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.

PKI: Protection of Stand Alone Certificates

A Windows 2000 (W2K) Stand-alone Offline Root Certificate Authority (SaORCA) is an extremely important element in an organization's W2K Public Key Infrastructure (PKI). A W2K SaORCA is the cornerstone of an organization's W2K Certificate Authority (CA) Hierarchy and an organization's W2K CA Hierarchy is the frame to support an effective organizational W2K PKI. Because of its importance, the W2K SaORCA requires an elevated level of protection to ensure the confidentiality and integrity of its own self-signed Root CA Cer...

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Sans Windows 2000 Security GCNT Practical Exercise:

Microsoft Windows 2000 Security:
Windows 2000 Stand-alone Offline Root Certificate Authority Protection Guide

William S. Pachucki
March 2000

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

Microsoft Microsoft Windows 2000 Security:
Windows 2000 Stand-alone Offline Root Certificate Authority Protection Guide

A Windows 2000 (W2K) Stand-alone Offline Root Certificate Authority (SaORCA) is an extremely important element in an organization's W2K Public Key Infrastructure (PKI). A W2K SaORCA is the cornerstone of an organization's W2K Certificate Authority (CA) Hierarchy and an organization's W2K CA Hierarchy is the frame to support an effective organizational W2K PKI.

Because of its importance, the W2K SaORCA requires an elevated level of protection to ensure the confidentiality and integrity of its own self-signed Root CA Certificate(s), of its own private key(s), and the issued and/or revoked Certificates that belong to its subordinate W2K CAs.

This protection guide is designed to offer a starting point for seasoned W2K Server Administrators assigned the organizational W2K PKI role and responsibility of W2K SaORCA Administrator. This guide is the combination of:

- a number of pre-existing Windows NT and Windows 2000 Security Checklists
  - Windows NT C2 Configuration Checklist
    http://www.microsoft.com/technet/security/C2config.asp
  - Windows 2000 Installation Security Checklist.
    http://www.labmice.net/articles/securingwin2000.htm

- a number of PKI references (both offline and online)
  - *Windows NT Security: Step by Step* & *Windows 2000: PKI (J. Fossen)*
  - The IETF Security Working Group: Public-Key Infrastructure (X.509) (pkix) http://www.ietf.org/html.charters/pkix-charter.html
  - The RSA Public Key Cryptography Standards
    http://www.rsasecurity.com/rsalabs/pkcs/

- a number of years of experience the author has had with
  - Public Key Infrastructure (business, policy & technology)
  - Information Security
  - Windows NT 4.0 Security
  - Windows 2000 Security

This guide covers both technical and non-technical best practices to assist administrators protect the SaORCA and attain a degree of confidentiality and integrity that is required and in accordance with the organization's W2K PKI Certificate Policy, Certificate Practice Statement, and/or all other applicable security policies.

Note: Although this guide was specifically designed to protect a W2K SaORCA server that <u>DOES NOT</u> have a network connection, it may be used as a baseline document to create a protection guide for a W2K SaORCA server that does have network connectivity.

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

Part 1: Obtain the Knowledge to Protect the W2K SaORCA

- **Research/Review Public Key Infrastructure Concepts**

Administrators new to PKI should familiarize themselves with PKI concepts, technology, and operations, such as: Public-Private Key Pair, Digital Signature, Certificate Policy (CP), Certificate Practice Statement (CPS), Certificate Authority (CA), Registration Authority (RA), Directory Service (DS), Certificate Revocation List (CRL), X.509 Certificates, Public Key Cryptography Standards (PKCS), and the list goes on and on.

A great way to start is by attending a PKI Training Course offered by a reputable PKI vendor or Technical Training Organization. Many vendors offer both online and traditional face-to-face classroom instruction. Here are just a few:

- Verisign PKI Training
  http://www.verisign.com/training/courses/pki/index.html

- Xcert Resources
  http://www.xcert.com/resources/index.html

- Entrust PKI Training
  http://www.entrust.com/training/courses.htm

Another way to acquire PKI knowledge, specifically W2K PKI knowledge, is through the Certificate Services. Once installed additional Windows 2000 PKI information is available via the Certificate Services built-in help files. If the help files are not available at this time, much of the same PKI information can be found online. Here are some the online links to start with:

- Planning Your Public Key Infrastructure -
  http://www.microsoft.com/technet/win2000/dguide/chapt-12.asp

- Windows 2000 Certificate Services Best practices -
  http://windows.microsoft.com/windows2000/en/server/help/sag_cs_bestpract.htm

- Creating a certification hierarchy with an offline root certification authority -
  http://windows.microsoft.com/windows2000/en/server/help/sag_CS_Checklist_Offline.htm

- To install a stand-alone root certification authority -
  http://windows.microsoft.com/windows2000/en/server/help/sag_CSprocsInstallRoot_SA.htm

- Certificate Overview -
  http://windows.microsoft.com/windows2000/en/server/help/default.asp

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

For additional information concerning PKI, here are just a few excellent online resources to begin with:

- The IETF Security Working Group: Public-Key Infrastructure (X.509) (pkix) - http://www.ietf.org/html.charters/pkix-charter.html

- The RSA Home Page - http://www.rsasecurity.com/

- Site dedicated to listing PKI References - http://www.pkiforum.org/resources/

Reminder: It is a good idea to start a PKI Favorites Folder in I.E. before you start browsing. Once you get out and onto the PKI information highway you'll be able to quickly "Add" your preferred PKI websites with a quick click of the mouse.

- ***Review Organizational Security Policies***

To effectively administer the SaORCA an administrator must be familiar with all organizational information security (InfoSec) policies. SaORCA Administrators will definitely become extremely familiar with the W2K PKI CP and CPS. (Keeping a copy close by is a recommended… "best practice".)

When reviewing the CP/CPS administrators should pay particular attention to the areas that will affect W2K SaORCA administrative tasks as well as protective measures. Here are the normal CP areas to look out for:

- Compliance audit frequency and topics
- Security audit procedures used to describe event logging and audit systems
- Key changeover
- Compromise and disaster recovery
- CA termination
- Physical security controls
- Technical security controls like PINs, passwords, or manually-held key shares
- Network security controls like disabling unnecessary services
- Cryptographic module engineering controls that addresses identification of the
- Cryptographic module roles and services, physical security, operating system security, algorithm compliance, etc.

- ***Review Organizational PKI Design and/or Implementation Plan***

An organization's PKI Design and/or Implementation Plan covers a number of issues relevant to SaORCA administration. For instance, the CA hierarchy plan addresses the naming convention that, in turn, directly affects the SaORCA Computer Name.

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

Part 2: Physically Protect the W2K SaORCA

- **Physical Protection**

Ensure the physical protection of the W2K SaORCA, (and the W2K SaORCA backup), is in accordance with the CP/CPS, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), etc. For example:

- When not in use, the SaORCA is stored in a locked room with video monitoring and logged access
- When not in use the SaORCA is stored in a locked cabinet in the server room
- Surveillance cameras are required inside and outside the data center
- Physical access to the machine requires the "two man rule"
- When not in use, the hard drive must be removed and placed in the vault
- Backup media is stored at an alternate site (at least 25 miles away)

- **Machine Requirements**

Ensure the selected computer meets the minimum system requirements outlined by Microsoft for a Windows 2000 Server (plus Certificate Services).

Computer's hardware configuration is in compliance with the organization's CP/CPS:

- The CP may specifically state that the SaORCA will not have networking capability – no NIC, no Modem, no infrared capability, etc.

- The Computer has Power on Password Protection (If required and/or available)

- Third party products are authorized for use:

    - Smart card readers used in two-factor authentication
    - Zip disk drive used to transport certificates and certificate requests

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

Part 3: Protect W2K SaORCA Operations

- **Network Connectivity**

As a rule of thumb, a root ca should not be connected to a network and should only issue Subordinate CA Certificates. The certificates are transported via a peripheral media device such as a floppy or zip disk.

Organizational business objectives and money play important roles in whether or not the SaORCA is connected to the network or not.

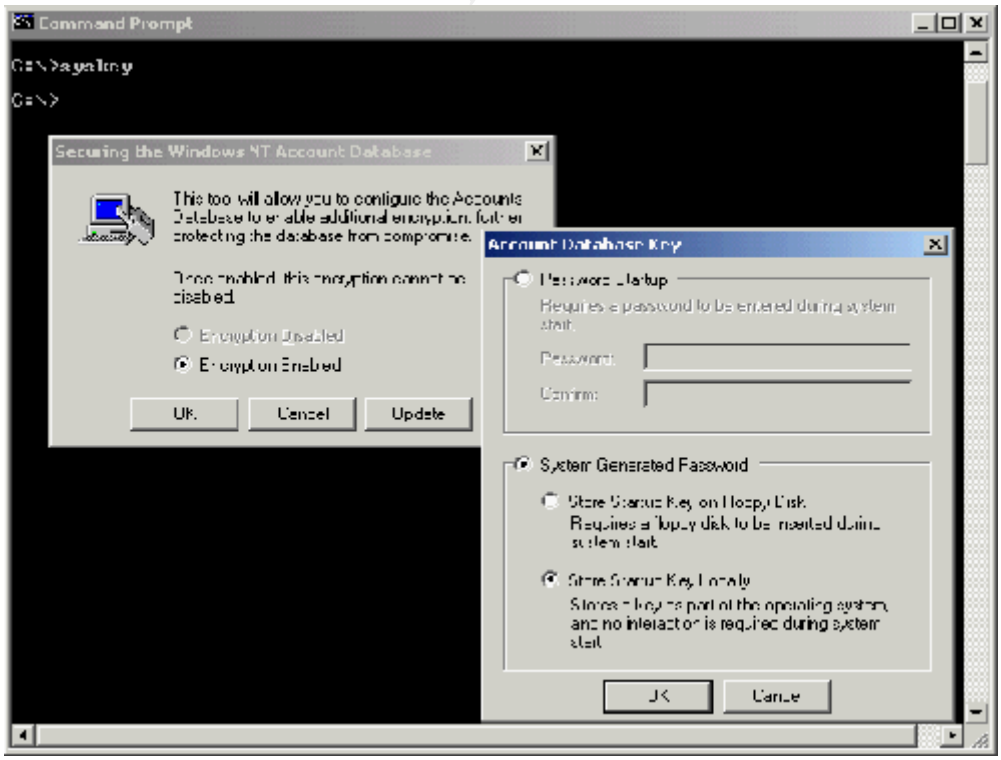
Remember,… this guide is designed for a **"connectionless"** computer.

- **Operating System**

The W2K SaORCA contains only one Operating System: Windows 2000 Server or Windows 2000 Advance Server.

- **Boot Protection**

Windows 2000 Server offers "syskey" as another layer of protection to limit access to the Operating System. The use of "syskey" is optional for a W2K SaORCA since it will be physically protected from access and not connected to a network.

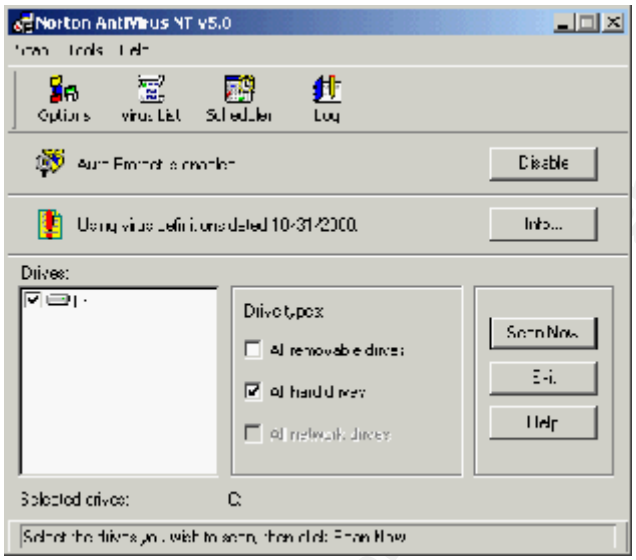


From the command line > "syskey" then, update for available options.

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

- **Anti-Virus Protection**

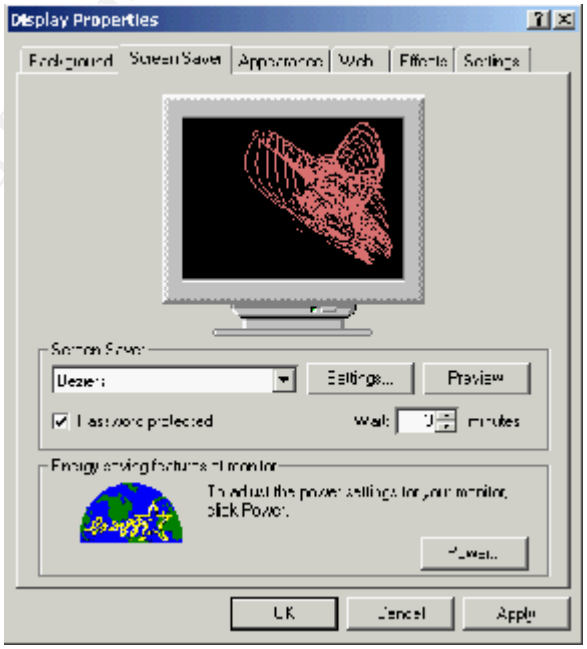
Anti-Virus Protection must be installed, operational, and current. Procedures must be in place to update the virus protection software package.



Anti-Virus Software provides an extra layer of protection when importing/accepting possibly infected certificate requests.

- **Screen Saver**

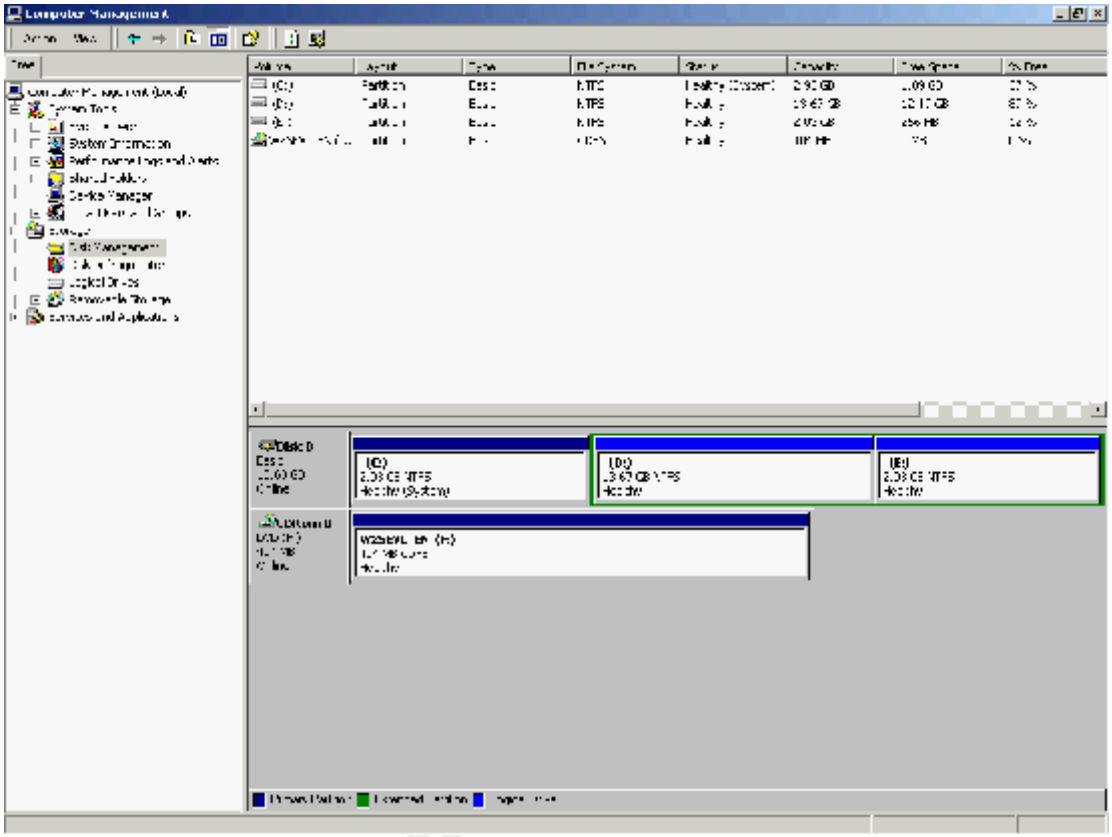
The password protected screen saver is yet another optional layer of protection that may be applied to a W2K SaORCA. (Policy will drive its use and configuration)



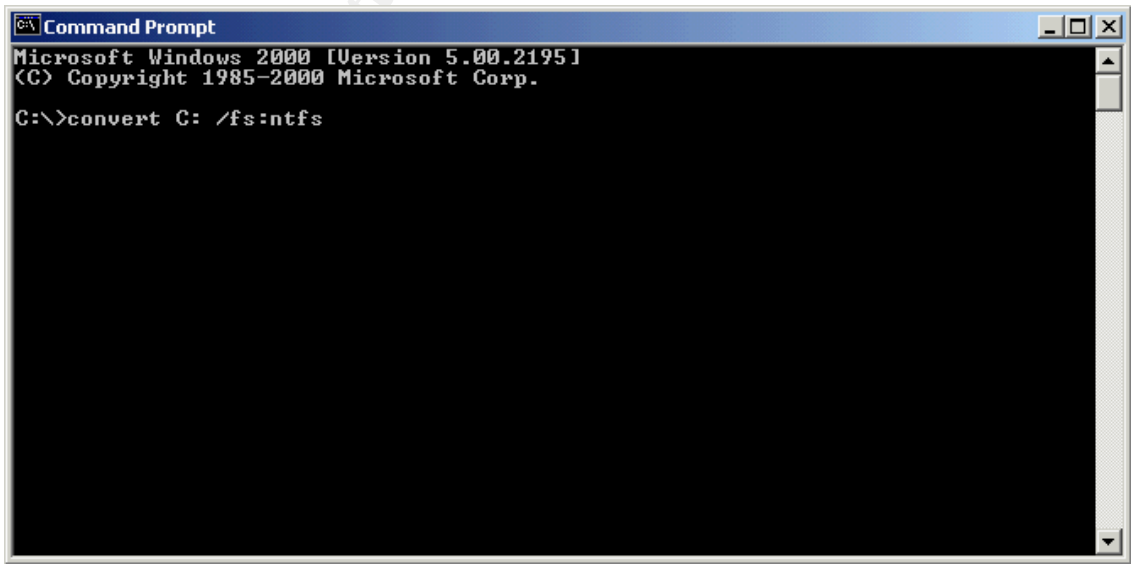
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- **Partitions**

All partitions must be NTFS. Right Click on a partition for formatting options.



Right Click: My Computer > Manage > Storage > Disk Management



To format from the command line.

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

- **High Encryption Pack**

The High Encryption Pack (HEP) must be installed on the computer. The Cipher Strength should read 128-bit.

From Desktop Select: Internet Explorer > Help > About Internet Explorer

The EHP upgrade only takes a few seconds and is available via internet download or CD. http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp

The upgrade will not affect previously created keys. If these previously created keys exist an upgrade is possible with the use of the Key Migration Tool. See next section, "Service Packs", for more information.

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

- **Service Packs**

The latest service pack must be installed on the computer. The Service Pack is available via internet download or CD.
http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp

Select: Start > Run > Open: "winver"

- **Microsoft Security Notification Service**

All Windows 2000 Administrators, including W2K CA Administrators, should subscribe to the Microsoft Security Notification Service to keep abreast of the latest security vulnerabilities.

To subscribe visit the following website:
http://www.microsoft.com/technet/security/notify.asp

Most bulletins and their related patches are for network related issues and will not directly affect W2K SaORCA operations. But, for audit purposes, the CA Administrator must be aware of all known server vulnerabilities and their fixes. Administrators must also be on the look out for performance related issues.

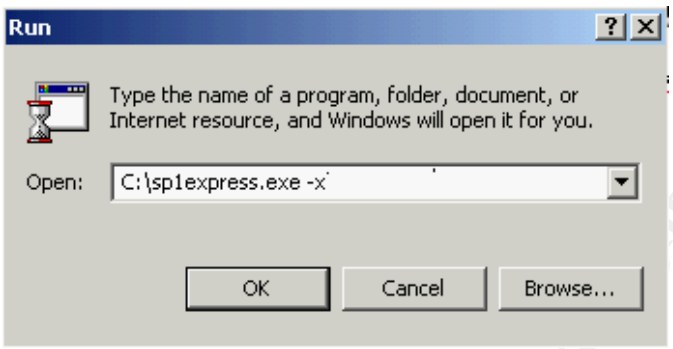
To view current bulletins or search for earlier bulletins visit the following website:
http://www.microsoft.com/technet/security/current.asp

Note: Ultimately, the CA Administrator is responsible for being aware of all known vulnerabilities and performance issues and then deciding which fixes to apply.

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

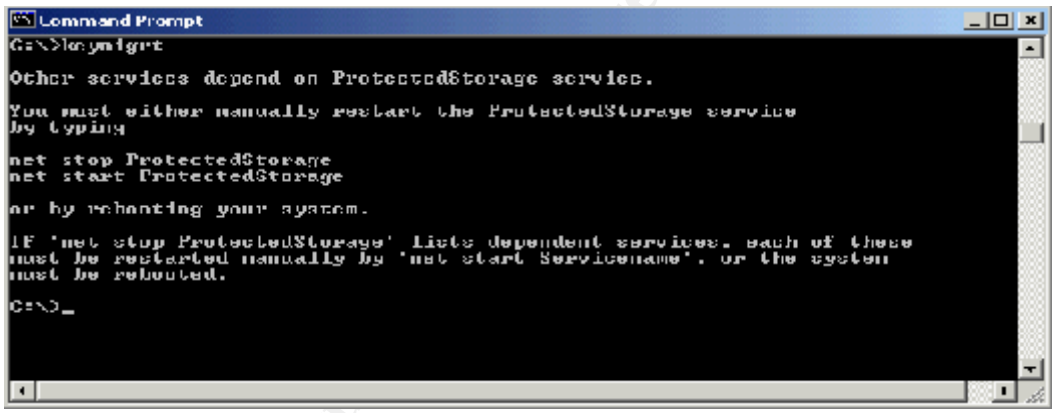
- **Key Migration Utility**

Once the **Service Pack** is installed the Key Migration Tool may be extracted for use.

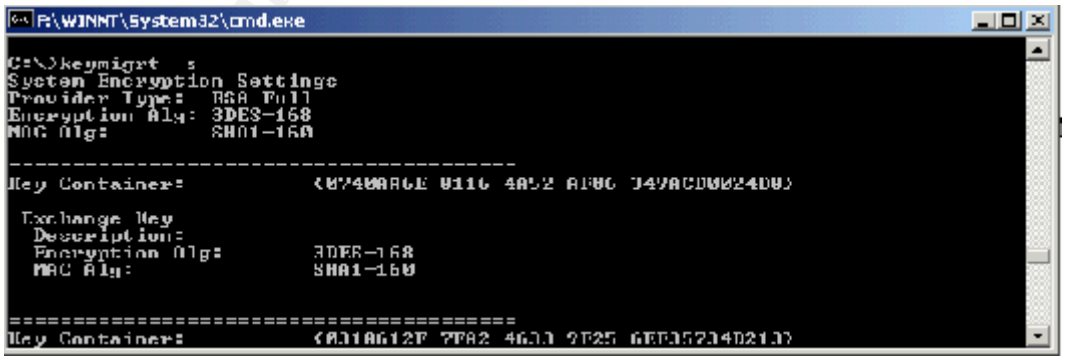


The "keymigrt" executable can be extracted for use with the "–x" switch.

Use the "keymigrt" tool to verify key(s) upgrade status.



Execute: >"keymigrt" and then, Stop Storage



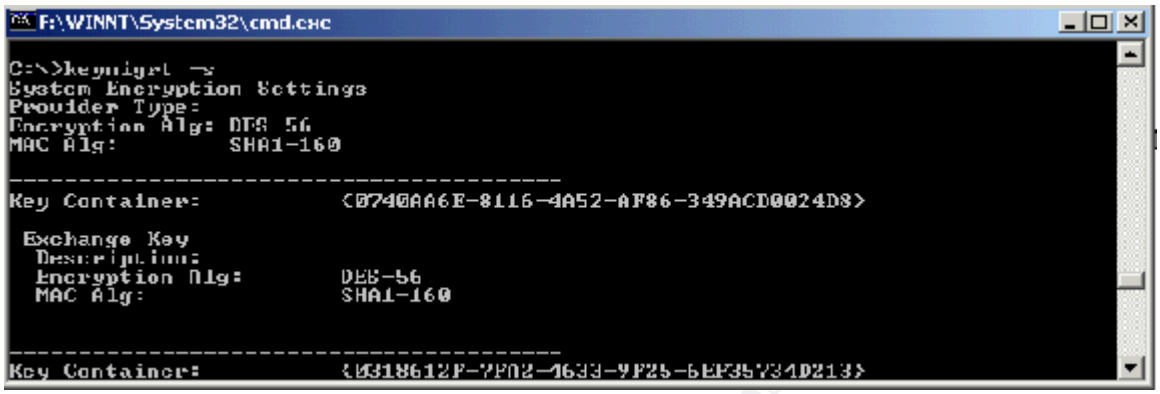
Execute: >"keymigrt -s"

As seen above, the System Encryption Settings indicate encryption upgrade status. If private keys and containers exist they also appear.

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

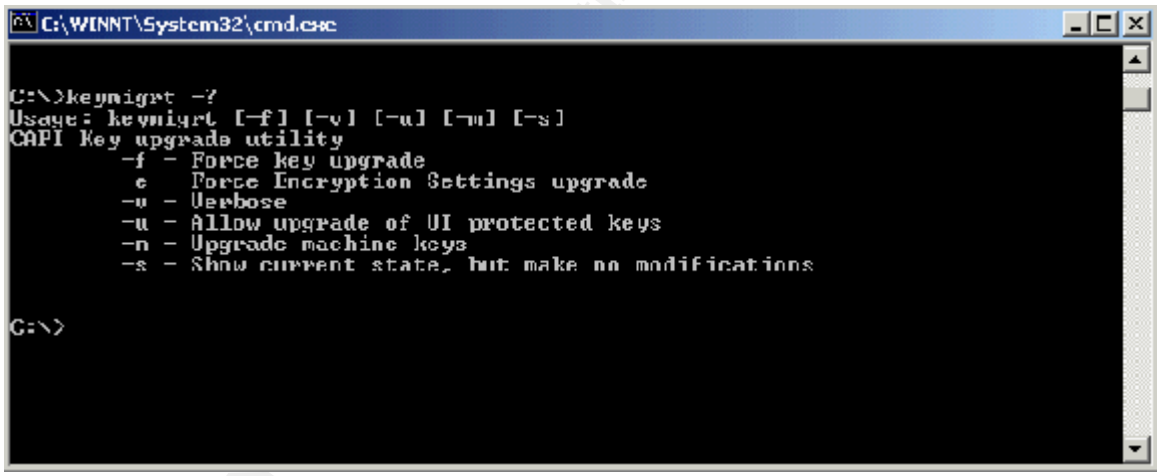
"Keymigrt" was designed to upgrade keys that were created prior to an EHP upgrade.

As seen below, if weak keys exist, simply migrate the encryption keys using the tool. (Migrate keys that are less than 3DES-168)



Execute: "keymigrt –s"

Using the command "Keymigrt –s >> output.txt" will create a text file that can be used for audit and analytical purposes.



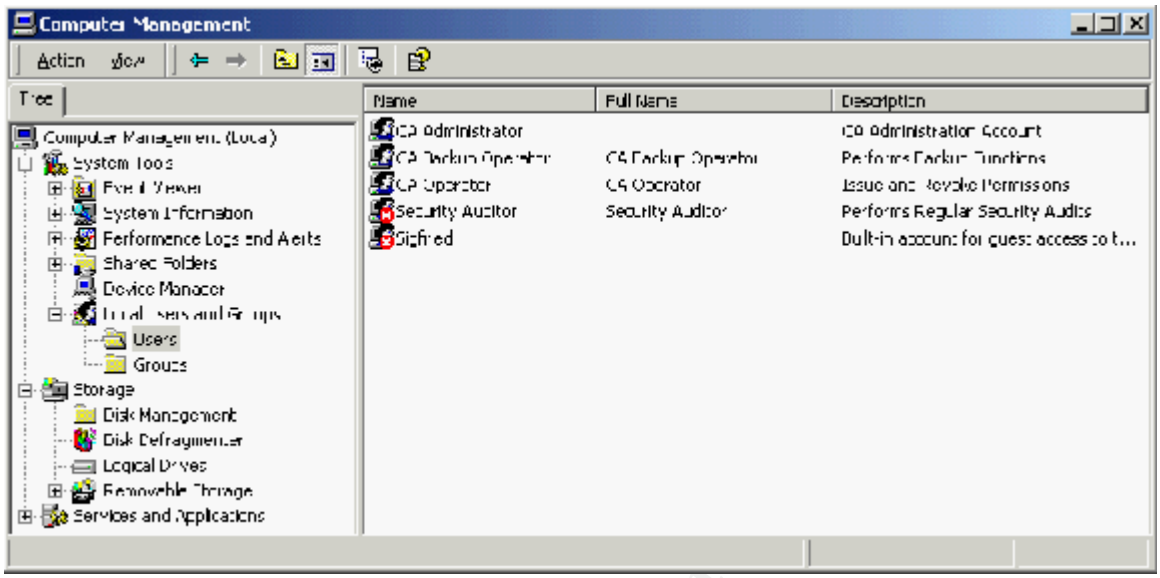
To view all "keymigrt" options … ***Execute: > "keymigrt –?"***

To perform a complete upgrade ***Execute: > "keymigrt –v –m –u –f –e"***

Note: To avoid Key Migration issues of any kind, ensure the EHP is installed prior to Certificate Service Installation.

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

- **Manage Accounts**



- Limit accounts to only those PKI Roles specified in the CP/CPS. Normal PKI Administration Roles are: CA Administrator (Renamed Administrator Account), CA Operator, Security Auditor, and CA Backup Operator.

- Disable all newly created accounts, i.e., Security Auditor, until they are needed.

- Delete built in accounts that are not required.

- Disable the Guest Account (renamed) and create an extremely complex password.

- Keep account management simple. W2K SaORCA access auditing/record keeping is extremely important to the integrity of SaORCA Operations. Look to CP/CPS for further guidance.

- **Shut down unnecessary Devices**

The SaORCA hardware configuration should consist of the minimum required devices to get the job done. The SaORCA normally requires peripheral storage devices such as Floppy Drives and/or Zip Drives for Certificate Management.

When dealing with a connectionless SaORCA, services like TCP/IP and accompanying tcpip.sys driver are not a concern.

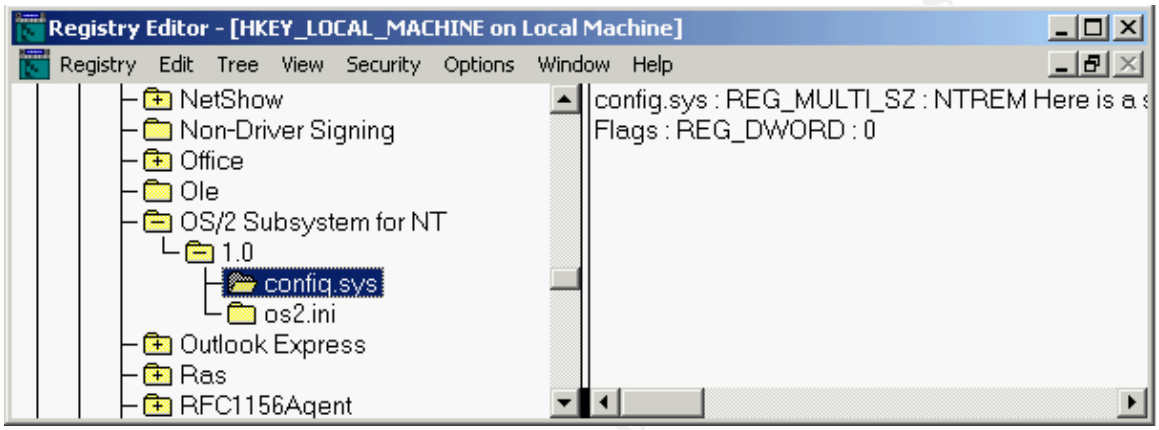
The primary concern over devices in a connectionless SaORCA is for audit purposes and system performance.

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

- **Remove the OS/2 and POSIX Subsystems**

Removing these subsystems only help to improve the system's performance. If performance is an issue, disable these subsystems by simply making the following changes to the Registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT



Delete all sub keys

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment

  Delete the value for Os2LibPath

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

  Delete the value for Optional

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

  Delete entries for Posix and OS/2

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

Part 4: Protect W2K SaORCA Operations with Local Computer Policy

Since the machine is connectionless, the Local Computer Policy settings will effectively protect a great majority of the standard Windows 2000 Operating System features. (Features normally considered to be, security "holes.")

In the sub-sections that follow:

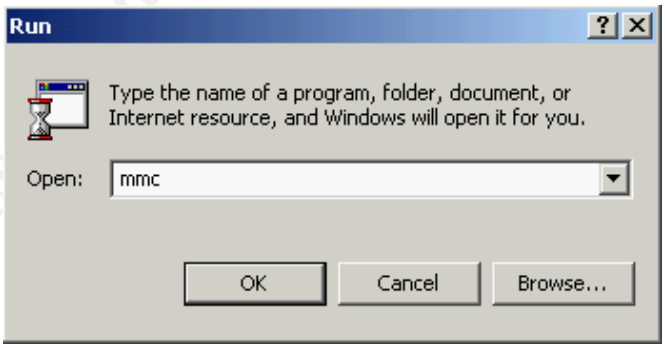
- Part 4a: Create a W2K SaORCA High Security Template (SaORCAHiSec.inf)
- Part 4b: Analyze Local Computer Policy and update SaORCAHiSec.inf
- Part 4c: Save and Implement SaORCAHiSec.inf Template

A Windows 2000 Security Template will be created, saved, and then, applied to the W2K SaORCA. Application of the template will directly affect the following containers:

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

Part 4a: Create a W2K SaORCA High Security Template (SaORCAHiSec.inf)

- **Create the new Template**



Open: "MMC" or, Execute from Command Line " gpedit.msc"

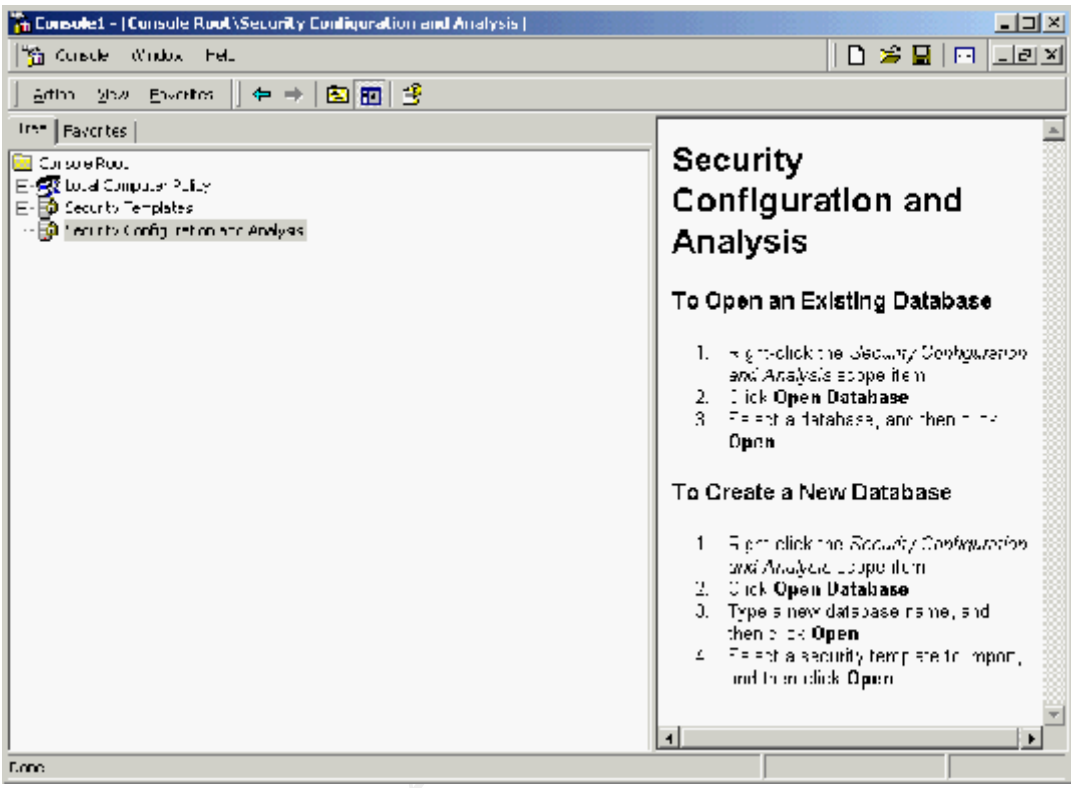
Load the "Local Computer Policy", "Security Templates", and "Security Configuration and Analysis" Snap-ins. Expand "Security Templates" and then, right click the "hisecdc.inf" security template and "Save as... SaORCAHiSec.inf". The new template may now be used to analyze the local computer.

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

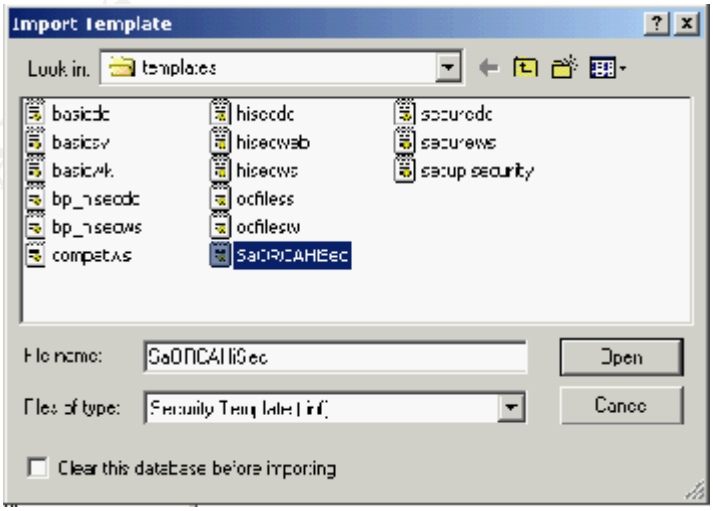
Part 4b: Analyze Local Computer Policy and update SaORCAHiSec.inf

- **Perform the analysis**

Analyze the current local policy using the new "SaORCAHiSec.inf" security template.



Instructions to analyze the computer appear automatically in the "mmc". For more information view the built-in help files.

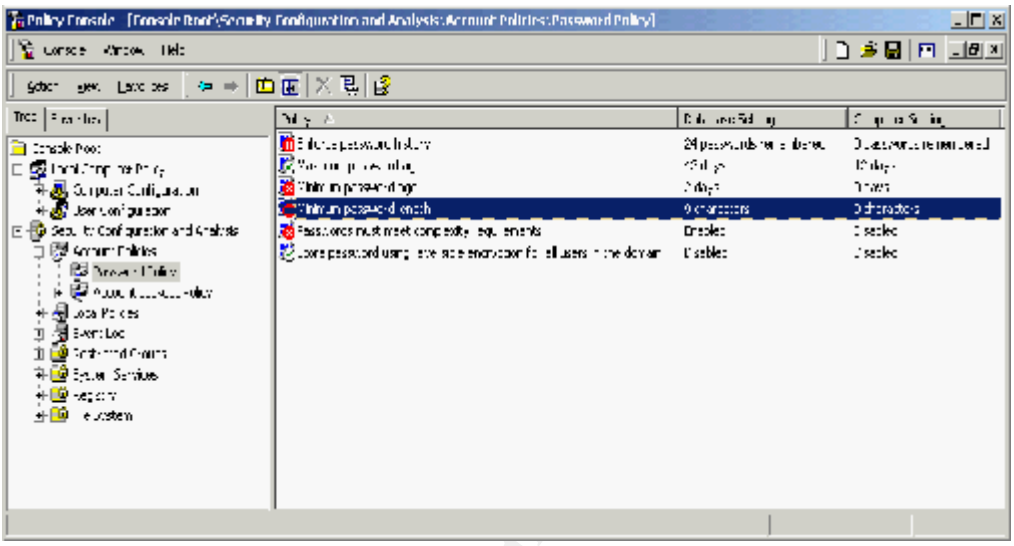


Select the new template to be used in the analysis

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

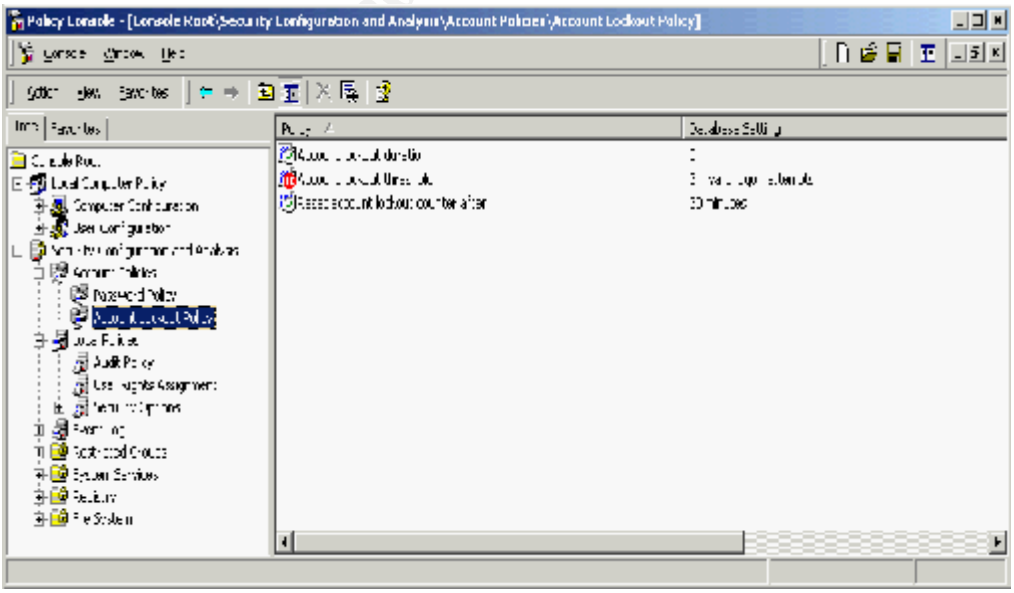
- **Account Policies\Password Policy**

Logon/Authentication: Change Minimum Password Length Computer Setting to **9** Characters. Logon passwords must be in accordance with security policy. Recommended password policy: complex password (mixed letters/numbers and three special characters) with a minimum of 9 characters.



- **Account Policies\Account Lockout Policy**

Change Threshold to **3** attempts



- **Local Policies\Audit Policy**

Change Audit Process Tracking to: **Success, Failure**

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

- **Local Policies\User Rights Assignment**

Make the fourteen (14) changes to highlighted User Rights Policy Elements based on the following snap shot display.

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	Backup Operators
Bypass traverse checking	Not defined
Change the system time	Administrators
Create a pagefile	Administrators
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	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	Not defined
Log on as a batch job	Not defined
Log on as a service	Not defined
Log on locally	Backup Operators,Users,Administr
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Not defined
Replace a process level token	Not defined
Restore files and directories	Backup Operators,Administrators
Shut down the system	Administrators
Synchronize directory service data	Not defined
Take ownership of files or other objects	Administrators

Note: Once again, the CP/CPS will play a significant role in determining specific user rights assignments

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

- **Security Options**

Make the six (6) changes to highlighted Policy Options based on the following snap shot display. Update: Audit Backup, Message Text & Title, Rename Administrator & Guest Accounts, and unsigned non-driver installation behavior.

Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only)	Disabled
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	15 minutes
Audit the access of global system objects	Disabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Enabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Enabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	Warning! Only authorized personnel allowed. If you do not...
Message title for users attempting to log on	Access Warning!
Number of previous logons to cache (in case domain controller is not available)	10 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Rename administrator account	Not defined
Rename guest account	Sigfried
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Disabled
Smart card removal behavior	Force Logoff
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
Unsigned driver installation behavior	Do not allow installation
Unsigned non-driver installation behavior	Warn but allow installation

- **Logon/Authentication Warning Dialog Box**

Supply an easy to understand legal warning. Refer to CP/CPS for detail.

- **Built in Lock**

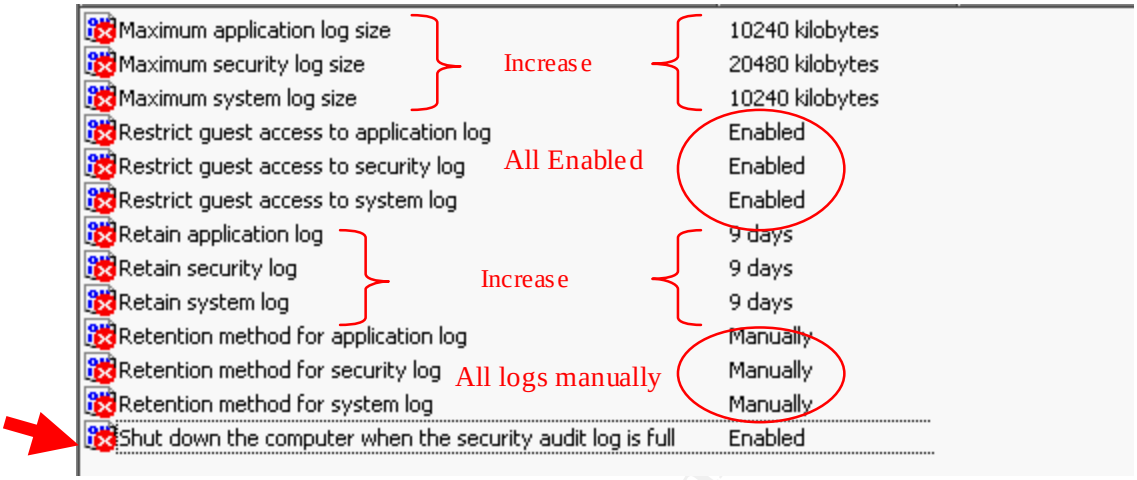
After a prescribed amount of "idle" time (15 minutes as seen here) the computer must automatically lock requiring re-authentication for continued access. See CP/CPS.

Note: The CP/CPS, (or other applicable security policies,) will supply guidance for these and other possible Security Option Settings.

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

- **Event Log Settings**

Make the ten (10) changes to the Event Log Settings based on the following snap shot.



- **Restricted Groups**

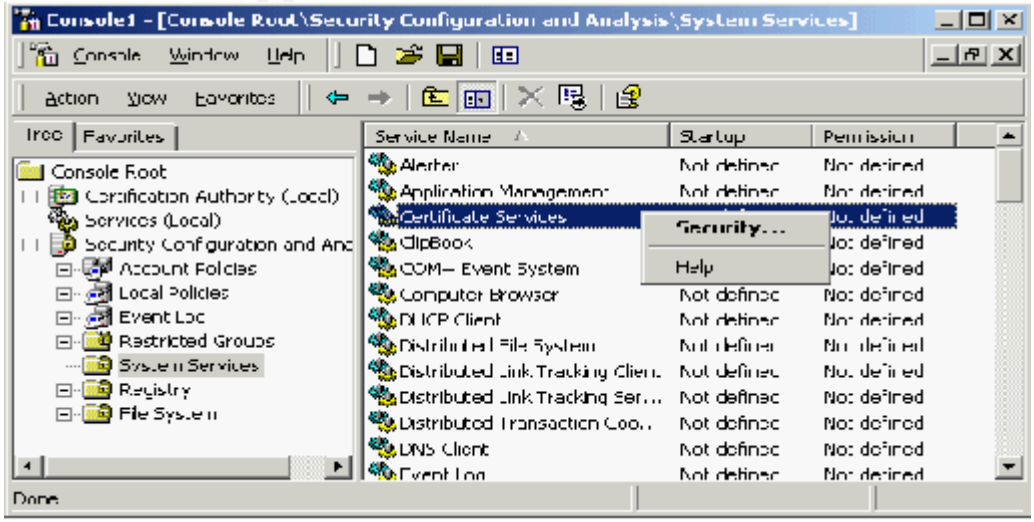
Leave the default settings. Restricted Groups do not affect the connectionless SaORCA. (Restricted Groups will be significant in the administration of specific groups if and when connected to a network.)

- **System Services**

A record of the running services is required for audit purposes.

Disabling unnecessary services can only help to improve performance, if it is an issue.

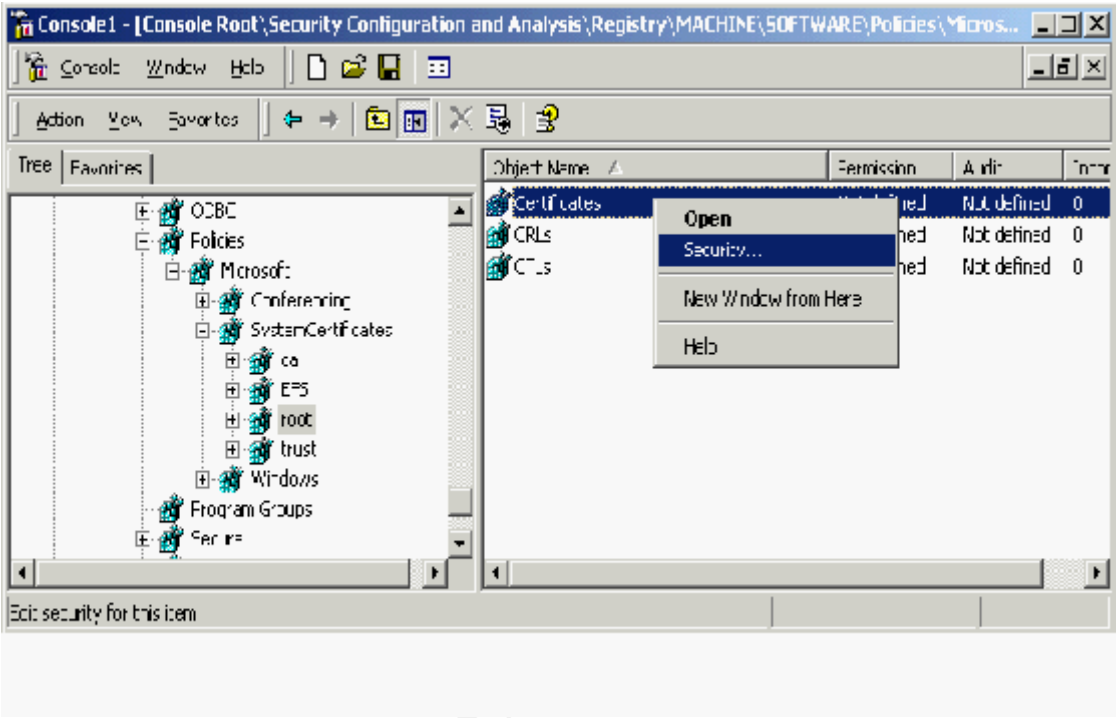
Individual services, (i.e., Certificate Services), may be audited by a simple 'right click" and then selecting "Security". (See Object Access Auditing later in this guide.)



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

- **Registry**

Individual Registry Objects, (i.e., Root Certificates), may be audited by a simple 'right click" and then selecting "Security". (See Object Access Auditing later in this guide.)



NOTE: The following registry setting update requires actual registry access! (Open: regedt32.exe)

HKEY_CURRENT_USER\Software\Microsoft
Windows NT\CurrentVersion\SeCEdit
Reg Values\MACHINE/System\CurrentControlSet

Set the CrashOnAuditFail value to "1"

The setting compliments the Event Log Setting noted earlier: "Shut down the computer when the security audit log is full."

The setting adds a layer of protection to protect the integrity of the audit logs. If the computer crashes and the value is set to "1" the only one allowed to logon on to the machine is the SaORCA Administrator. The Administrator can then bring the machine up and perform the required backup.

Important: If the crash takes place the value will have to be reset to ensure this protection continues to be available.

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

- **File System**

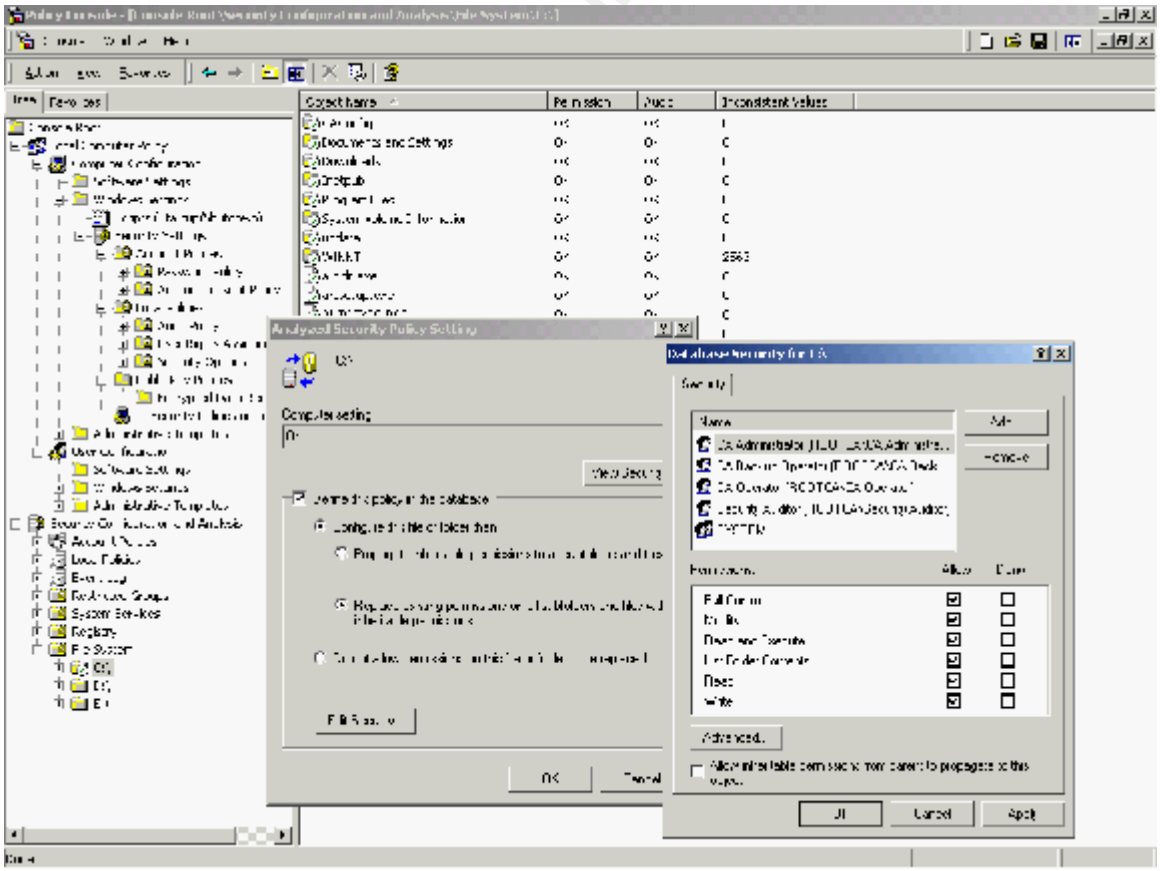
Due to a high level of protection of the **System Directories, Folders, and Files with Permissions** and the limited number of accounts that will access the SaORCA, the following Access Control List adjustments must be made…

First, right click the "\" folder, (C:\ below), and select Security…

- Select "Replace existing permissions on all subfolders and files with inheritable permissions."
- Select "Edit Security"
- Remove "Everyone" and add the appropriate CA Administrator and users
- Assign the appropriate permissions:

\

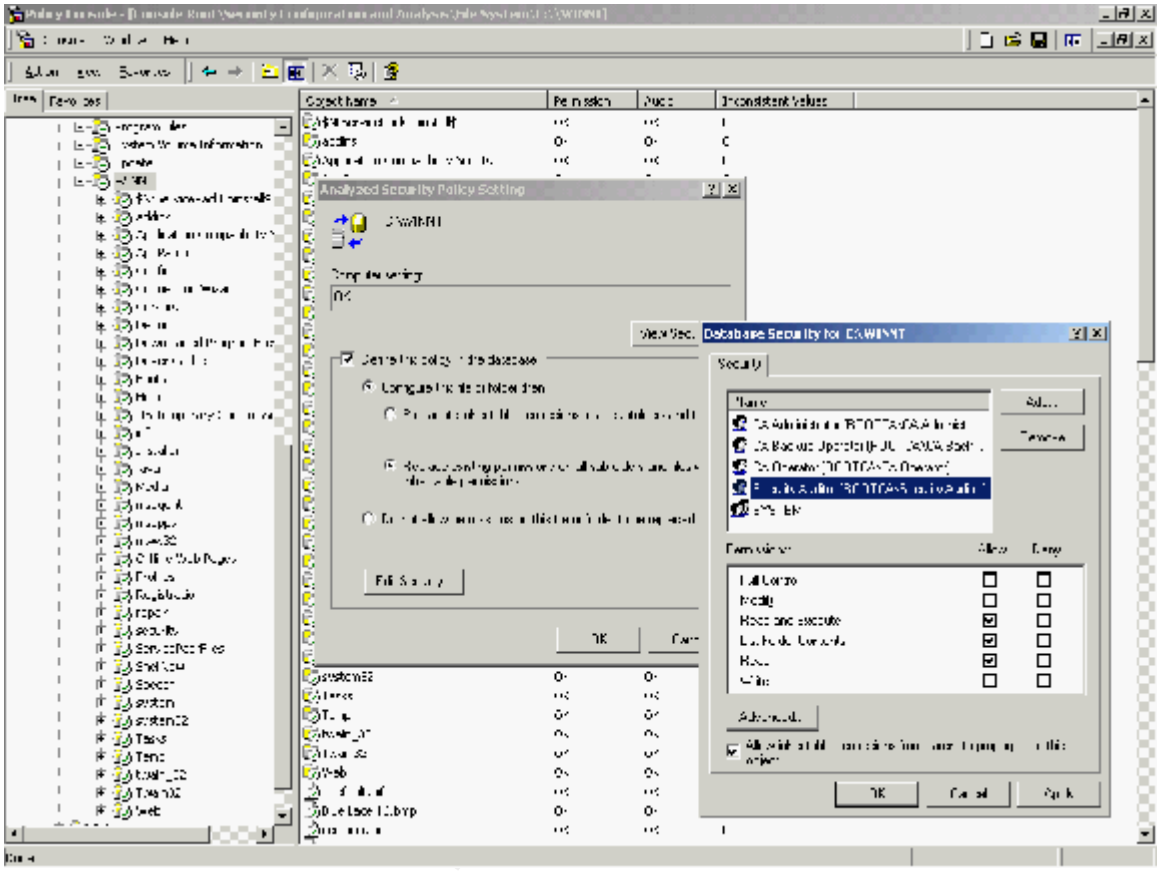
CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read



Once additions and permissions are set click OK to save the settings.

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

For the following directories, folders, and files perform the same steps. Make sure the following box is checked: "Allow inheritable permissions from parent to propagate to the object box." (See the %System Root% example below.)



Now navigate to the directories, folders, and files listed on the next few pages. For each remove the "Everyone" Account and add the appropriate SaORCA roles as prescribed in the CP/CPS.

!!! When adding accounts to the Security Tab **each** role defaults to the following permissions:

Read & Execute, List Folder Contents, and Read !!!

Reminder: This practical exercise is using the five accounts: CA Administrator Account, the CA Backup Operator Account, the CA Operator Account, the Security Auditor Account, and the System Account.

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

- **System Directories, Folders, and Files to protect and corresponding ACL/Permission Settings:**

\

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\%System Root%

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\%System Root%\system32

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\%System Root%\system32\config

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\%System Root%\system32\drivers

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\%System Root%\system32\spool

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

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

- **System Directories, Folders, and Files to protect (continued)**

\%System Root%\repair

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\boot.ini

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\ntdetect.com

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\ntldr

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\autoexec.bat

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\config.sys

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

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

- **Protect the Certificate Log Folder, Certificate Database, Certificate Database Log, and CA Configuration files:**

\%System Root%\system32\ certlog

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\%System Root%\system32\ certlog\%ROOT%.edb

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\%System Root%\system32\ certlog\edb

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\CAConfig

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

Note: Fine-tuning of the permissions, in accordance with the CP/CPS, is preformed by selecting the "Advanced…" button for each role/account.

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

- **Protect the Security Audit Logs and Security Configuration file**

\%System Root%\repair\security

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

\%System Root%\system32\ config\security

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

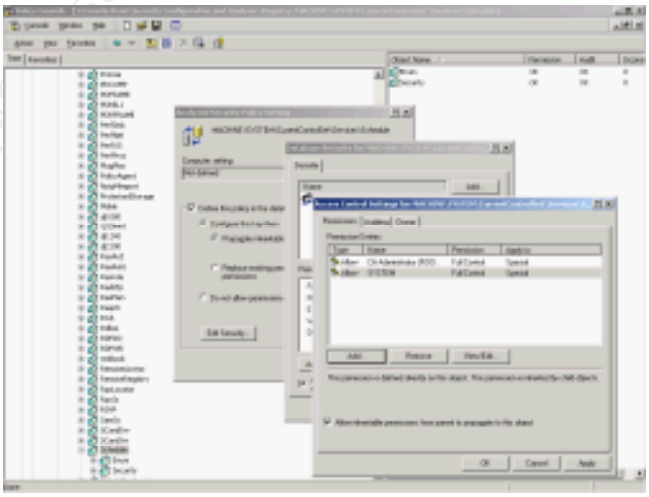
- **Protect the Security Event Log**

\%System Root%\system32\Config\SecEvent.Evt

CA Administrator	Full Control
System	Full Control
Security Auditor	Read & Execute, List Folder Contents, and Read
CA Operator	Read & Execute, List Folder Contents, and Read
CA Backup Operator	Read & Execute, List Folder Contents, and Read

- **Limit Scheduler list access: Optional**

The Scheduler service in Windows 2000 allows commands to execute at specific times; the commands run as "System". An important fact to note is that the scheduler also lists this information. To limit viewing make appropriate changes.



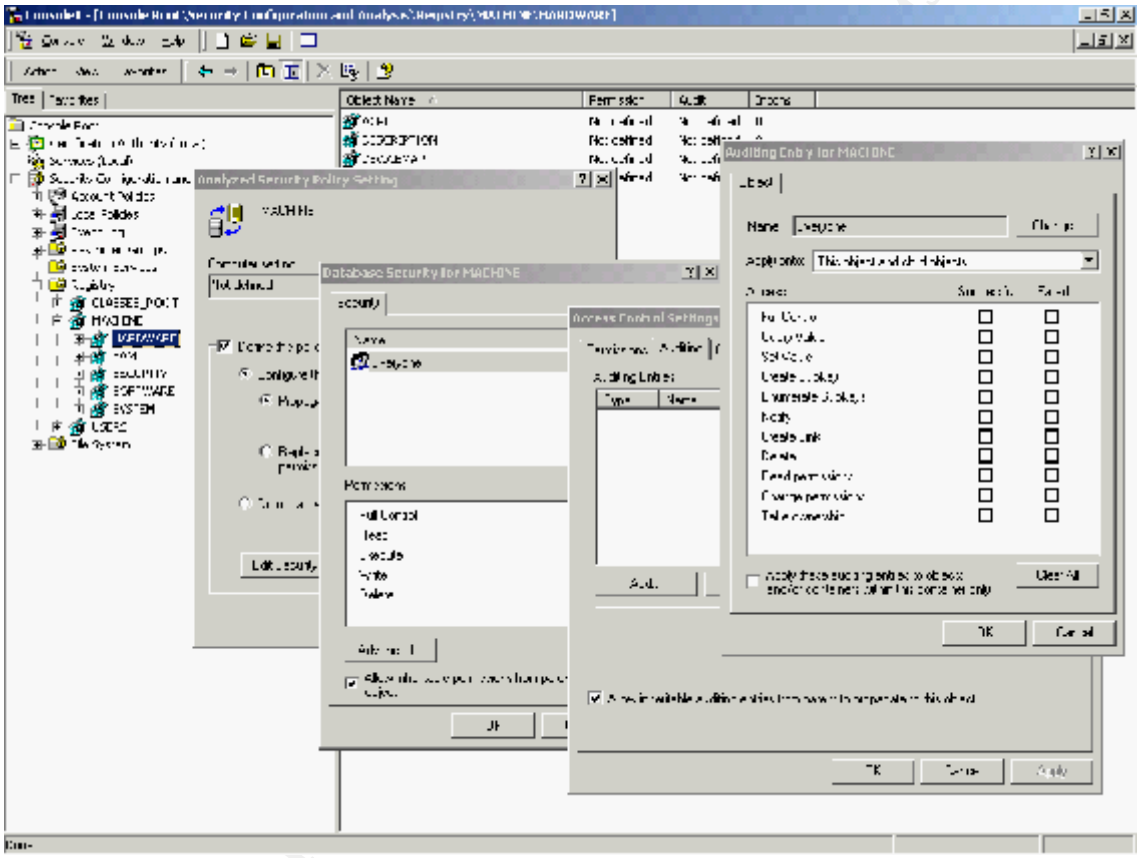
Optional due to the limited number of authorized users. Consult the CP/CPS.

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

- **Object Access Auditing (Enhancing system integrity)**

Each file or folder listed above may be audited with an extra click on the "Advanced" button. This is yet another excellent way to ensure the integrity of the SaORCA platform and SaORCA operations.

Enable auditing by simply selecting a container file or folder, selecting the user(s) whose actions are to be audited, and then choose the actions to be audited, (such as attempts to delete the same object).



- **Certificate Services Auditing**

From the Systems Services container you can identify Certificate Services for auditing: Audit for **Success and Failure.**

Many of the SaORCA objects may be selected for audit to enhancing system integrity.

Consult the CP/CPS, (and other security policy), for CA object auditing guidance.

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

- **Systems Utilities Auditing**

Windows 2000 server comes with a number of powerful executables that perform sensitive administrative activities. To enhance SaORCA integrity audit the following utilities for success and failure:

Registry Executable
\%System Root%\regedit32.exe

Command Scheduling Executable (lists schedules commands and programs)
\%System Root%\system32\at.exe

Backup Functions Executable
\%System Root%\system32\ntbackup.exe

Permissions Executable (allows access to additional permissions from current logon)
\%System Root%\system32\runas.exe

System Security Executable
\%System Root%\system32\secedit.exe

Additional Encryption Executable
\%System Root%\system32\syskey.exe

- **Startup Programs Auditing (Optional)**

Many of following registry keys and files can automatically launch programs when the machine boots. The "mmc" snap-in permits auditing assignment for most of these entries:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce\

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

Startup Programs Auditing (Continued)

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run

%systemroot%\win.ini

%systemroot%\Profiles\All Users\Start Menu\Programs\Startup

%systemroot%\Profiles\Administrator\Start Menu\Programs\Startup

Assigning permissions to any (and all) of the above keys and files will provide an excellent extra layer of protection.

Note: Effective Permissions and Auditing must be well planned and well documented!

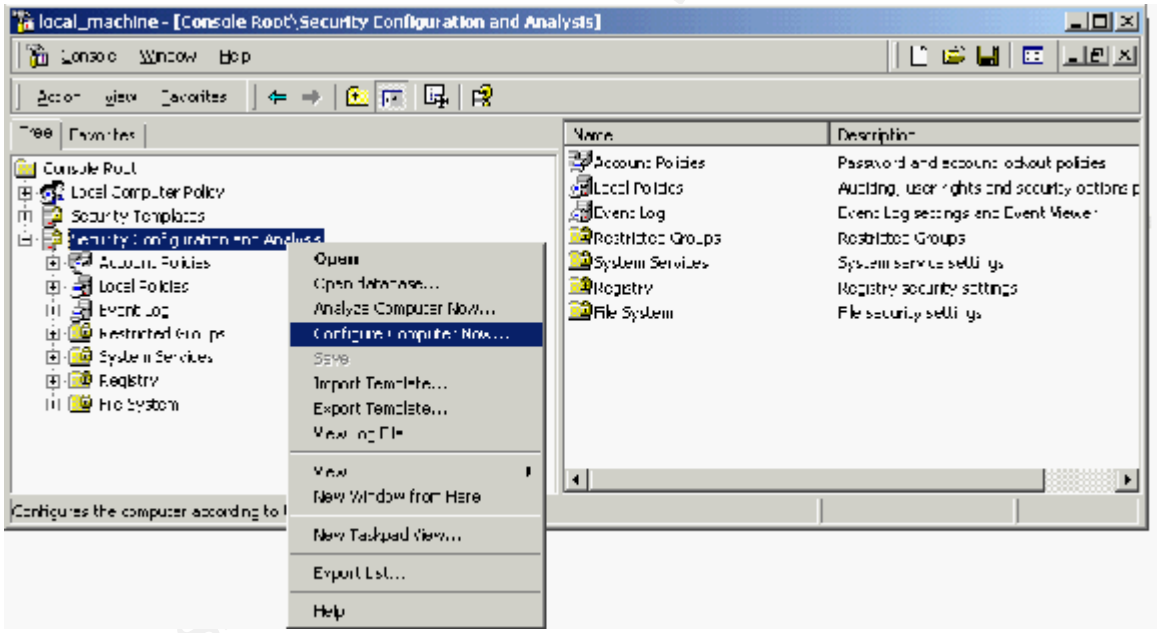
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Part 4c: Save and Implement SaORCAHiSec.inf Template

IMPORTANT!

- **Save SaORCAHiSec.inf settings**
  - Right Click on Security Analysis and Configuration Container and select Save.
  - Right Click on Security Analysis and Configuration Container and Export Template and select to replace SaORCAHiSec.inf

- **Implement SaORCAHiSec.inf settings**
  - Right Click on Security Analysis and Configuration Container and select Configure Now.



Note: Once the SaORCA has been configured with the newly created template logoff, reboot, logon, and verify all protection features have been implemented.

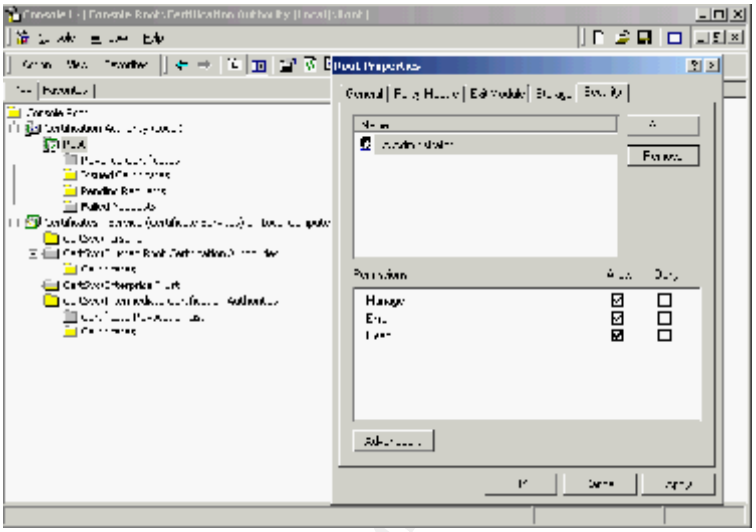
DO NOT FORGET… Before logging off,…
make sure the CA Administrator password is in compliance with new password policy!

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

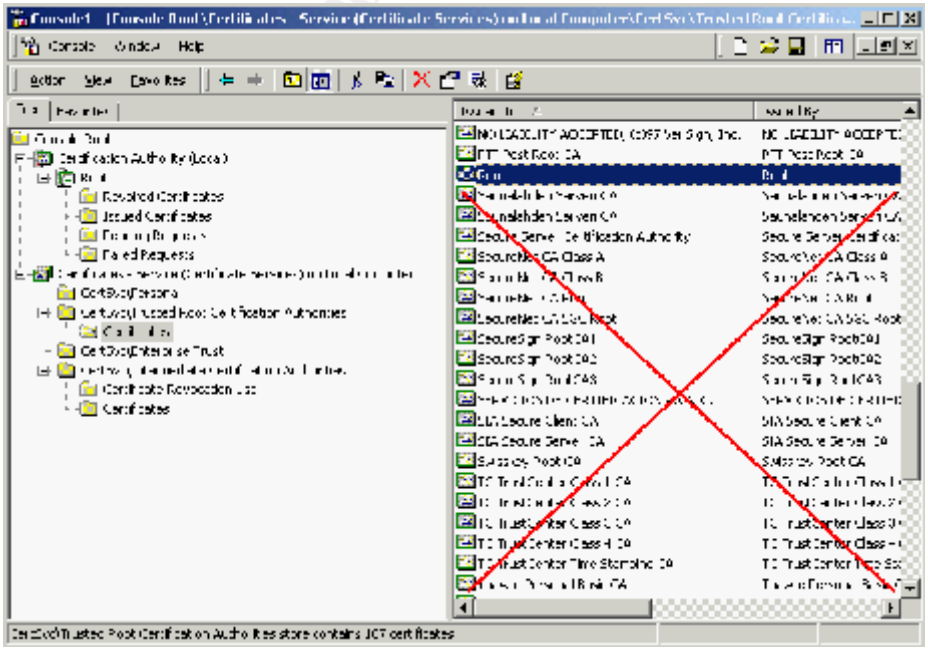
Part 5: Certificate Authority Protection

- **Grant appropriate permissions.**

The CA Administrator is granted manage, enroll and read permissions while a CA Operator is granted enroll and read permissions. All others granted read. Consult CP/CPS for additional guidance.



- **Remove all Trusted Root and Intermediate Certificates that are not needed.**



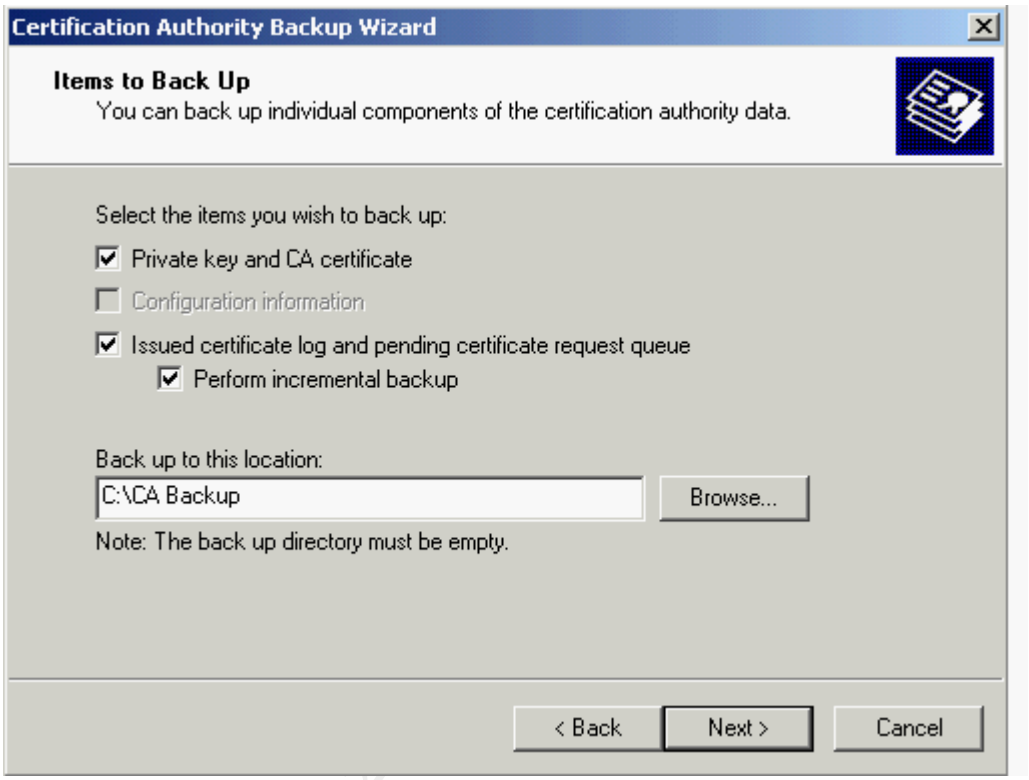
Note: Certain Certificates are required to load software, i.e., Microsoft intermediate certificates are used to verify Iomega drivers for compatibility with Windows 2000.

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

Part 6: Backup and Recovery Security Procedures

- **Back up Certificate Authority Key, Certificate, Log and Queue.**

The CP/CPS will offer further guidance on regular backup of the SaORCA.



- **Back up appropriate Folders and Files at regular intervals**

The CP/CPS will offer further guidance on scheduling and procedures for regular backup of the SaORCA. CA Administrators and CA Backup Operators must be familiar with policy and procedure concerning SaORCA backup and disaster recovery.

Folders to backup Daily (or as required by CP/CPS):

- \%System Root%\system32\Certlog
- \%System Root%\system32\Config
- \%System Root%\repair
- \CA Backup

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

- **Emergency Repair Disk (ERD)**

The ERD must be updated whenever a change to the SaORCA's configuration takes place, (files, partition boot sector, startup environment, etc.). The ERD must be backed up.

Windows 2000 Backup and Recovery Tools are used to back up necessary folders and files in accordance with the CP/CPS.

- **Secure and Protect Backup Media**

All backup Media, (folders, files, and ERD files), must be treated with the same level of protection as the primary SaORCA items. The media must be stored in a secure alternate location at least 25 Miles from the primary SaORCA.

(Back up media is great as long as it is not destroyed along with the original.)

- **Keep the primary ERD protected at the same level as the SaORCA.**

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

References

Securing Windows NT Security, Step by Step, By Jason Fossen, The SANS Institute GIAC Training, 2001

Windows 2000: PKI, By Jason Fossen, The SANS Institute GIAC Training, 2001

Windows 2000 Active Directory and Group Policy, By Jason Fossen, The SANS Institute GIAC Training, 2001

Applied Cryptography, Second Edition. By Bruce Schneier, John Wiley & Sons, 1996.

Hardening Windows 2000 Advanced Server for Internet Participation, by Andy Brock, March 2001

The Windows 2000 Server Deployment and Planning Guide (from the Windows 2000 Resource Kit) http://www.microsoft.com/technet/win2000/dguide/home.asp

Chapter 11 - Planning Distributed Security - (see Deploying Secure Applications) - http://www.microsoft.com/technet/win2000/dguide/chapt-11.asp

Chapter 12 - Planning Your Public Key Infrastructure - http://www.microsoft.com/technet/win2000/dguide/chapt-12.asp

Windows 2000 Installation Security Checklist
htttp://www.labmice.net/articles/securingwin2000.htm

Step-by-Step Guide to a Common Infrastructure for Windows 2000 Server Deployment. Part One: Installing a Windows 2000 Server as a Domain Controller - http://www.microsoft.com/technet/win2000/depprof1.asp

Checklist: Performing a new W2K Server installation
http://windows.microsoft.com/windows2000/en/server/help/checklist_preparing_for_a_new_installation.htm

Internet X.509 Public Key Infrastructure Certificate and CRL Profile, The PKIX Working Group, IETF
http://www.ietf.cnri.reston.va.us/rfc/rfc2459.txt

Step-by-Step Guide to Setting up a Certification Authority
http://www.microsoft.com/windows2000/library/planning/security/casetupsteps.asp

Checklist: Creating a certification hierarchy with an offline root certification authority
http://windows.microsoft.com/windows2000/en/server/help/sag_CS_Checklist_Offline.htm

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

Last Updated: May 26th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
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**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 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 San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**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 Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**