" will **Enabled** us to set time restrictions outside of normal school hours (7am – 6pm).
- "LAN Manager Authentication Level" will be set to **Send LM & NTLM – use NTLMv2 sessions security if negotiated**. This is required to allow the remaining Windows 9x PCs access to the network. We could install the Active Directory Client on these PCs, but they will be retired this year. Then the setting will be returned to the NSA default to achieve a higher level of security.

- "Message Title for users attempting to log on" will be: **DC POLICY WARNING:** This computer is being monitored. (The purpose of labeling the text box this way is to allow verification after the policy is applied later in this document.)
- "Message text for users logging on" will include a warning and information to make sure the user knows they are accessing a secured systeme that is being monitored. It will refer to the Student PC Policy in the Student Handbook that each student must read and sign at the beginning of the year before being assigned an account.
- "Rename the Administrator account" is **Enabled**. It will be set to "tompsong" to make if more difficult for hackers to identify the account (user names are based on the users last name and first initial). Then, we will create a "fake" administrator account with a highly secure password and then disable the account.
- "Rename the guest account" is **Enabled** and will be "robertsm" for the same reasons as above, and then disable it.
- "Shut down system immediately if unable to log security audits" is **Disabled** to minimize the risk that the logs overflow during a holiday or time when the teacher administrators are not on campus. Since the school year follows such a unique holiday schedule, this option will not be used.



Settings for Event Logs

The NSA provides for a lot of space to hold logs, making it easier for administrators who may need to look back over several weeks of time to see a pattern of abuse or probing. We will only change the following settings:



- "Retain application log, security log and system log" will be set to **90 days** and
- "Retention method for application log, security log and system log" will be changed to **By days**. Again, due the the erratic nature of the school schedule, there is not always an administrator on campus. If logs fill up while a teacher is on Spring Break, and the server automatically shuts down, it would interupt network availability unnecessarily. In order to make sure the logs aren't overflowing with attacks and going unnoticed, we will use LanGuard's System Event Log Monitor (SELM). SELM will be configured to alert administrators of suspicious activity via pagers and email.
- "Shut down the computer when the security audit log is full" will be **Disabled** for the same reason as above.

Restricted Groups

The NSA template doesn't define any restricted groups, but we will add for Administrator and Faculty. The Administrators group will be limited to two teachers and one computer consultant. Since the Faculty group has access to sensitive information on the Student network, and will be using PCs in classrooms where students are, this will add an extra level of security.

- Administrator group = local administrator and Domain Admins and Enterprise Admins Global groups, two teachers and consultant.
- Faculty group = all teachers and staff who logon to the Student network.

System Services

The NSA templates don't attempt to define which services a system might need. That's because depending on the type of server, web, file and print, terminal server, etc., it would be impossible to predict! By default, Windows 2000 loads many services automatically that may or may not be needed. Some services are set to manual, which means they are accessible if called by an application. Some of these services could

present a serious security risk to the server and the organization. Therefore, we will lockdown and use only the services required, without inhibiting the proper functionality of the server. Some services will be left at Manual, so they can still be started if need by the Operating System.

Below is a table[7] of services I downloaded from Tech Republic, which defines their roles and and reasons/drawbacks for enable/disabling them. It provides a good starting place for deciding which services to enable or disable and why. I have taken this table and updated it to include the specific settings for this environment.

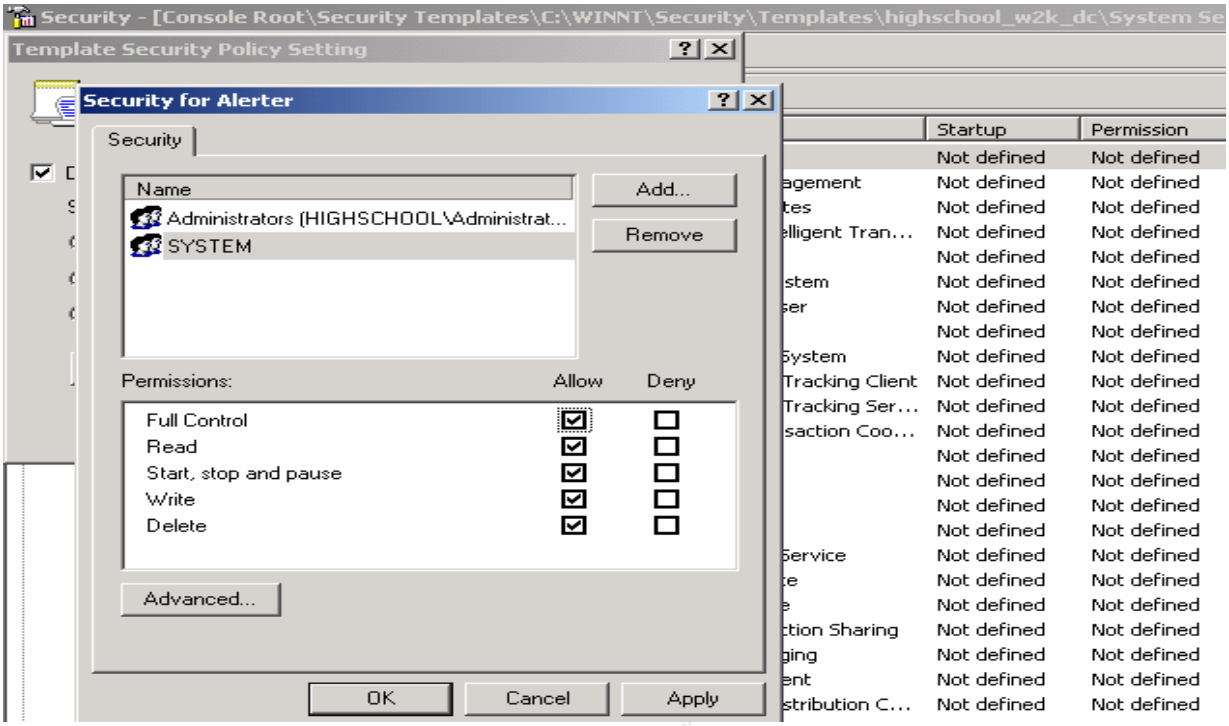
Service	Description	Startup	Reason
Alerter	Is used to display "pop-up" messages on administrative alerts. This service is not needed.	Disable	Administrators will have to carefully watch Event logs for messages. LanGuard's SELM will be configured to do this via email.
Automatic Updates	An Administrator can configure the server to obtain updates from Microsoft automatically via an internet connect.	Disable	This service is disabled because we want to review all updates and patches before appying them. We will be using LanGuard's Network Scanner to do this.
DHCP Client	Allows the system to automatically obtain IP addressing information, WINS server information, routing information, etc., and is required to update records in Dynamic DNS	Disable	This service starts automatically, but the server will be configured with a static address.
Fax service	Provides centralized fax services to network clients.	Disable	Will not be needed.
IIS Admin	Enables administration of an Internet Information Services Web server	Disable	This service starts automatically but is not needed. We will not need to administer Web, FTP, or other Internet services.
Internet Connection Sharing	Allows the server to act as a ??? to share an internet connection	Disable	The Cisco routers and switches will be configured with routing tables and access lists to provide the appropriate internet access to students and faculty.
Messanger	Allows users to send broadcast messages over the network to other users.	Disable	Due to the vulnerabilites of this service being used for DOS attacks, and to keep students from misusing it via the NBSTAT utility, this service will be disabled.
NetMeeting Remote Desktop Sharing	Used to allow colaboration and remote control of the desktop.	Disable	NetSchool is used for sharing and remote controll.
Network News Transport Protocol (NNTP)	Used for provideding news group services.	Disable	Will not be needed.
NT LM Security Support Provider	Allows clients to log on using NT LAN Manager (NTLM) authentication	Automatic	Will allow Windows NT and 9x clients to log in to the network.
Remote Access Auto Connection Manager	Allows for a dial-up connection to be established if remote network connections are down.	Disable	Will not be needed.
Remote Registry Service	Provides a mechanism to remotely manage the system registry	Manual	This opens systems to possible vulnerabilities, but is required by LanGuard and other 3rd party vendors monitoring tools. Disabling it can affect their operation. Setting it to Manual will allow the System to start it as needed.

[7] Allen V. Rouse "Design and document a Win2K Infrastructure." Tech Republic April9, 2003

Routing and Remote Access	Allows the server to route trafic to other networks.	Disable	Will not be needed.
Simple Mail Transport Protocol (SMTP)	Transfers email messages.	Disable	Will not be needed.
Smart Card	Support for Smart Card technology	Disable	Will not be needed.
Smart Card Helper	Help.	Disable	Will not be needed.
Telephony	Used to provide voice over IP services and telephony API.	Disable	Will not be needed.
Telnet	Allows remote access to the server.	Disable	Numerous vulnerabilites and the fact that Telnet uses clear text transmissions, this service is not desired.
Terminal Services	Allows for administrative remote contoll of the server, or access to applications on the server depending on how it is configured.	Disable	The server is in the administrators office and in close proximity to teaching labs. Remote access from outside the school is not available due to the firewall service run by the school district.
Windows Time (or W32Time)	Uses NTP to keep computers in the domain synchronized; critical for Kerberos authentication to consistently function	Automatic	The navy's time clock ntp2.usno.navy.mil will be used to provide accurate time to the server.
Windows Internet Name Service (WINS)	Provides NetBIOS naming services; required for networks with clients running versions of Windows prior to Windows 2000	Automatic	Will be used by Windows NT and 9x clients to obtain domain information and use domain resources.
World Wide Web Publishing Service	Ability to run web services.	Disable	There are too many risks and no benefit at this point to running a web server on the domain controller. When added, it will run on a stand alone server.

Security must also be set on the services so that users can't change the desired settings. This is accomplished by by adding the desired users or groups and assigning the appropriate security to each. To change the permissions on services do the following:

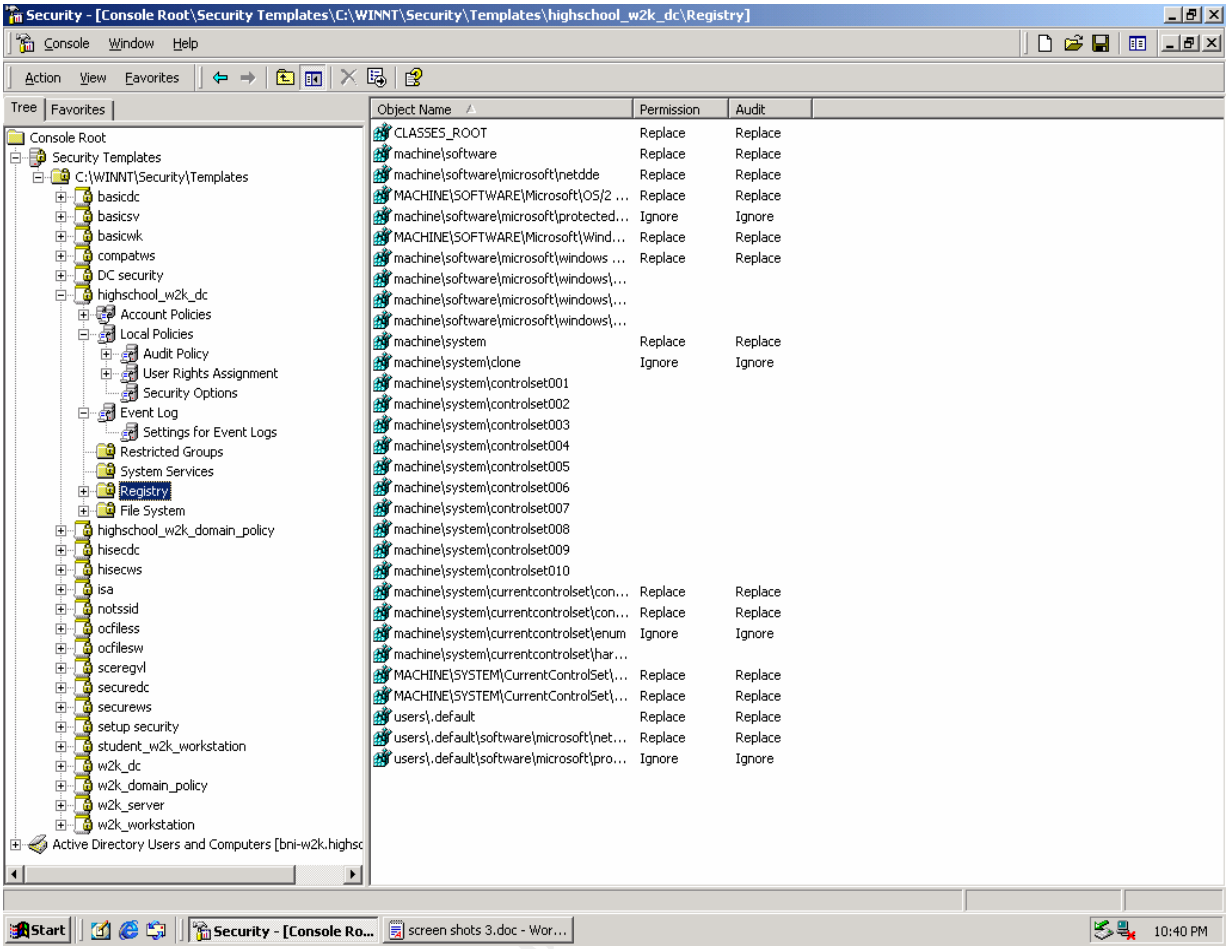
1. Double-click System Services in the "highschool_w2k_dc_policy.inf".
2. Double-click on the service you want to change.
3. Click the check box to define the policy setting – **Automatic, Manual or Disable**.
4. Click on the **Edit** Security box to display the Security tab that contains the names of the users and group who will be allowed access to this service.
5. We will **remove** the group **Everyone** and **add Administrators and System** with **Full Contol**. No other permissions will be necessary.



6. Click on **OK** and **OK** again to close.
7. Continue configuring the settings for all services, not just the ones the ones that are disabled.

Registry Settings

The NSA's settings for domain controllers are appropriate for this server in this environment. The default settings will be used.



File System Permissions

Since the only people who will be logging on locally are administrators, the NSA File System settings are suitable to this environment. If this server was being used as a Terminal Server, we would implement much tighter file security. Security is limited to Administrators and System, which get Full Control Permissions over the following folders:

- %Program Files%
- %System Directory%
- %System Drive%
- %System Root%

8. In the MMC, right-click on each new template, then select **Save**.

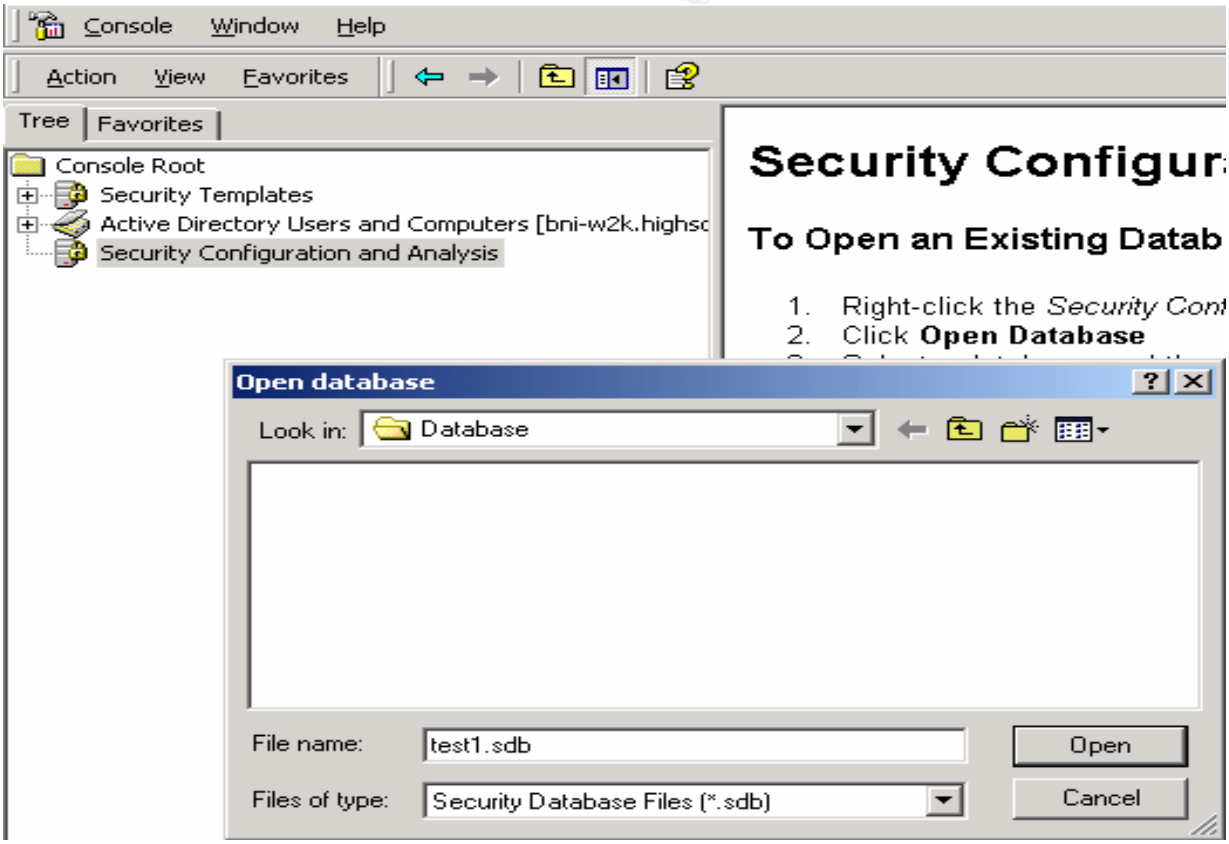
IV. APPLY, TEST AND EVALUATE:

Verify Using the System Configuration and Analysis Tool

You can use this tool to test the affect of the policies on a server before and after applying the templates. It allows you to load a single template, or multiple templates to get a "composite" template for analysis. In our case that would be the highschool_w2k_domain_controller.inf and the highschool_w2k_dc.inf templates.

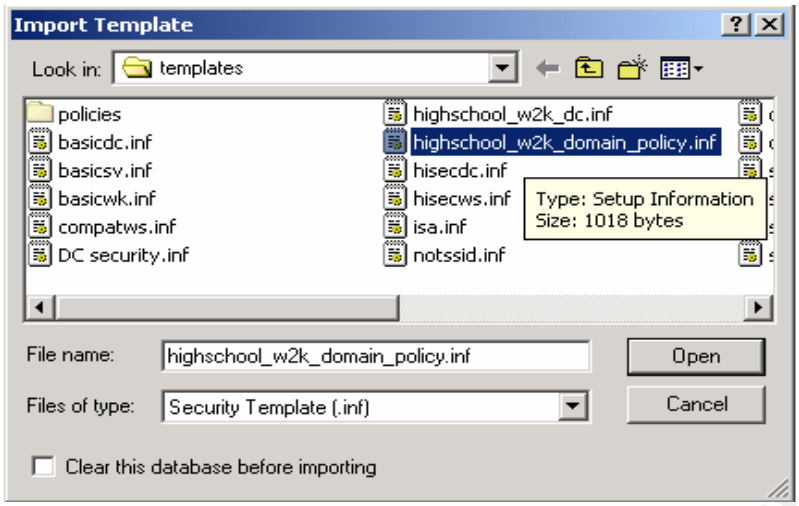
Before the templates are actually applied, or as you modify the templates, the configuration tool will show "Investigate", "Inconsistencies" and red X's on policy settings that don't match the local computer. We will use this tool to analyze how the settings compare to the existing computer settings and verify their settings. Now, we'll load the highschool_w2k_domain_policy.inf template into a database and verify the settings.

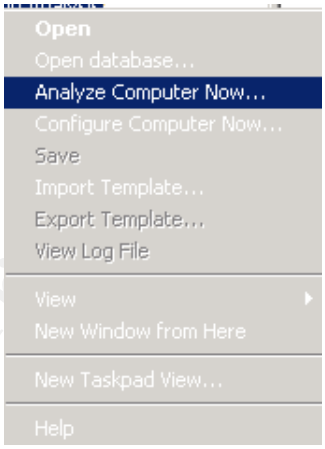
1) Right-click on "System Configuration and Analysis", and choose **Open database**.
2) Create a **Test1.sdb** to save the settings of the template we want to test.



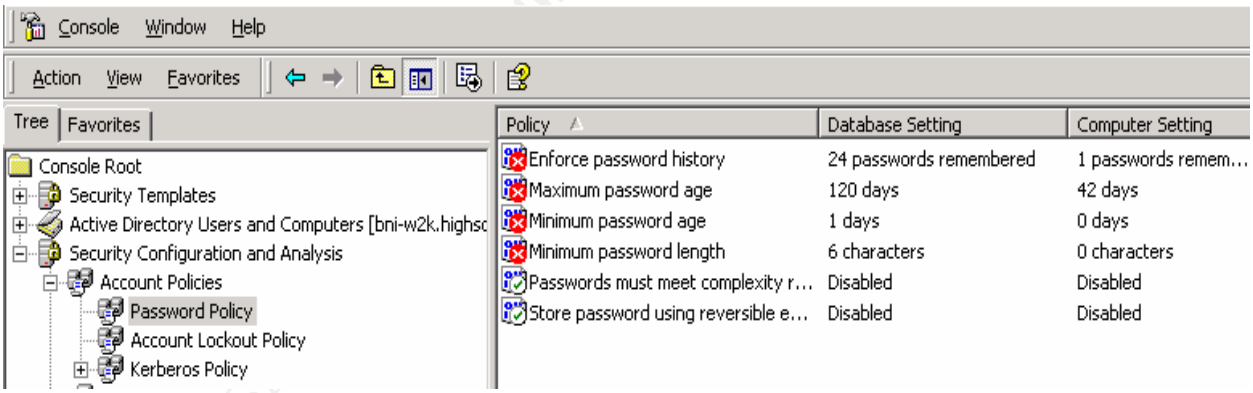
3) Select the "highschool_w2k_domain_policy.inf" file, and click **Open**.

(NOTE: We will NOT click the “Clear this database before importing” selection because we are going to load multiple templates to see their combined affect.)





4) Right-click on “System Configuration and Analysis” again, and select **Analyze Computer Now**.
5) Click **OK** to select the default log file path.
6) Verify that the Password, Account Lockout and Kerberos Policies are set as expected. In this case, we want to make sure the Database Setting is correct. After we apply the policy, the Computer Setting should match it.

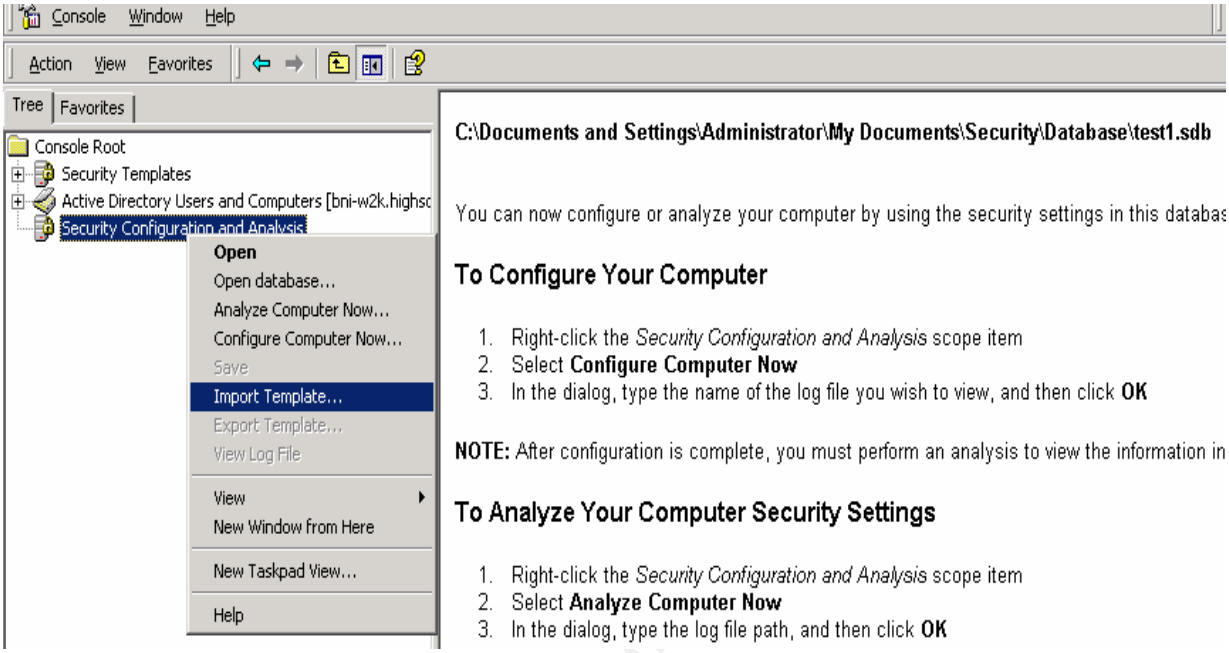


7) Make any corrections or updates needed to the appropriate template in the MMC under C:\WINNT\Security\Templates.
8) Right-click and **Save**.

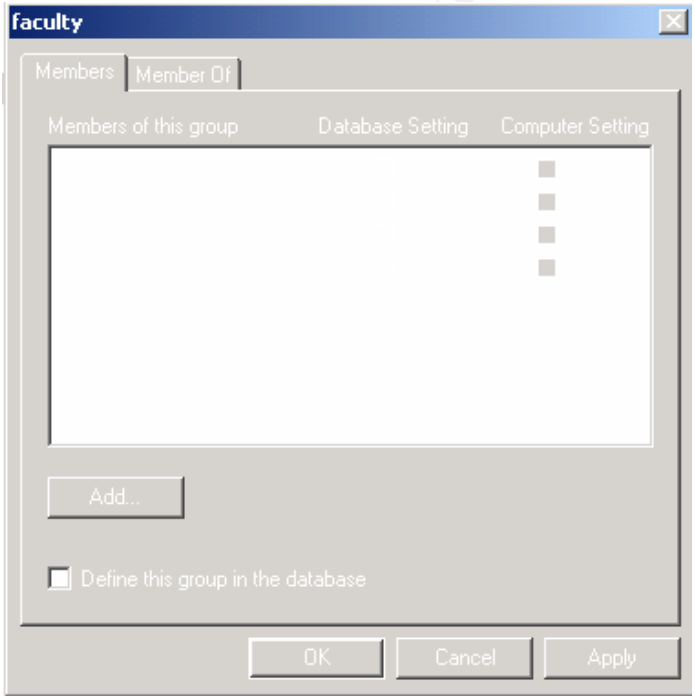
Next, we’ll add the highschool_w2k_dc.inf template to the same database and verify those settings. This gives us a “layered affect” and we can see how both policies will affect the server.

9) Right-click on “System Configuration and Analysis” in the MMC, and choose **Open database**.

10)Select the same **Test1.sdb** file, and click **Open**.
11)Right-click on “System Configuration and Analysis” and select **Import Template**. Choose “highschool_w2k_dc.inf” and click **Open**.

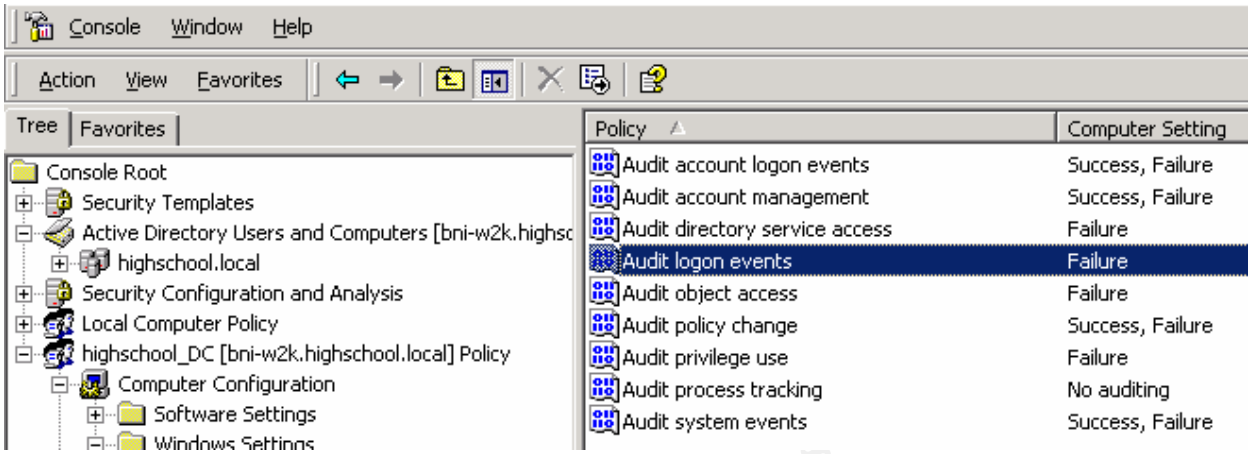


12)Right-click on “System Configuration and Analysis” again, and select **Analyze Computer Now**.
13)Click **OK** to select the default log file path.
14)Review the settings for Local Policies, Event Log, Restricted Group, System Services, Registry and File System Policies are set as expected.



15) Make any corrections or updates needed to the appropriate template in the MMC under C:\WINNT\Security\Templates.
16) Right-click and **Save**.

Applying the Templates using Group Policy

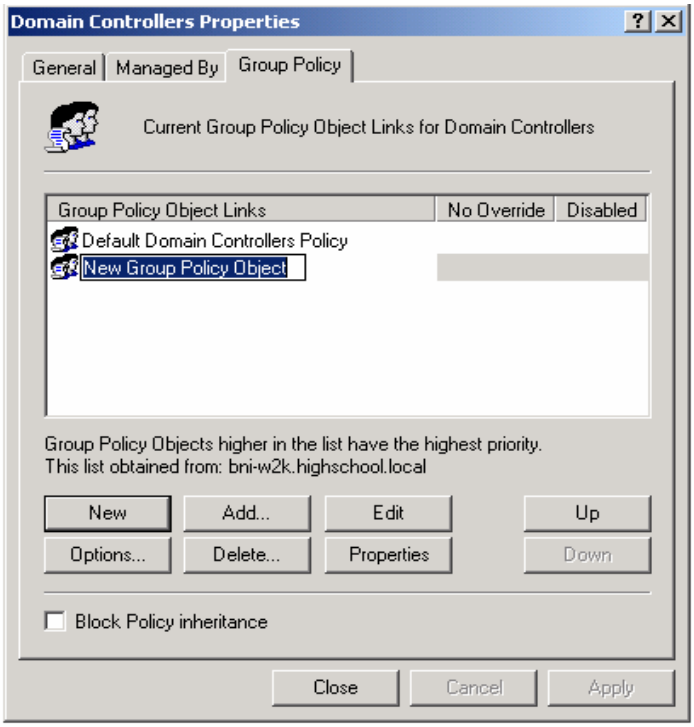


Now, the templates can be applied to the server. There are several methods we could use to accomplish this.

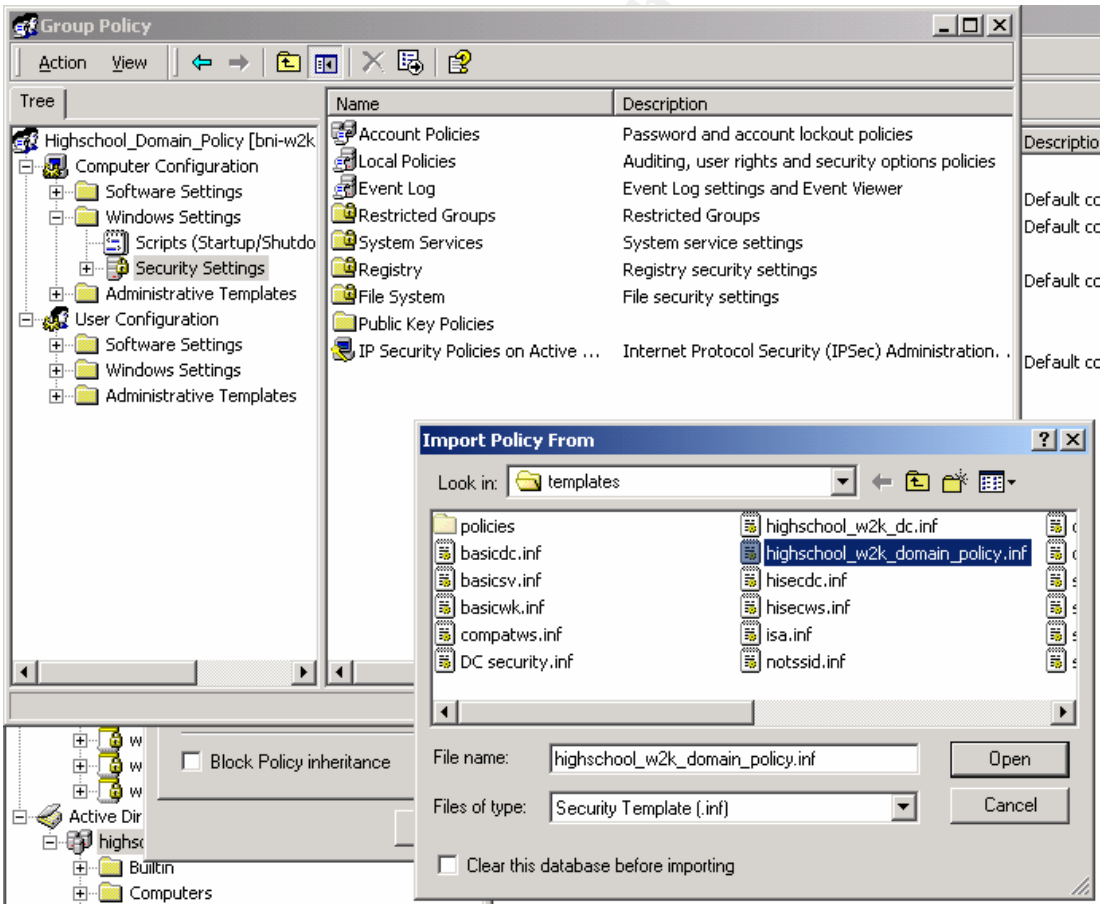
- use the System Configuration and Analysis tool – **Configure Computer Now…**
- import the new security settings into the **Local Policy** on the server
- use **SECEDIT** to apply the templates from the command line
- create a **Group Policy Object** (GPO), associated with an Active Directory OU, and import the template

This is the first domain controller, and other servers will be added to the network over time. Creating OU's and assigning Group Policies is an efficient way to manage these settings. Using Group Policy, we can easily modify the templates and control how often they are refreshed using the Administrative templates settings for "Refresh interval for Group Policy". We can also use Group Policy to set many other helpful settings to lock down and secure the server, such as: Software Installation, Internet Explorer Maintenance, Scripts and Folder Redirection.

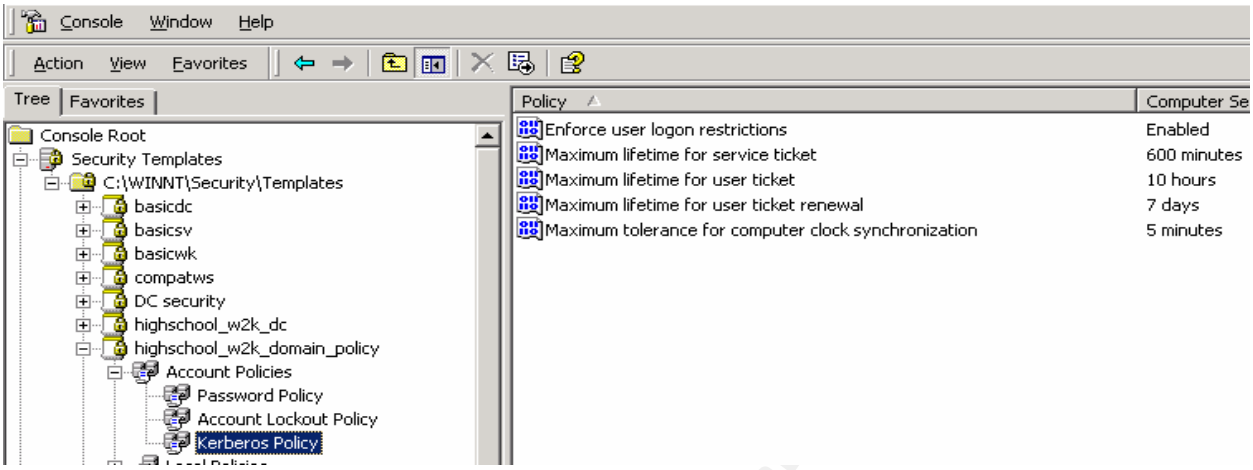
1. Double-click on "Active Directory Users and Computers", then double-click **highschool.local** to open the Domain.
2. Right-click on "Domain Controllers", select **Properties**, then select the **Group Policy** tab. (Notice that a Default Domain Controllers Policy has automatically been applied by Windows 2000 when this server was made a DC. We will leave this policy in place, unmodified, in case we want to rollback the new policies.)
3. Click **New** to create a new group policy object.



4. Give the new policy the name "Highschool_Domain_Policy".
5. Click the **Up** button to move the new policy to the top of the list, over the "Default" policy, and click **Apply**.
6. Click **Edit** to open the new GPO. Then double-click on "Computer Configuration", then "Windows Settings".
7. Right-click on "Security Settings", select **Import**, select "highschool_w2k_domain_policy.inf"



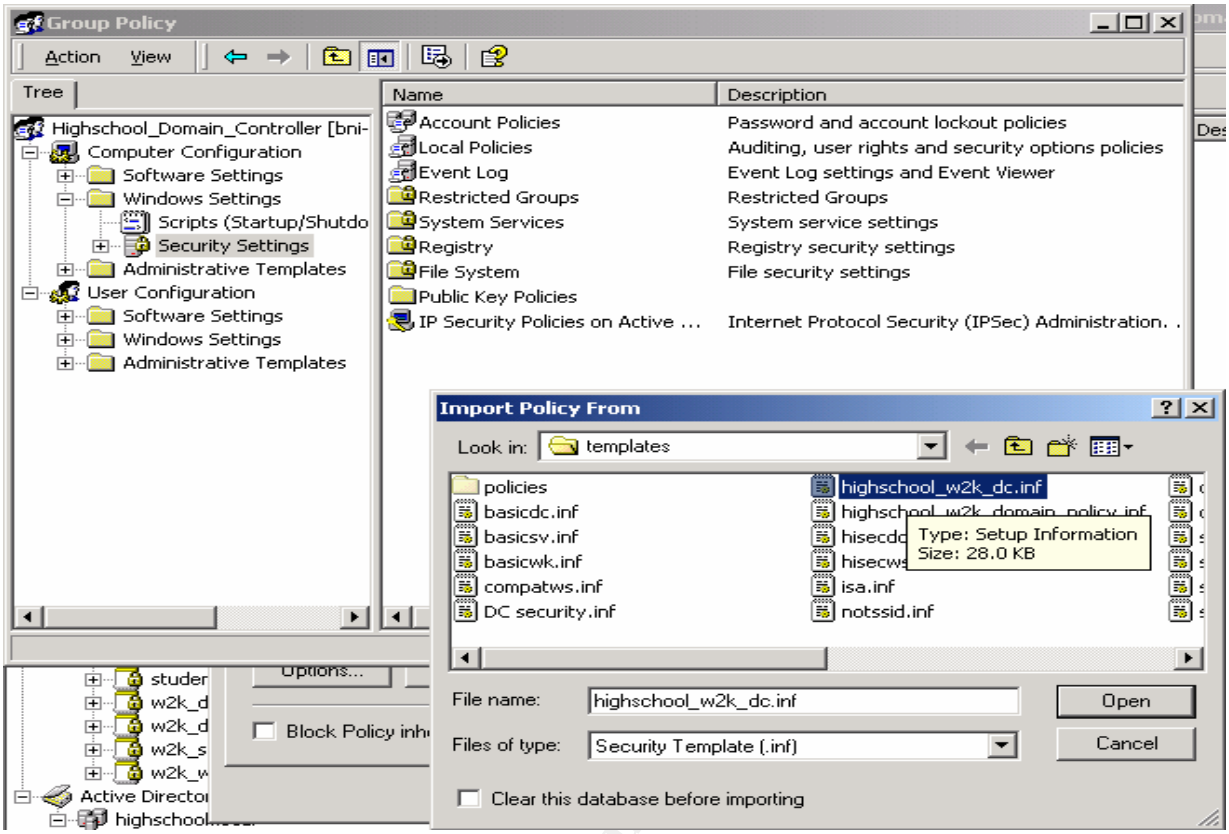
8. Open the “Account Policies” and verify that the “Password Policy”, “Account Lockout Policy”, and “Kerberos Policy” settings have been imported. The Database Setting should now match the Computer Setting.



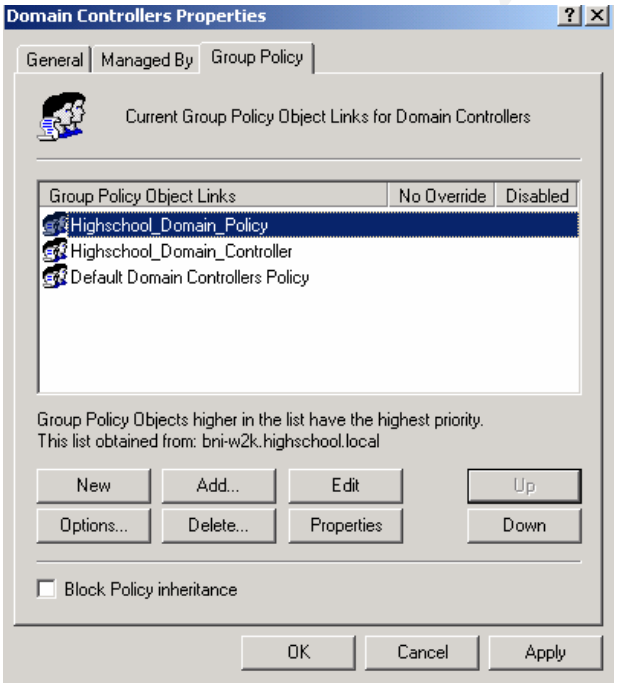
9. Click the **X** at the top right corner of the window to close the Policy.

Repeat these steps and create a new Group Policy for the domain controller settings:

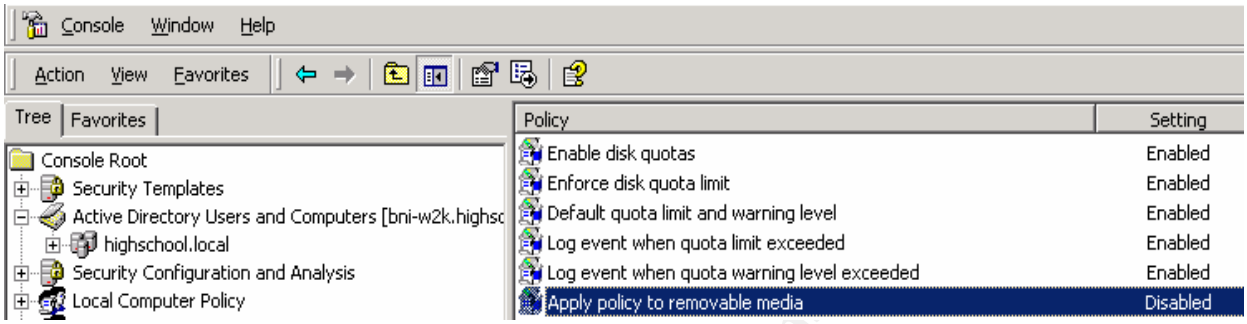
10. Click **New** to create a new group policy object.
11. Give the new policy the name “Highschool_Domain_Controller_Policy”.
12. Click **Edit** to open the new GPO. Then double-click on “Computer Configuration”, then “Windows Settings”.
13. Right-click on “Security Settings”, select **Import,** select “highschool_w2k_dc.inf”.



14. Click the **Up** button to move the new policy to the top of the list and click **Apply**. Make sure the Policies are in this order: Domain Policy, Domain Controller Policy, Default Policy.



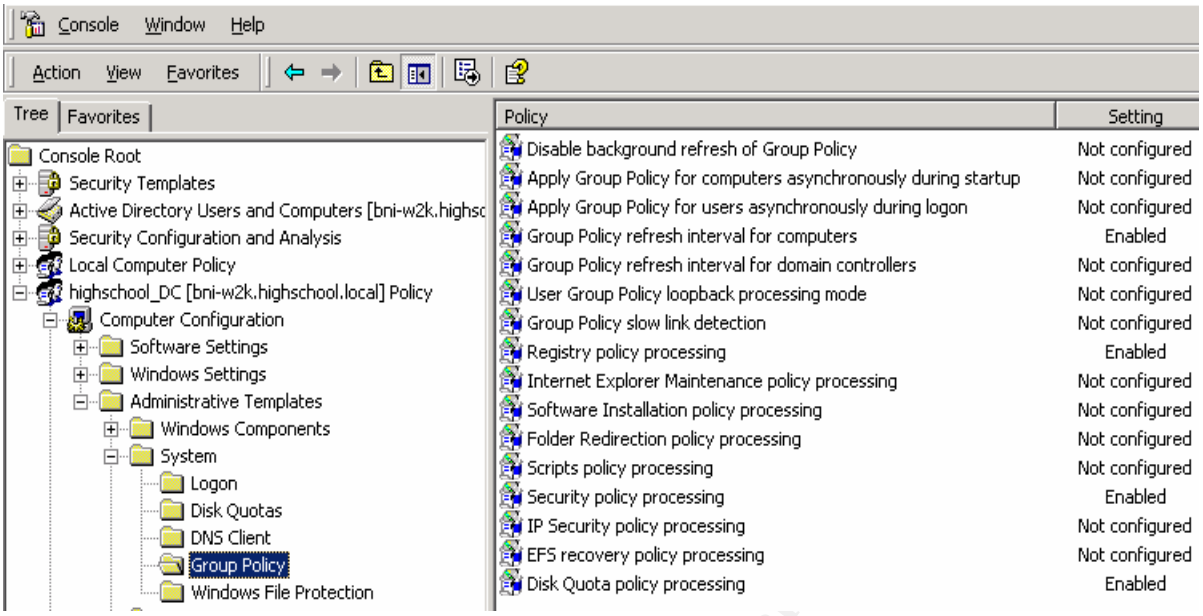
15. Click the **X** to close the Group Policy window, and **OK** to close the Domain Controllers Porperties.
16. To force the the new GPOs to apply and see their affect on the server, **re-boot**.
17. Disk Quotas will be added under the Computer Configuration, Administrative Templates, System, Disk Quotas settings as defined in the Security Goals of the school.



Maintaining the Policies

After applying the policies, they will be refreshed each time a the server is rebooted, or they can be forced to refresh by using the SECEDIT command. There are also settings in the Administrative Templates for maintaining and refreshing policies for both the domain controllers and workstations. We will use the following options to ensure the policies are up to date, without causing too much traffic on the network.

- Domain controllers will refresh policies by default every 5 minutes. This will be adequate for our environment.
- Computers on the network refresh policies by default every 30 minutes. We will raise that to 90 minutes, with 30 minute random intervals. This will help reduce network traffic.



Testing

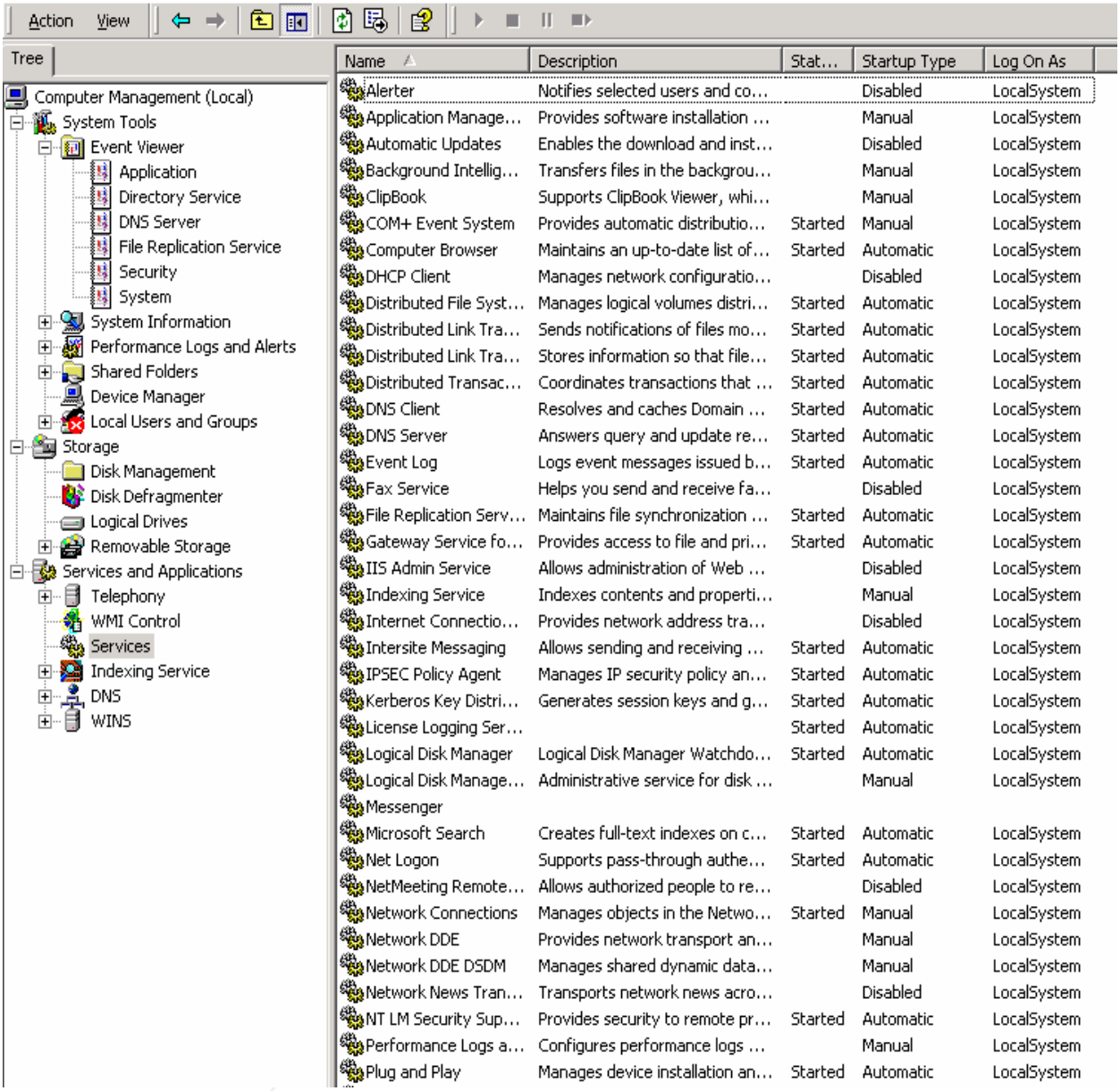
Test Security Settings

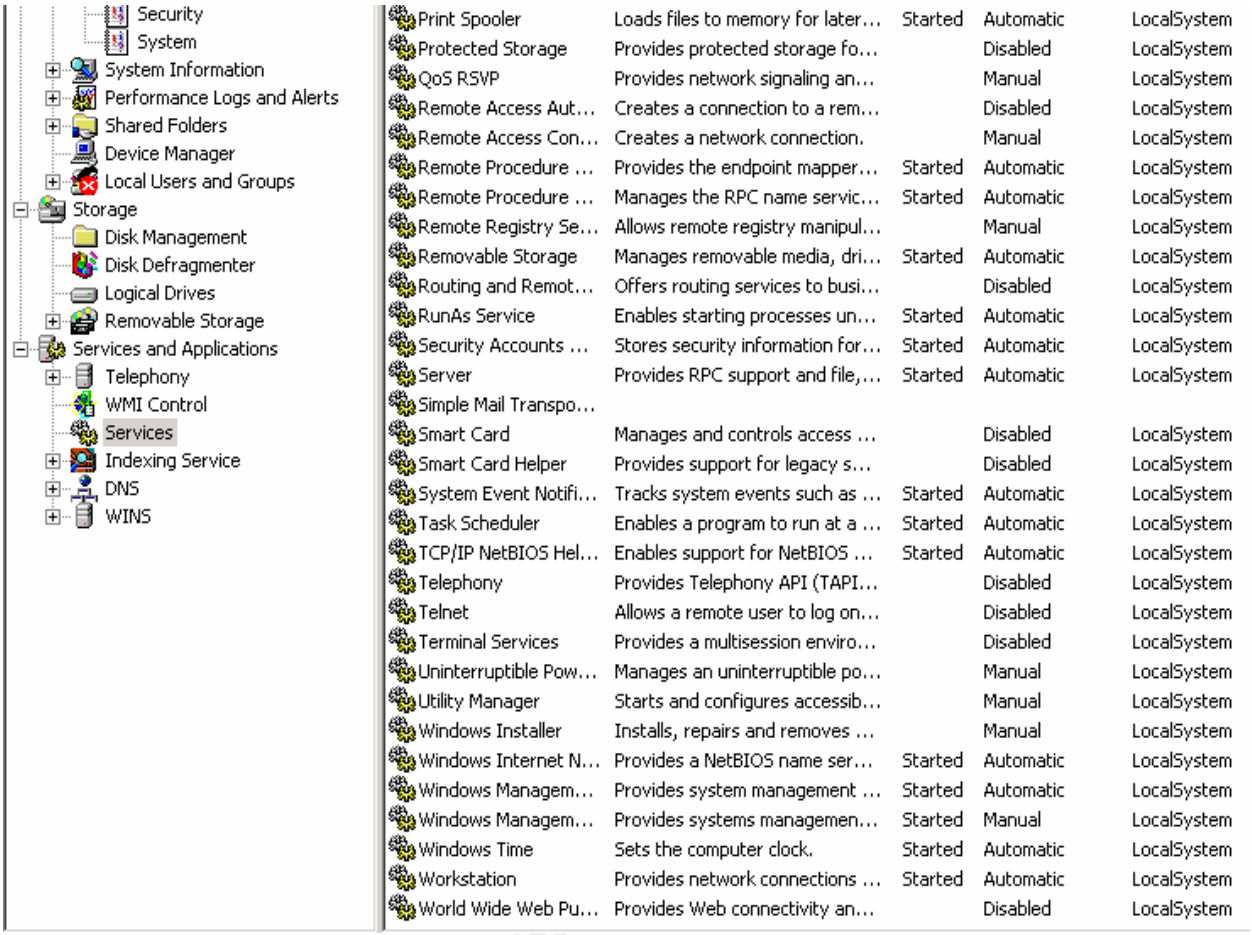
1. Verify and test that the security settings have been applied successfully. The first sign of this is after re-booting the server. When you press **Ctrl-Alt-Del** to logon, you see the logon banner which was set via the Security Options in the "Highschool_Domian_Policy".

We can tell this because the Message Title contains "**Domain Policy - WARNING:**". If the "Highschool_DC_Policy" were taking precedent, the Message Title would say "Domain DC – WARNING:". Note that the proper message based on the order in which the policies were applied shows the Domain policy text title.

(I was unable to capture picture!)

2. Disabled services were listed below. Checking the Administrative Tools, Services shows that the proper services were started automatically, or disabled.

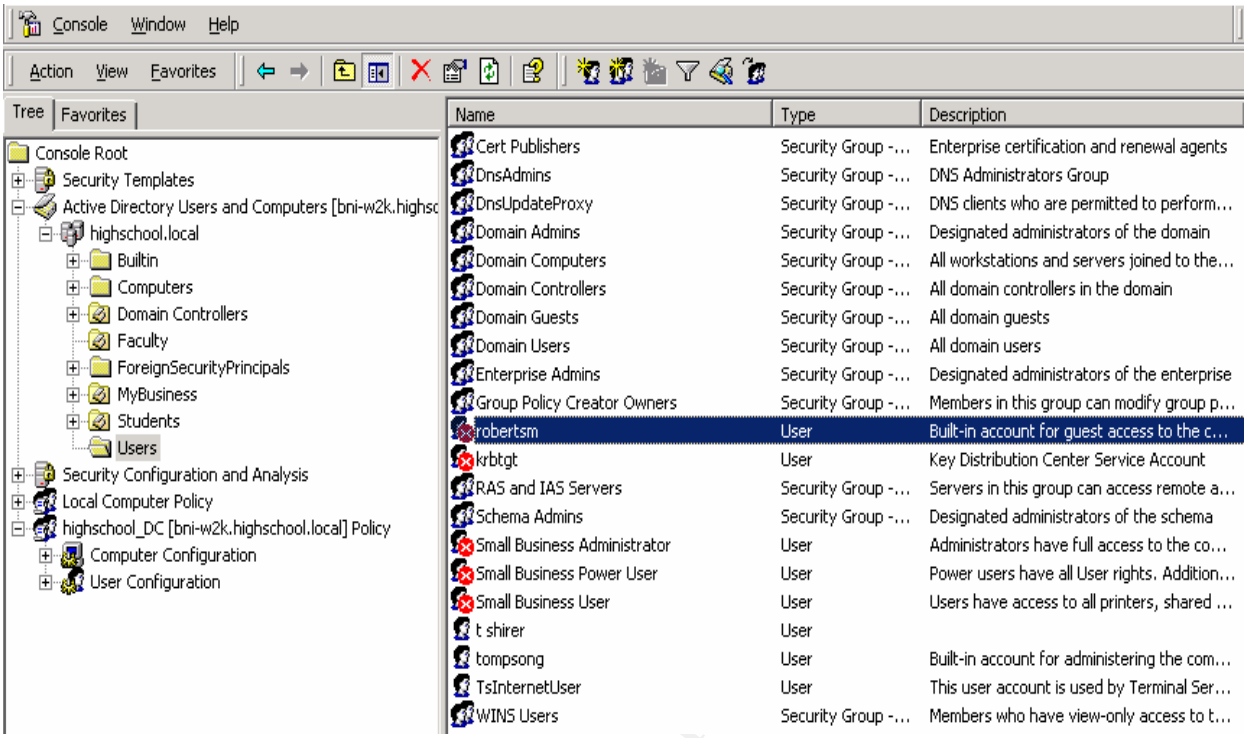




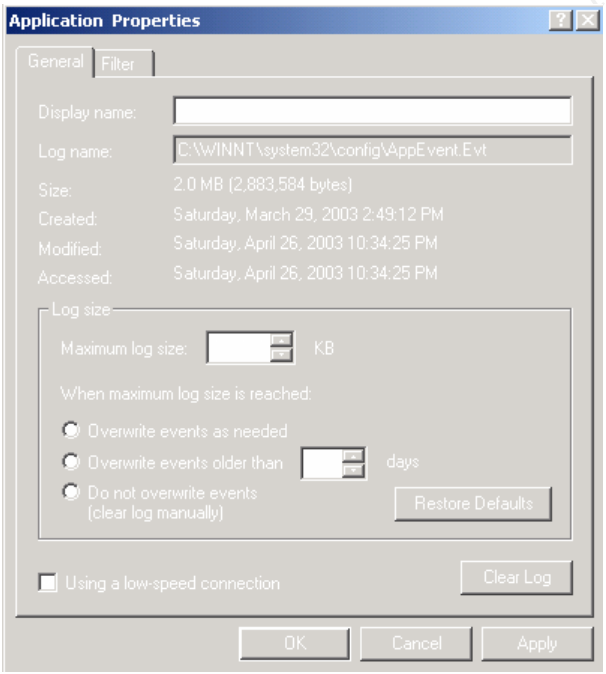
3. Now, we will try to logon to the server as a Student or Faculty member to show that the "Logon Locally" right has been revoked.

The error message "**The local policy of this system does not permit you to Logon interactively**" appears.

4. The administrator account was renamed. Checking in Active Directory Users and Computers, in the Users folder, we see that it is now "**tompsong**" as configured. The Guest account has been renamed as "**robertsm**" and disabled. I was able to logon as "tompsong" and had full administrative privileges. I was unable to logon as "robertsm", receiving the message "**Your account has been disabled. Please see your system administrator**."

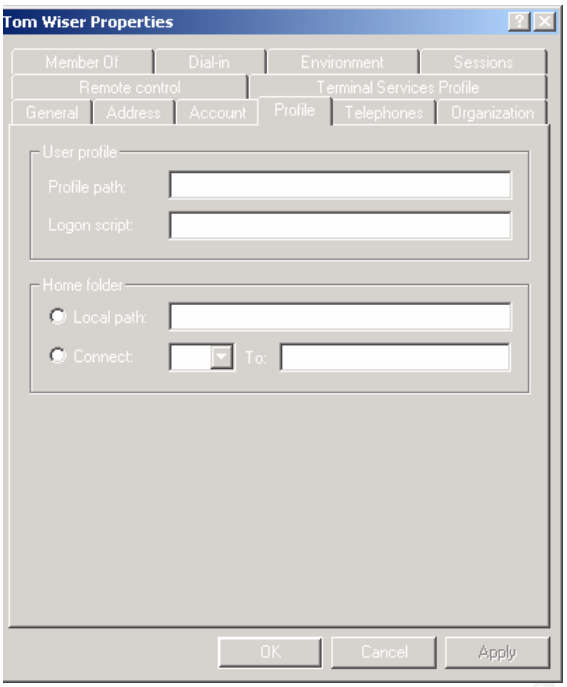


5. I verified that the Event log settings were correct.

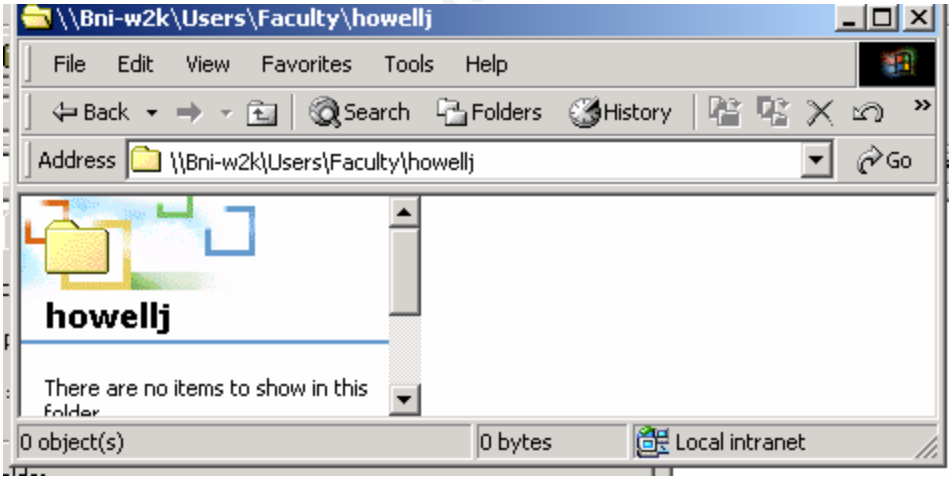


Test System Functionality

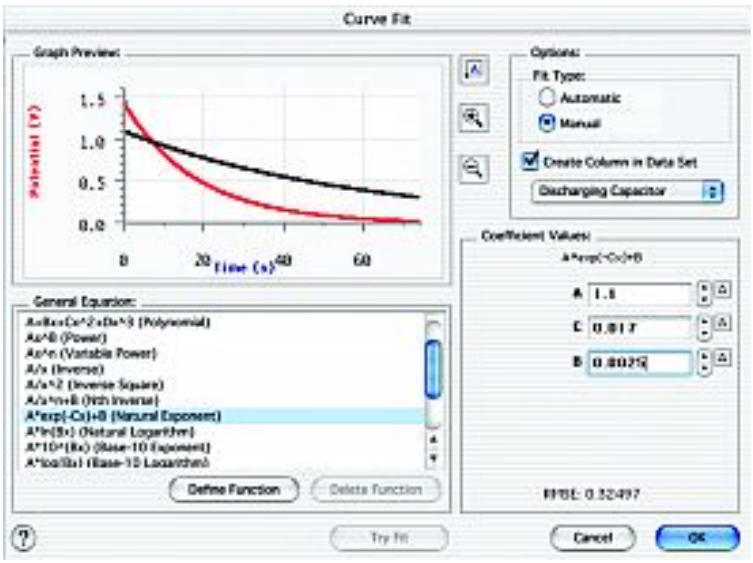
1. I tested the ability of Students and Faculty to logon to the server and access their personal secured folder, which was configured on the Profile tab of their User Properties.



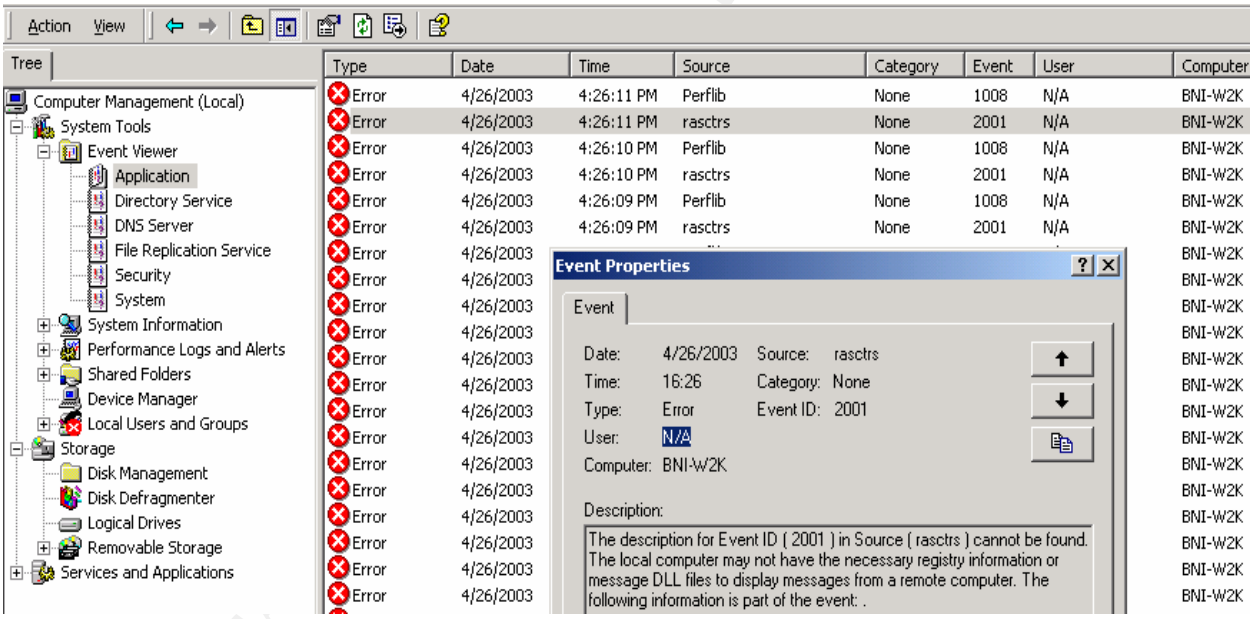
They were able to see only their own folders and 10MB quota was set. (PICTURE) I tested printing to network printers which worked without any problems.



2. I tested that students were able to access the Logger Pro program offered by the Science department. The rights given to the %SystemRoot%\Program Files folders were adequate.



3. Several Event Log Errors were noted after applying the policies. They were related to System Services that had been disabled.

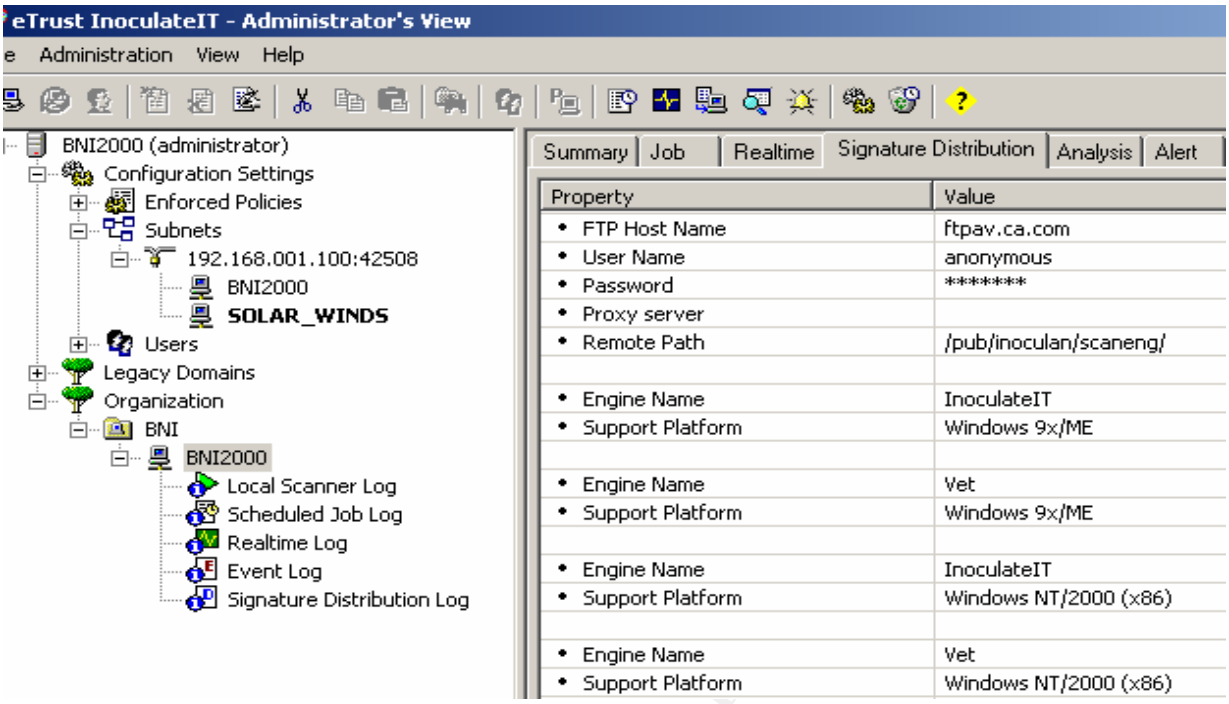


After researching on the internet, the errors were determined to be “cosmetic”. Since the Telephony and Remote Access Services had been disabled, the Performance Monitor was unable to get statistics from them.

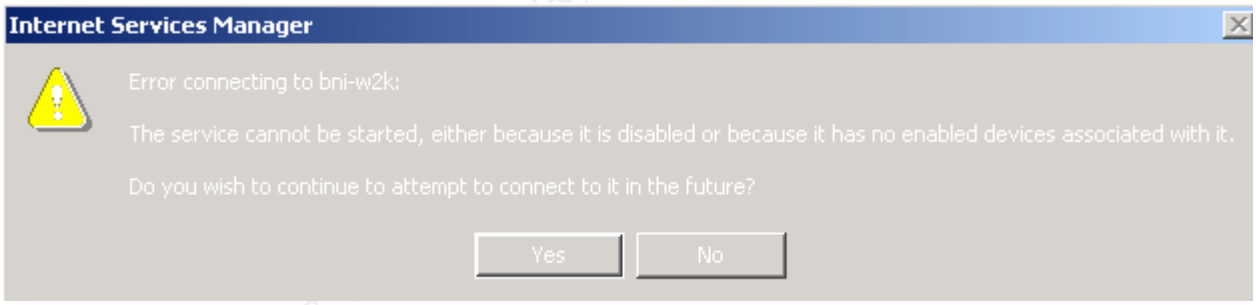
Event ID: 2001	
Source	rasctrs
Type	Error
Description	The description for Event ID (2001) in Source (rasctrs) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. The following information is part of the event: .
Comments	**Gary Busby** Windows 2000 (any edition) issue that is caused when the following three services are disabled: Remote Access Auto Connection Manager, Remote Access Connection Manager, Telephony (all of which are set to Manual by default). Typically, someone would disable these services on Domain Controllers (or other editions) to reduce the number of unncessary services running, of which, these three are not needed as long as RAS is not needed. This message can be especially troublesome on a DC due to it appearing every 60 seconds and filling up/creating large "Application" event log file. However, it is a harmless error. To resolve: 1. Run "unlodctr rasctrs.dll" to unload the counter. 2. Delete the performance counter registry key: HKLM\System\CurrentControlSet\Services\RemoteAccess. Delete the entire "Performance" key. The error will cease. Note: This problem is fixed in Windows XP.
Links	Q246805 , Q811089

See the above notes from www.EventID.com. After applying the recommended fix, the errors stopped.

4. Testing the functionality of the anti-virus's Administrator Console, I was able to connect to remote PCs, install Etrust InoculateIT, distribute virus pattern updates and manage the PC settings.

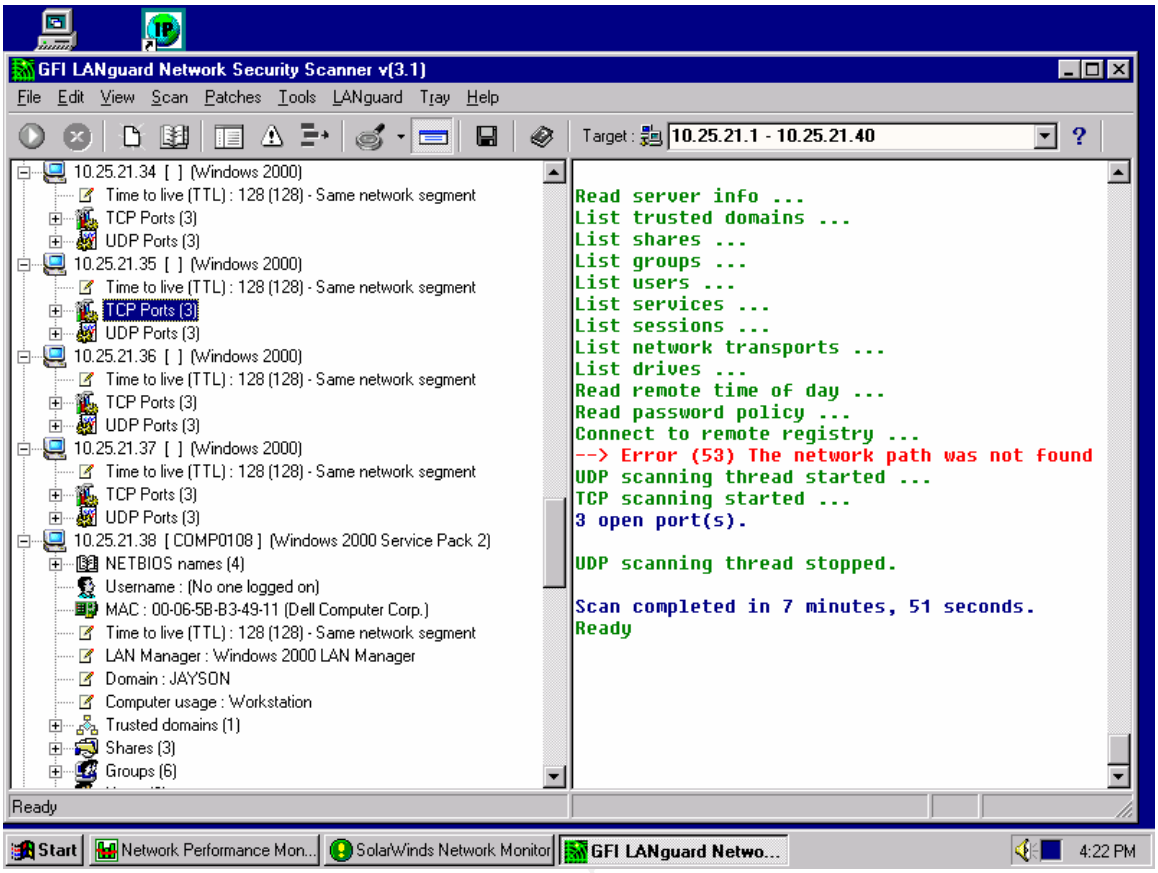


5. The following Error Message occurred when opening Services and Applications from the Computer Management screen. It was related to the IIS Service Manager which had been disabled. Since IIS will not be needed on this server, I used Add / Remove Programs to remove this feature, which was installed by default with the OS.



Once these policy changes were made, I applied them by re-booting the server. I verified that the error messages had stopped.

6. Finally, I tested the ability of GFI's LanGuardNetwork Security Scanner to monitor the Event Logs of the server and scan for port or system vulnerabilities. Initially, I received "**Error 53 – Network Path not Found**".



This error was caused by the setting of the Remote Registry Service. I was able to sucessfully scan the server and monitor the event log after changing this service to start Automatically

V. Evaluate the Effectiveness of the Security Templates

The NSA templates applied have been successful in securing the server for the proposed environment and achieving the level of security outlined in the Security Goals. Some were required by the special circumstances of the environment, some were preferences, and a few were not defined by NSA like the System Services.

Higher level of authentication	Configure **NSA** templates to NTLM authentication (will need to retire Windows NT and 9x clients), and cached credetials
More detailed auditing of system with alert notification of possible intrusion, tampering or problems	Configure **NSA** Auditing Policies and Event Log settings; user 3rd party tools from GFI, SolarWinds and APC
Have fewer system administrators and restrict access to secure areas	Configure **NSA** Restricted Group settings; keep all equipment behind locked doors.
Tighter server security to protect available services, file system and registry security	Configure **NSA** System Service, File System and Registry Policy settings
Prevent students from using too much space on server hard disks; could prevent large downloads	Configure **NSA** Administrative Template settings for System, Quota Policies

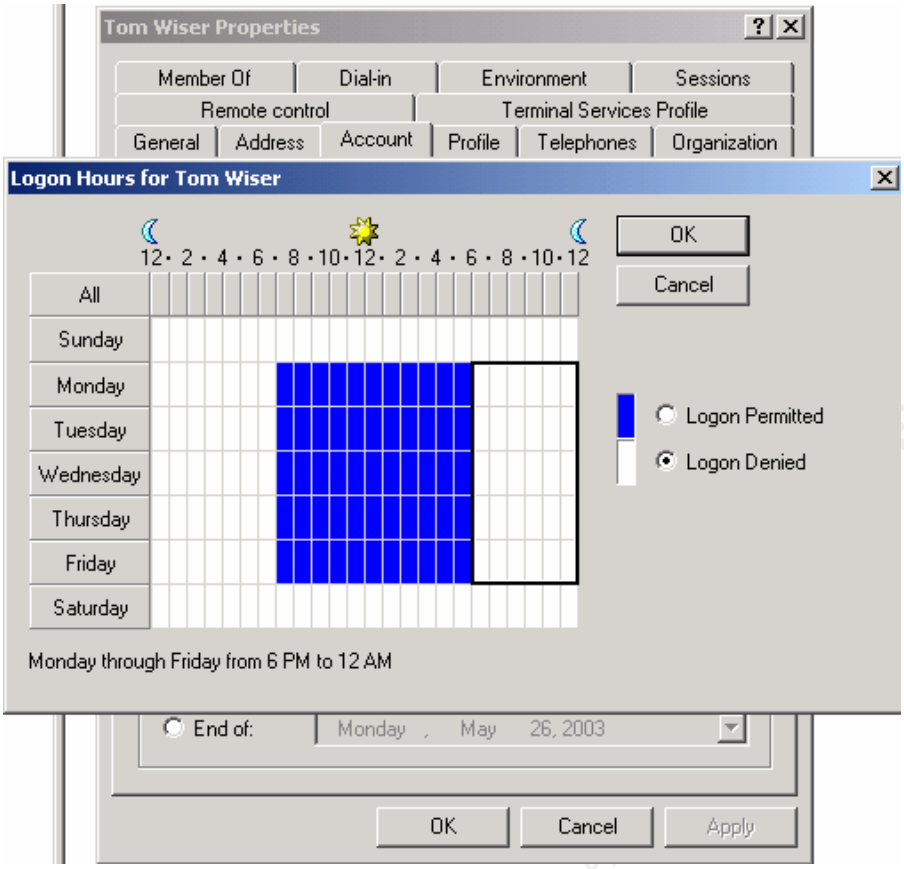
The default **Password Policies** from the NSA were too strong and needed to be modified to address the term of the school semester system. Complex passwords were not desired due to the age of the users.

Some of the **Audit** and **Event Log Policies** were changed to keep the logs from becoming too large. Due to the nature of the daily school schedule, over 300 students and faculty will logon to the network every hour at the beginning of class. This would make the auditing of all logon events, object access and directory service access too high. I also disabled the Automatic Shut down of the system if the event logs got full, due to the erratic nature of the school schedule and availability of Faculty Administrators of the system.

The NSA's recommended **User Rights** were adequate in providing a higher level of security at the server by replacing the Users group with Authenticated Users.

Several settings "Not defined" by the NSA templates were changed in the **Security Options Policies**. The Logon Text Messages remind students on a daily basis of the school's Computer Policy against cheating, and the disciplinary action that would follow if violations occurred. This should be left to the administrator to determine what is best for their environment.

I took advantage of renaming the Administrator and Guest accounts, which the NSA does not do by default in the **Security Options**. This also should be left up to the administrator to determine. And, I implemented restricted logon hours for Students in conjuction with automatic logoff when time expires and an idle time limit to reduce the possiblities of Student tampering. I think the auto logoff is an overall good idea for any site, but the Logon Hours would be site and user specific.



The NTLM authentication level needed to be loosened to allow for some remaining Windows NT and 9x users. The Active Directory Client could be used, but these PCs will be retired at the end of the semester so we did not use it.

The settings for configuring **Restricted Groups** allowed me to limit the members of the Administrators and Faculty groups.

The NSA does not pre-configure **System Services** nor give any recommendations. I found information that helped me secure this area of the system at Tech Republic, the NIST site and Tech Net. The NSA could publish their own recommendations to help administrators by defining the services, determine which services are required for basic system performance and which are optional. This could be a big task since the services required would be based on server role!

The tools we chose to monitor the network, send alerts and update anti-virus software functioned properly, after including the Remote Registry setting on Automatic in the System Services. We were able to secure services adequately.

The Administrative Templates provide many more options for advanced security using Group Policy. We used the options to limit disk quotas for Students to 10MB and control Group Policy updates.

The **File System and Registry Settings** were more than adequate for this environment and there were no problems with system functionality caused by applying them. Students and Faculty were able to access their personal folders and print. The special applications used by the Science department were unaffected.

The **Security Configuration and Analysis** tool was very helpful in testing and verifying that the desired settings were applied. I found it as powerful but easier to use than the command line SECEDIT tool.

Overall, I found that the NSA templates saved a lot of time configuring this server, and that as a guideline the security recommended was more than adequate to meet our Security Goals.

Information Sources:

National Security Agency "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset." March 5, 2003

Allen V. Rouse MCSE, MCDBA, CCNA "Design and Document a Win2K Infrastructure." Tech Republic April 9, 2003

SANS Institute Securing Windows 2000: Step by Step vers 1.5 July 1, 2001

National Security Agency "Microsoft Windows 2000 Network Architecture Guide." March 5, 2003

National Security Agency "Guide to Securing Microsoft Windows 2000 Group Policy." March 5, 2003

Microsoft Technet "Chapter 3, Managing Security with Windows 2000 Group Policy." March 2003

Microsoft Technet #309689 "HOW TO: Apply Predefined Security Templates in Windows 2000." October 26, 2002
http://support.microsoft.com/default.aspx?scid=kb;en-us;309689

Microsoft Technet #318753 "How To Create a System Policy Setting in Windows 2000." http://support.microsoft.com/default.aspx?scid=kb;en-us;318753

Mark Burnett "The Power of Security Templates." InstantDoc #25576 August 2002
http://www.windowswebsolutions.com/Articles/Index.cfm?ArticleID=25576

MicrosoftTechnet #256345 "HOW TO: Configure Group Policies to Set Security for System Services." http://support.microsoft.com/default.aspx?scid=kb;en-us;256345#2