Global Information Assurance Certification Paper

Usefulness and Shortcomings of the Preconfigured Security Policy Templates that are Included with Windows 2000

Robert Huie

GCNT Practical Assignment

Capital SANS 2000

Washington DC

December 2000

Table of Contents

List of Figures and Tables

1 Scope

The purpose of this document is to provide an overview of the usefulness and shortcomings of the security policy templates that are provided with Windows 2000 (Win2K).

Win2K provides a set of tools called the Security Configuration Tool Set to analyze, configure, and distribute these security policy templates. With this tool set the Account Policies, Local Policies, Event Log Settings, Group Member Control, System Registry Settings, and the File System settings, can all be analyzed and edited for use.

Win2k is packaged with several security policy templates. The main policy templates are pre-fixed with either basic, hisec (Highly Secure Environment), or secure (Secure Environment). These represent the level of security desired. These pre-fixes are then followed by wk (Professional / Workstation), ws (Professional / Workstation), sv (Server), or dc (Domain Controller). This document will focus more on these templates rather than the other additional templates. The Account Polices, Local Policies, and Event Log policies will be analyzed more in depth than the file and registry permissions.

2 Security Configuration Tool Set

The Security Configuration Tool Set consists of several components.

The Security Templates Snap-In, is an MMC snap-in that enables you to create, edit, and save security configurations.

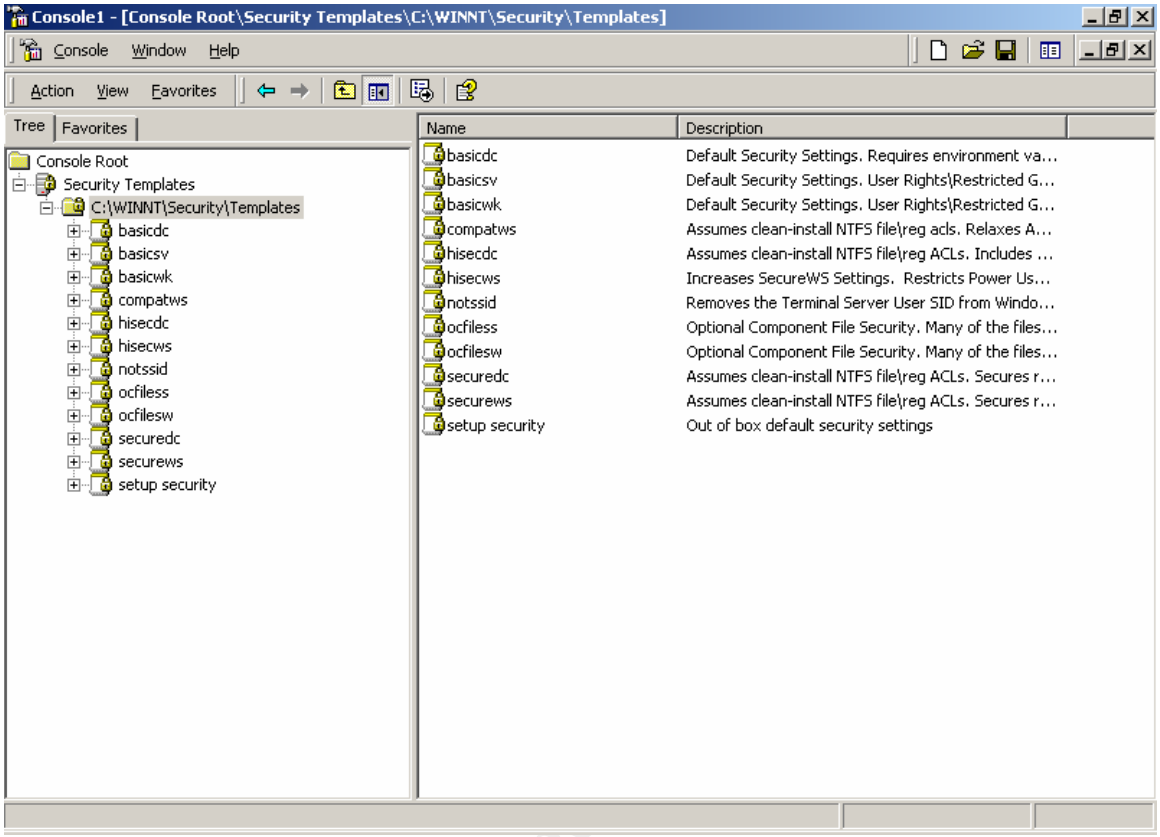

Figure 2.1 Security Configuration Tool Set

The Security Configuration And Analysis Snap-in, is an MMC snap-in that allows you to perform several operations. With this tool you can import a template into a database for analysis. You can then apply the imported configuration to the computer or analyze the configuration against the current configuration of the computer.

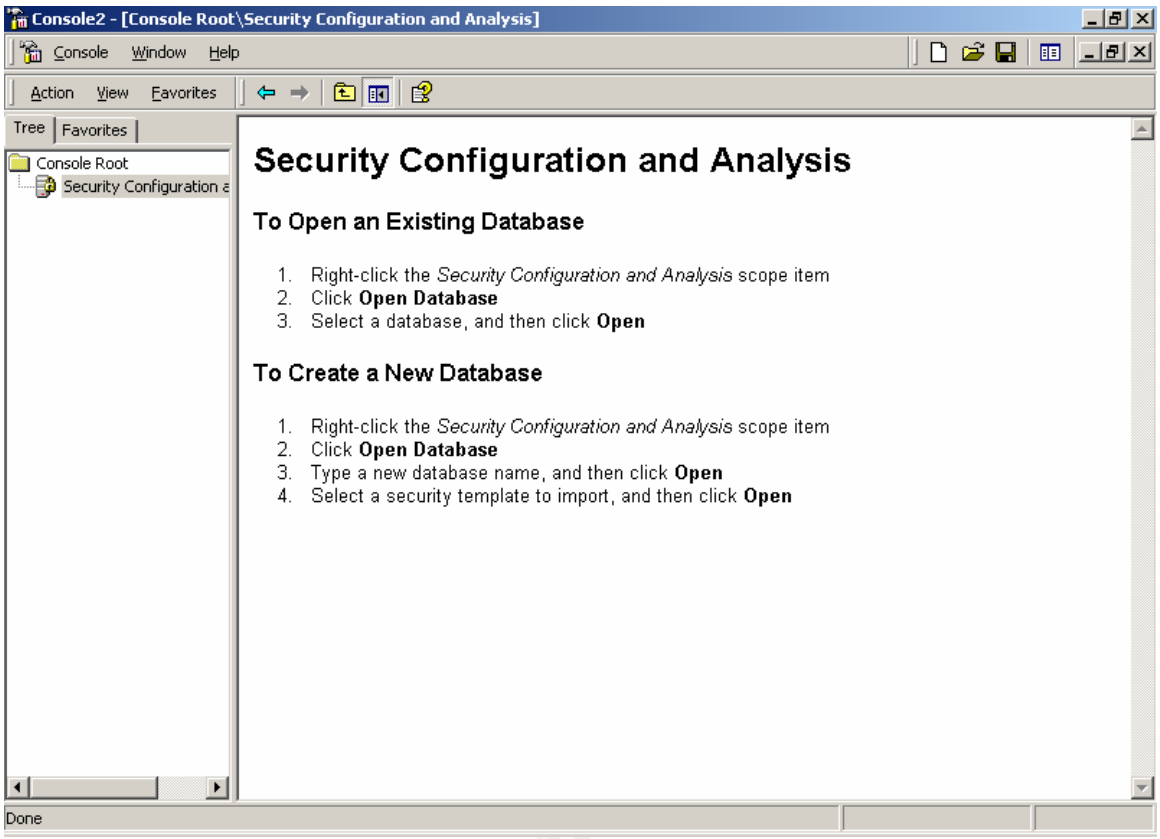

Figure 2.2 Security Configuration Analysis

The Security Settings extension is a snap-in tool that extends the Groups Policy editor. It allows you to define a security configuration as part of a Group Policy Object (GPO). With this add on a security template can be applied to a specific computer, domain or an organization unit (OU), as a GPO.

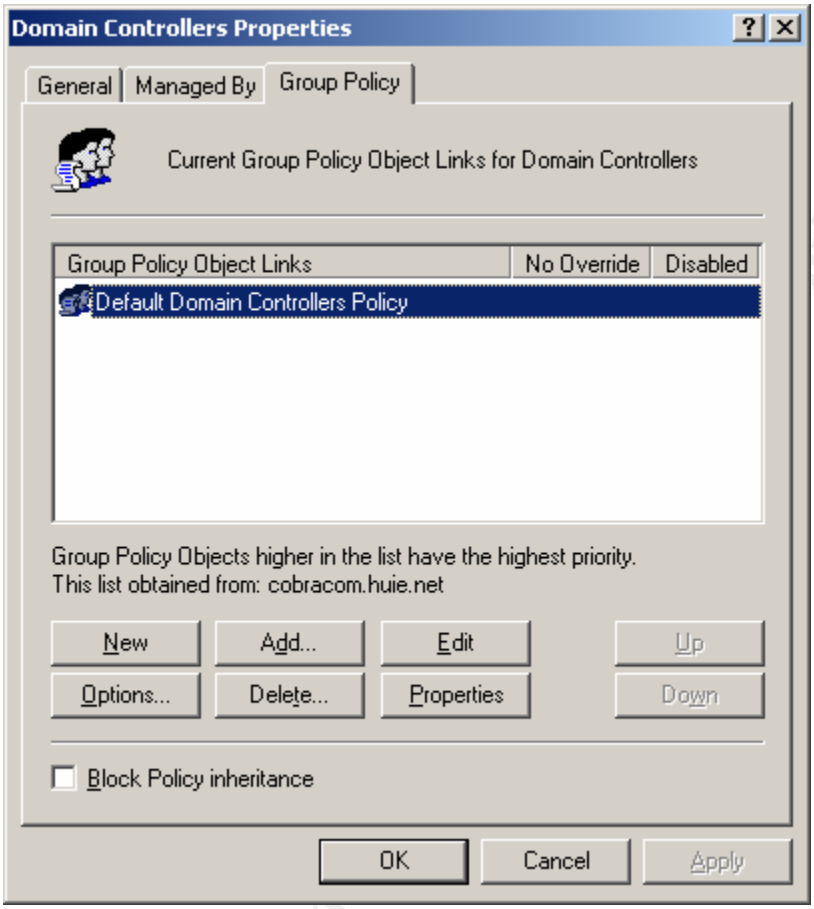

Figure 2.3 Group Policy Editor Extension

The Secedit.exe (secedit) command-line tool is a command line that allows you to perform configuration and analysis functions without the use of the snap-ins described above.

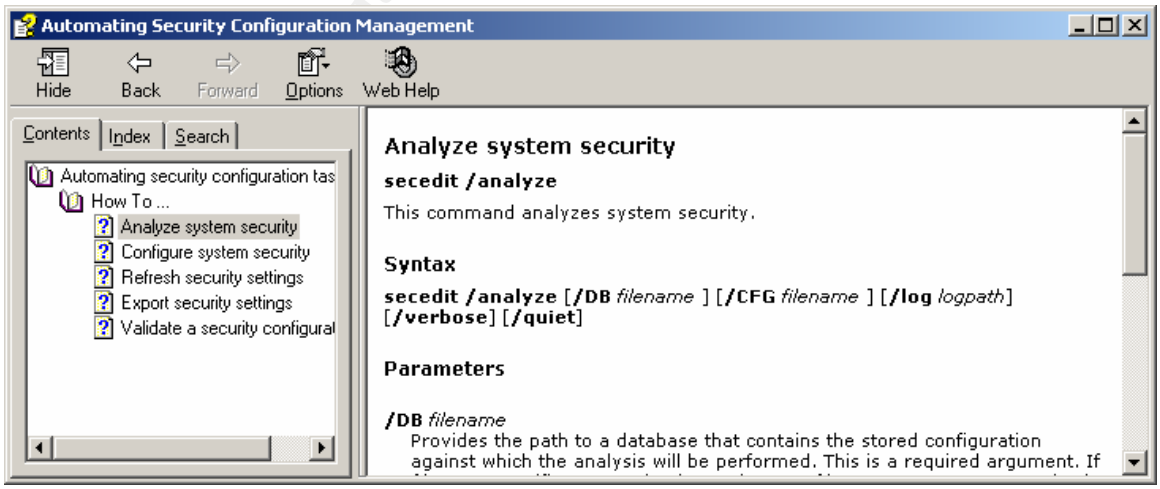

Figure 2.4 Help Screen for Secedit.exe

3 Security Policy Templates

Within the security policy templates each policy is categorized according to policy.

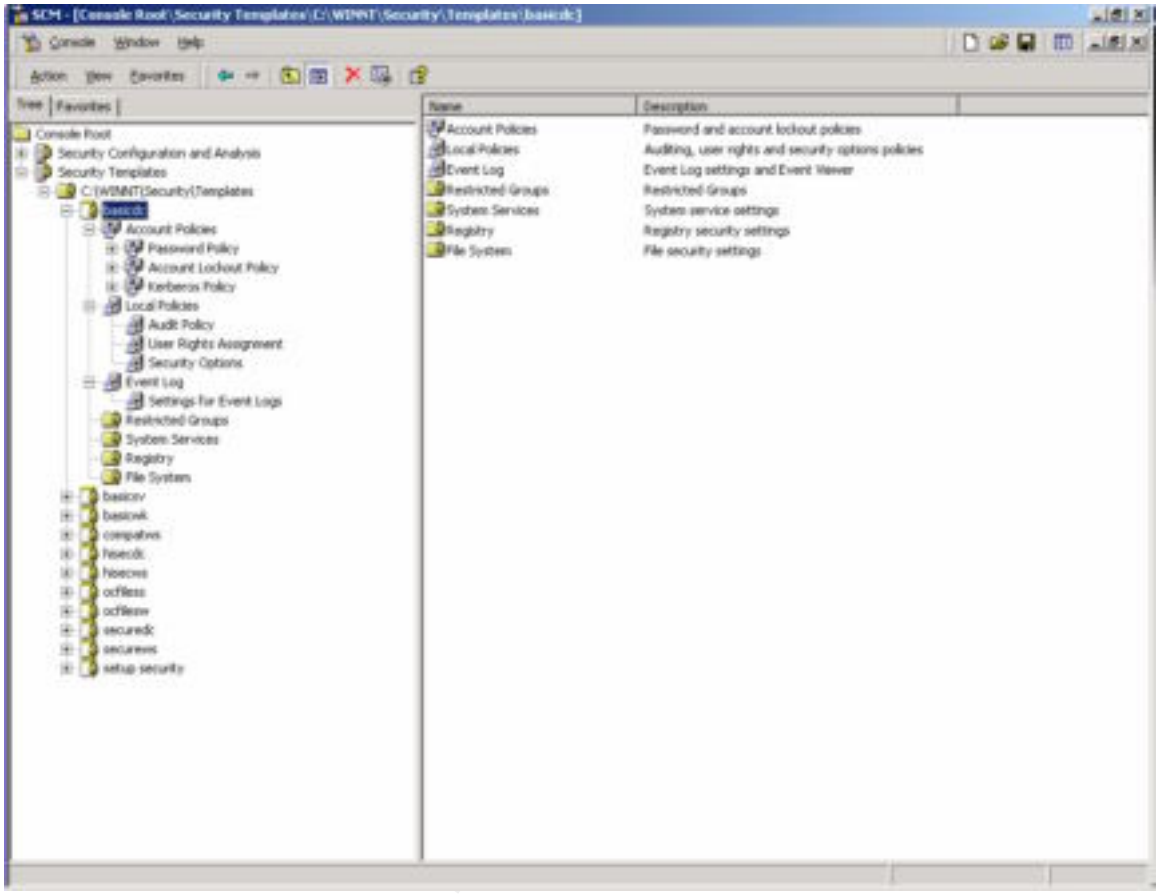

Figure 3.1 Policy Categories

The Account Policies section sets the policies for passwords, account and kerberos. From the Password Policy section sets the password history, maximum age, minimum age, length, complexity, and reversible encryption. The Account Lockout Policy section sets the lockout duration, threshold, and counter. The Kerberos Policy section sets the logon restrictions, maximum lifetime for service ticket, maximum lifetime for user ticket, maximum lifetime for user ticket renewal, and maximum tolerance for computer clock synchronization.

The Local Policies section sets the policies for auditing, user rights assignment, and security options. The Audit Policy sets the policy for what types of events are to be audited. The User Rights Assignment sets the policy for user rights to the computer. Rights such as log on locally or logon as service. The Security Options sets the policy for options that can be located in the registry. Registry settings such as a warning or log on text option.

The Event Log Policy sets the policy for the event viewer. From this section, the log sizes for each event can be set. Guest access to the event logs can be restricted or granted from this policy. The duration of how long the logs are retained can be established. The retention method from this policy, can be set to overwrite by days, overwrite as needed, or to clear logs manually. Finally the computer can be set to shutdown when the event logs are full.

The Restricted Groups section allows for the control of group membership to groups that may have sensitive capabilities such as Administrators, Server Operators, Power Users, etc…

From the Systems Services section, the policy for how servers are started and which account has permissions to log on as the service can be set. The predefined services can be set to start Automatic, Manual, or Disable.

The Registry section, sets the policy for permissions assigned to registry keys.

The File System section, sets the policy for permissions assigned to the file system.

For the Registry and File System policy the predefined keys and files are not limited. More keys and files can be added to the policy.

4 Windows 2000 Pre-Defined Security Policy Templates

The policies that are included with Windows 2000 are meant to be applied incrementally (Q234926). They should be applied to a cleanly installed Windows 2000 computer, and not an upgraded computer from Windows NT 4.0. In an upgrade from Windows NT 4.0 to Windows 2000, the security settings are kept from the previous version of the operating system.

The default security policy templates contain three separate templates for each type of computer, a basic policy, a secure policy, and a high-security policy. Each policy contains the word basic, secur, or hisec then followed by wk (Professional / Workstation), ws (Professional / Workstation), sv (Server), or dc (Domain Controller). For example a basic policy for workstation would be basicwk.

Table 4.1 shows a breakdown of all the default templates that are included with Windows 2000:

Template Name	*Description*
basicdc	Default Security Settings. Windows 2000 Domain Controller
basicsv	Default Security Settings. Windows 2000 Server
basicwk	Default Security Settings. Windows 2000 Professional
compatws	Assumes clean-install NTFS fil\reg acls. Relaxes ACL's for Users
hisecdc	Assumes clean-install NTFS fil\reg acls. Includes SecureDC settings with Windows 2000-only enhancements

hisecws	Increases SecureWS settings. Restrices Power User and Terminal Server ACLs
octfiless	Optional Component File Security
octfilesw	Optional Component File Security
securedc	Assumes clean-install NTFS fil\reg acls. Secures remaining areas.
securews	Assumes clean-install NTFS fil\reg acls. Secures remaining areas.
setup security	Out of box default security settings

Table 4.1 Default Windows 2000 Security Templates

4.1 Workstation Security Policy Templates

The table below shows the basic, secure, and high-security policies for the Account, Local, and Event Log policies, of a workstation:

	Basic Workstation	***Secure Workstation***	***High-Security Workstation***
Account Policies			
Password Policy			
Enforce password history	0 passwords remembered	24 passwords remembered	24 passwords remembered
(PasswordHistorySize)			
Maximum password age	42 days	42 days	42 days
(MaximumPasswordAge)			
Minimum password age	0 days	2 days	2 days
(MinimumPasswordAge)			
Minimum password length	0 characters	8 characters	8 characters
(MinimumPasswordLength)			
Passwords must meet complexity requirements (PasswordComplexity)	Disabled	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled	Disabled
Account Lockout Policy			
Account lockout duration	Not defined	30 minutes	0
(LockoutDuration)			
Account lockout threshold (LockoutBadCount)	0 invalid logon attempts	5 invalid Logon attempts	5 invalid Logon attempts
Reset account lockout counter after (ResetLockoutCount)	Not defined	30 minutes	30 minutes
Local Policies			
Audit Policy			
Audit account logon events	No auditing	Success/Failure	Success/Failure
(AuditAccountLogon)			
Audit account management	No auditing	Success/Failure	Success/Failure
(AuditAccountManage)			
Audit directory services access	Not defined	Not defined	Not defined
(AuditDSAccess)			

Audit Logon events	No auditing	Failure	Success/Failure
(AuditLogonEvents)			
Audit object access	No auditing	No auditing	Success/Failure
(AuditObjectAccess)			
Audit policy change	No auditing	Success/Failure	Success/Failure
(AuditPolicyClaange)			
Audit privilege use	No auditing	Failure	Success/Failure
(AuditPrivilegeUse)			
Audit process tracking	No auditing	No auditing	No auditing
(AuditProcessTracking)			
Audit system events	No auditing	No auditing	Success/Failure
(AuditSystemEvents)			
User Rights			
Access this computer from the network	Not defined	Not defined	Not defined
Act as part of the operating system	Not defined	Not defined	Not defined
Add workstations to the domain	Not defined	Not defined	Not defined
Backup Files & Directories	Not defined	Not defined	Not defined
Bypass traverse checking	Not defined	Not defined	Not defined
Change system time	Not defined	Not defined	Not defined
Create a Token Object	Not defined	Not defined	Not defined
Create Pagefile	Not defined	Not defined	Not defined
Create Permanent Shared Objects	Not defined	Not defined	Not defined
Debug Programs	Not defined	Not defined	Not defined
Deny access to this computer from the network	Not defined	Not defined	Not defined
Deny logon as a batch job	Not defined	Not defined	Not defined
Deny logon as a service	Not defined	Not defined	Not defined
Deny logon locally	Not defined	Not defined	Not defined
Enable computer and user accounts to be trusted for delagation	Not defined	Not defined	Not defined
Force shutdown from a remote system	Not defined	Not defined	Not defined
Generate security audits	Not defined	Not defined	Not defined
Increase Quotas	Not defined	Not defined	Not defined
Increase Scheduling Priority	Not defined	Not defined	Not defined
Load and unload device drivers	Not defined	Not defined	Not defined
Lock Pages in Memory	Not defined	Not defined	Not defined
Log on Locally	Not defined	Not defined	Not defined
Logon as a batch job	Not defined	Not defined	Not defined
Logon as a service	Not defined	Not defined	Not defined
Manage auditing & security log	Not defined	Not defined	Not defined
Modify firmware environment variables	Not defined	Not defined	Not defined
Profile a single process	Not defined	Not defined	Not defined
Profile system performance	Not defined	Not defined	Not defined
Replace a process level token	Not defined	Not defined	Not defined
Restore files & directories	Not defined	Not defined	Not defined
Shut down the system	Not defined	Not defined	Not defined
Take ownership of files & other objects	Not defined	Not defined	Not defined

Security options			
Additional restrictions for anonymous connections COMPUTER\System\CurrentControlSet\Control\Lsa\RestrictAnonymous	None: Rely on default permissions	Do not allow enumeration of SAM accounts and shares	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only) COMPUTER\System\CurrentControlSet\Control\Lsa\SubmitControl	Not defined	Not defined	Not defined
Allow system to be shut down without having to log on COMPUTER\Software\Microsoft\Winodws\CurrentVersion\Policies\System\ShutdownWithoutLogon	Enabled	Not defined	Not defined
Allowed to eject removable NTFS media COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD	Administrators	Administrators	Administrators
Amount of idle time required before disconnecting session COMPUTER\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoDisconnect	15 minutes	15 minutes	15 minutes
Audit the access of global system objects COMPUTER\Systern\CurrentControlSet\Control\Lsa\AuditBaseObjects	Disabled	Disabled	Disabled
Audit use of Backup and Restore privilege COMPUTER\System\CurrentControlSet\Control\Lsa\AuditBaseObjects	Disabled	Disabled	Disabled
Automatically log off users when logon time expires COMPUTER\System\CurrentControlSet\Control\Lsa\Services\LanManServer\Parameters\EnableForcedLogOff	Not defined	Not defined	Not defined
Automatically log off users when Logon time expires (local) [Not in the Registry]	Enabled	Enabled	Enabled
Clear virtual memory pagefile when system shuts down COMPUTER\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown	Disabled	Disabled	Enabled
Digitally sign client communication (always) COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature	Disabled	Disabled	Enabled
Digitally sign client communication (when possible) COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature	Enabled	Enabled	Enabled
Digitally sign server communication (always) COMPUTER\System\CurrentControlSet\Services\LanManServer\Parameteres\RequireS	Disabled	Disabled	Enabled

ecuritySignature			
Digitally sign server communication (when possible) COMPUTER\System\CurrentControlSet\Services\LanManServer\Parameteres\EnableSecuritySignature	Disabled	Enabled	Enabled
Disable Ctrl+Alt+Del requirement for to logon *COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD*	Not defined	Disabled	Disabled
Do not display last username in logon screen COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName	Disabled	Disabled	Enabled
LAN Manager Authentication Level COMPUTER\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel	Send LM & NTLM responses	Send NTLM response only	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText			
Message title for users attempting to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption			
Number of previous logons to cache (in case domain controller is not available) COMPUTER\Software\Microsft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount	10 logons	10 logons	10 logons
Prevent system maintenance of computer account password COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange	Disabled	Disabled	Disabled
Prevent users from installing printer drivers COMPUTER\System\CurrentControlSet\Control\PrintProviders\LanMan Print Services\Servers\AddPrinterDrivers	Disabled	Enabled	Enabled
Prompt user to change password before expiration COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpireWarning	14 days	14 days	14 days
Recovery Console: Allow auto-matic administrative logon COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel	Disabled	Disabled	Disabled

Recovery Console: Allow floppy copy and access to all drives and all folders COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand	Disabled	Disabled	Disabled
Rename administrator account [Not in the Registry]	Not defined	Not defined	Not defined
Rename guest account [Not in the Registry]	Not defined	Not defined	Not defined
Restrict CD-ROM access to locally logged-on user only COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms	Disabled	Disabled	Disabled
Restrict floppy access to locally logged-on user only COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies	Disabled	Disabled	Disabled
Secure channel: Digitally encrypt or sign secure channel data (always) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignorSeal	Disabled	Disabled	Enabled
Secure channel: Digitally encrypt secure channel data (when possible) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel	Enabled	Enabled	Enabled
Secure channel: Digitally sign secure channel data (when possible) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel	Enabled	Enabled	Enabled
Secure channel: Require strong (Windows 2000 or later) session key COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey	Disabled	Disabled	Enabled
Secure system partition (for RISC platforms only) [Not in the Registry]	Not defined	Not defined	Not defined
Send unencrypted password to connect to third-parry SMB servers COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword	Disabled	Disabled	Disabled
Shut down system immediately if unable to log security audits COMPUTER\System\CurrentControlSet\Control\Lsa\CrashonAuditFail	Disabled	Disabled	Disabled
Smart card removal behavior COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption	No Action	Lock Workstation	Lock Workstation

Strengthen default permissions of global system objects (e.g. Symbolic Links) COMPUTER\System\CurrentControlSet\Control\Session Manager\ProtectionMode	Enabled	Enabled	Enabled
Unsigned driver installation behavior COMPUTER\Software\Microsoft\Driver Signing\Policy	Not defined	Warn but allow installation	Do not allow installation
Unsigned non-driver installation behavior COMPUTER\Software\Microsoft\Non-Driver Signing\Policy	Not defined	Silently succeed	Silently Succeed
Event Log			
Settings for Event Logs			
Maximum application log size (MaximumLogSize)	512 kilobytes	Not defined	Not defined
Maximum security log size (MaximumLogSize)	512 kilobytes	5120 kilobytes	10240 kilobytes
Maximum system log size(MaximumLogSize)	512 kilobytes	Not defined	Not defined
Restrict guest access to application log (RestrictGuestAccess)	Disabled	Enabled	Enabled
Restrict guest access to security log (RestrictGuestAccess)	Disabled	Enabled	Enabled
Restrict guest access to system log(RestrictGuestAccess)	Disabled	Enabled	Enabled
Retain application log (RetentionDays)	7 days	Not defined	Not defined
Retain security log (RetentionDays)	7 days	Not defined	Not defined
Retain system log (RetentionDays)	7 days	Not defined	Not defined
Retention method of application log (AuditLogRetentionPeriod)	By days	Not defined	Not defined
Retention method for security log (AuditLogRetentionPeriod)	By days	As needed	As needed
Retention method for system log (AuditLogRetentionPeriod)	By days	Not defined	Not defined
Shut down the computer when the security audit log is full (CrashOnAuditFull)	Not defined	Not defined	Not defined

Table 4-2 Workstation Security Policy Templates

4.1.1 Basic Workstation Security Policy Template

Table 4-2 Workstation Security Policy Templates, column two lists the security policy settings involved with using the Basic Template. This template is a very simple template. This template provides some security, but it does not provide the best security.

4.1.1.1 Basic Workstation Account Policies

This template does not enforce a password history. Users may use the same password regardless if they are forced to change their passwords. The minimum password age is set

to 0 days. This setting allows a user to change a password back to an old password after a password change immediately. The password complexity setting is set to disable. With this setting set to disable, a user will be able to choose a password that can be easily compromised with a password cracker. Complex password enforcement would force the user to choose a password that can't be as easily compromised.

For the account lockout policy of this template, there is no lockout policy. Users can try to guess a password for as many times as they want. The accounts will not lockout if there are a certain amount of failed attempts. Having a lockout policy will also slow down a password hacker. If the accounts were locked the hacker would have to wait till the account is reset to try again.

4.1.1.2 Basic Workstation Local Policies

An audit policy is also not defined. No records of any changes to the system or policies will be logged.

The user rights to this template are also listed as not defined. For these settings it will take the default user rights of the computer. Table 4-3, Default User Rights, is listed below:

User Rights	
Access this computer from the network	Everyone, Users, Power Users, Backup Operators, Administrators
Act as part of the operating system	
Add workstations to the domain	
Backup Files & Directories	Backup Operators, Administrators
Bypass traverse checking	Everyone, Users, Power Users, Backup Operators, Administrators
Change system time	Power Users, Administrators
Create a Token Object	
Create Pagefile	Administrators
Create Permanent Shared Objects	
Debug Programs	Administrators
Deny access to this computer from the network	
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	

Enable computer and user accounts to be trusted for delagation	
Force shutdown from a remote system	Administrators
Generate security audits	
Increase Quotas	Administrators
Increase Scheduling Priority	Administrators
Load and unload device drivers	Administrators
Lock Pages in Memory	
Log on Locally	%COMPUTERNAME%\Guest, Users, Power Users, Backup Operators, Administrators, Power Users
Logon as a batch job	
Logon as a service	
Manage auditing & security log	Administrators
Modify firmware environment variables	Administrators
Profile a single process	Power Users, Administrators
Profile system performance	Administrators
Replace a process level token	
Restore files & directories	Backup Operators, Administrators
Shut down the system	Users, Power Users, Backup Operators, Administrators
Take ownership of files & other objects	Administrators

Table 4-3 Default User Rights

User rights will be discussed in depth later in this document.

For the basic workstation security template, the security options allow a user to shut down the computer without logging on. This would allow the user to shut down the computer abnormally without using the computer's normal operating switches. The user may also tend to just turn the computer off with this option allowed, by the policy. No auditing is set for this template, therefore access to internal system object and backup and restore usage rights are not audited. Files and directories may be replaced with out any audit trails. The pagefile is not set to clear for this template. Although the pagefile can be protected by the file system, it may be good to clear the page file as a precautionary. This ensures that sensitive information is not available for malicious use. There is no warning message set for this template. It is best to use a warning message to warn users that they are liable to any changes to their computers.

4.1.1.3 Basic Workstation Event Log

The event logs are set to 512 KB for the system, application and security logs. Logs that are too small may tend to fill up. Administrators will need to clear and save the logs often. The retention days are set to 7 days. 7 days may not be a long enough duration. Security logs may be needed in case of a security breach. They are also set to overwrite by days. Again, overwriting the logs may prevent sufficient evidence collection, in the case of a security breach. The restriction of guest access to the security logs are disabled. This will allow any user to view the events in the event viewer.

4.1.2 Secure Workstation Security Policy Template

The Secure Workstation Security Policy Templates, provides for a little bit more security. Table 4-2, column 3 lists the configuration for the Secure Workstation Security Policy Template.

4.1.2.1 Secure Workstation Account Policies

The secure template provides a better password policy than the basic. The secure template enforces a password history of 24 passwords. This will force the user to use a different password for next 24 passwords when they are requested to change it. The user will also be allowed to change the password after 2 days, which will prevent them from reverting to an old password immediately. There is also a minimum password length of 8 characters. With the enforcement of complex passwords and an 8-character minimum, this policy will hinder hackers from guessing a users password.

This policy sets the account lockout duration to 30 minutes. After 30 attempts the user can try to logon again. A value of 5 for the invalid logon attempts before the account is locked out. After 5 bad attempts to logon the user's account will be locked out. The bad logon count will be reset after 30 minutes. These settings again will hinder a brute-force password cracking / guessing attack.

4.1.2.2 Secure Workstation Local Policies

This template does set an auditing policy. It audits the logon events, account management, object access, audit policy changes, and audit privilege use. This type of auditing only audits security events and not system events. Changes to the system are left untracked.

No user rights are defined for this policy. Therefore the default users rights will be used, for this policy.

These templates are meant to be applied incrementally. Applying just one template with out the other templates may leave a couple of settings unconfigured.

The security option for logging on to shutdown the system is left as undefined. For the basic template the setting is set to disabled. If the basic template were applied before the

secure template, then the setting is configured to disabled. If the secure template were applied by itself, then this setting would be configured from the default setting.

Unlike the basic template, the secure templates prevent a user from installing a print driver. With this option enabled, an administrator will be needed to install a printer driver, when needed. Any abnormal smart card removal behavior will lock the workstation for the secure template. For any unsigned driver, the computer will warn but allow for the installation of an unsigned driver to be installed. An unsigned driver may come from someone with malicious intent that may cause the computer to behave abnormally.

4.1.2.3 Secure Workstation Event Log

The workstation event logs for the secure workstation template increases the size of the security logs to 5120 kilobytes. Restrictions to guest access to the event logs have been enabled. A guest user will not be able to view any event logs unless they are granted permissions. The retention days are not defined, but these templates are assuming that each template will be applied incrementally. The retention method for the security log is set to As needed, this setting will clear the event logs as needed or when they have reached the set log size. This allows for more retention time for review the security logs.

4.1.3 High-Security Workstation Security Policy Template

The high-security workstation security policy template settings are listed in Table 4-2, column 4. These settings are very similar to the secure workstation settings. There are several differences.

4.1.3.1 High-Security Workstation Account Policy

The high-security policy has a password policy that is the same as the secure workstation policy. The policy remembers the previous 24 passwords as its password history. The maximum amount of days before a password needs to be changed is set to 42 days. The password cannot be changed until after 2 days. The password has a minimum length of 8 characters with the password complexity enabled.

There is no lockout duration. The value is set to 0. This means that an account remains locked until an administrator unlocks it. With this value set to zero this may a potential denial of service attack. However the built-in administrator account cannot be locked out.

4.1.3.2 High-Security Workstation Local Policy

Again there are not many differences between the secure policy and the high-security policy. A difference in the audit policy is that success and failure events are audited for Audit logon events, Audit object access, Audit privilege use, and Audit system events. This policy sets a more detailed auditing policy. This policy not only audits security events but systems events too. With these settings shutdown, startup and service events will be kept.

For the security options a couple of changes to the secure policy are seen. The pagefile.sys is set to clear at shutdown. This setting ensures that sensitive information in

the pagefile.sys is cleared is the pagefile.sys were to be compromised. All communications channels are set to digitally signed and encrypted. The username of the last person to logon is set to not display for this policy. This setting prevents a person from knowing if a computer is frequently used for system administration. Unsigned drivers are not allowed to be installed.

4.1.3.3 High-Security Workstation Event Log Policy

For the event policy, the security log is increased from 5120 kilobytes, on the secure policy, to 10240 kilobytes, on the high security settings. This allows larger amount of data to be kept before it is cleared. The logs are retained for 7 days. The security logs are cleared only as needed. These settings allow for sufficient evidence collection.

4.2 Server Security Policy Templates

The server security policy templates are similar to the workstation policies. The table for the basic template is listed in Table 4.4 for review. The default templates contain only a basic template for a server configuration.

	Basic Server
Account Policies	
Password Policy	
Enforce password history	0 passwords remembered
(PasswordHistorySize)	
Maximum password age	42 days
(MaximumPasswordAge)	
Minimum password age	0 days
(MinimumPasswordAge)	
Minimum password length	0 characters
(MinimumPasswordLength)	
Passwords must meet complexity requirements (PasswordComplexity)	Disabled
Store password using reversible encryption for all users in the domain	Disabled
Account Lockout Policy	
Account lockout duration	Not defined
(LockoutDuration)	
Account lockout threshold (LockoutBadCount)	0 invalid logon attempts
Reset account lockout counter after (ResetLockoutCount)	Not defined
Local Policies	
Audit Policy	
Audit account logon events	No auditing
(AuditAccountLogon)	
Audit account management	No auditing
(AuditAccountManage)	
Audit directory services access	Not defined
(AuditDSAccess)	
Audit Logon events	No auditing
(AuditLogonEvents)	
Audit object access	No auditing
(AuditObjectAccess)	
Audit policy change	No auditing
(AuditPolicyClaange)	
Audit privilege use	No auditing
(AuditPrivilegeUse)	
Audit process tracking	No auditing
(AuditProcessTracking)	
Audit system events	No auditing
(AuditSystemEvents)	
User Rights	
Access this computer from the network	Not defined
Add workstations to the domain	Not defined

Backup Files & Directories	Not defined
Bypass traverse checking	Not defined
Change system time	Not defined
Create a Token Object	Not defined
Create Pagefile	Not defined
Create Permanent Shared Objects	Not defined
Debug Programs	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 Device Drivers	Not defined
Lock Pages in Memory	Not defined
Log on Locally	Not defined
Logon as a batch job	Not defined
Logon as a service	Not defined
Manage auditing & security log	Not defined
Modify firmware environment variables	Not defined
Profile a single process	Not defined
Profile system performance	Not defined
Replace a process level token	Not defined
Restore files & directories	Not defined
Shut down the system	Not defined
Take ownership of files & other objects	Not defined
Security options	
Additional restrictions for anonymous connections COMPUTER\System\CurrentControlSet\Control\Lsa\RestrictAnonymous	None: Rely on default permissions
Allow server operators to schedule tasks (domain controllers only) COMPUTER\System\CurrentControlSet\Control\Lsa\SubmitControl	Not defined
Allow system to be shut down without having to log on COMPUTER\Software\Microsoft\Winodws\CurrentVersion\Policies\System\ShutdownWithoutLogon	Disabled
Allowed to eject removable NTFS media COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD	Administrators
Amount of idle time required before disconnecting session COMPUTER\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoDisconnect	15 minutes
Audit the access of global system objects COMPUTER\Systern\CurrentControlSet\Control\Lsa\AuditBaseObjects	Disabled
Audit use of Backup and Restore privilege COMPUTER\System\CurrentControlSet\Control\Lsa\AuditBaseObjects	Disabled

Automatically log off users when logon time expires COMPUTER\System\CurrentControlSet\Control\Lsa\Services\LanManServer\Parameters\EnableForcedLogOff	Not defined
Automatically log off users when Logon time expires (local) [Not in the Registry]	Enabled
Clear virtual memory pagefile when system shuts down COMPUTER\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown	Disabled
Digitally sign client communication (always) COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature	Disabled
Digitally sign client communication (when possible) COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature	Enabled
Digitally sign server communication (always) COMPUTER\System\CurrentControlSet\Services\LanManServer\Parameteres\RequireSecuritySignature	Disabled
Digitally sign server communication (when possible) COMPUTER\System\CurrentControlSet\Services\LanManServer\Parameteres\EnableSecuritySignature	Disabled
Disable Ctrl+Alt+Del requirement for to logon COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD	Disabled
Do not display last username in logon screen COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName	Disabled
LAN Manager Authentication Level COMPUTER\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel	Send LM & NTLM responses
Message text for users attempting to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	
Message title for users attempting to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	
Number of previous logons to cache (in case domain controller is not available) COMPUTER\Software\Microsft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount	10 logons
Prevent system maintenance of computer account password COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange	Disabled
Prevent users from installing printer drivers COMPUTER\System\CurrentControlSet\Control\PrintProviders\LanMan Print Services\Servers\AddPrinterDrivers	Enabled

Prompt user to change password before expiration COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpireWarning	14 days
Recovery Console: Allow auto-matic administrative logon COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand	Disabled
Rename administrator account [Not in the Registry]	Not defined
Rename guest account [Not in the Registry]	Not defined
Restrict CD-ROM access to locally logged-on user only COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms	Disabled
Restrict floppy access to locally logged-on user only COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies	Disabled
Secure channel: Digitally encrypt or sign secure channel data (always) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignorSeal	Disabled
Secure channel: Digitally encrypt secure channel data (when possible) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel	Enabled
Secure channel: Digitally sign secure channel data (when possible) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel	Enabled
Secure channel: Require strong (Windows 2000 or later) session key COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey	Disabled
Secure system partition (for RISC platforms only) [Not in the Registry]	Not defined
Send unencrypted password to connect to third-parry SMB servers COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword	Disabled
Shut down system immediately if unable to log security audits COMPUTER\System\CurrentControlSet\Control\Lsa\CrashonAuditFail	Disabled
Smart card removal behavior COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption	No Action

Strengthen default permissions of global system objects (e.g. Symbolic Links) COMPUTER\System\CurrentControlSet\Control\Session Manager\ProtectionMode	Enabled
Unsigned driver installation behavior COMPUTER\Software\Microsoft\Driver Signing\Policy	Not defined
Unsigned non-driver installation behavior COMPUTER\Software\Microsoft\Non-Driver Signing\Policy	Not defined
Event Log	
Settings for Event Logs	
Maximum application log size (MaximumLogSize)	512 kilobytes
Maximum security log size (MaximumLogSize)	512 kilobytes
Maximum system log size(MaximumLogSize)	512 kilobytes
Restrict guest access to application log (RestrictGuestAccess)	Disabled
Restrict guest access to security log (RestrictGuestAccess)	Disabled
Restrict guest access to system log(RestrictGuestAccess)	Disabled
Retain application log (RetentionDays)	7 days
Retain security log (RetentionDays)	7 days
Retain system log (RetentionDays)	7 days
Retention method of application log (AuditLogRetentionPeriod)	By days
Retention method for security log (AuditLogRetentionPeriod)	By days
Retention method for system log (AuditLogRetentionPeriod)	By days
Shut down the computer when the security audit log is full (CrashOnAuditFull)	Disabled

Table 4.4 Server Security Policy Templates

4.3 Domain Controller Security Policy Templates

The domain controller security policy templates are similar to the workstation and server policies. The table for the basic, secure, and high-security templates are listed in Table 5.4 for review.

	Basic Domain Controller	***Secure Domain Controller***	***High-Security Domain Controller***
Account Policies			
Password Policy			
Enforce password history	0 passwords remembered	24 passwords remembered	24 passwords remembered
(PasswordHistorySize)			
Maximum password age	42 days	42 days	42 days
(MaximumPasswordAge)			
Minimum password age	0 days	2 days	2 days

(MinimumPasswordAge)			
Minimum password length	0 characters	8 characters	8 characters
(MinimumPasswordLength)			
Passwords must meet complexity requirements (PasswordComplexity)	Disabled	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled	Disabled
Account Lockout Policy			
Account lockout duration	Not defined	30 minutes	0
(LockoutDuration)			
Account lockout threshold (LockoutBadCount)	0 invalid logon attempts	5 invalid Logon attempts	5 invalid Logon attempts
Reset account lockout counter after (ResetLockoutCount)	Not defined	30 minutes	30 minutes
Local Policies			
Audit Policy			
Audit account logon events	No auditing	Success/Failure	Success/Failure
(AuditAccountLogon)			
Audit account management	No auditing	Success/Failure	Success/Failure
(AuditAccountManage)			
Audit directory services access	Not defined	Not defined	Not defined
(AuditDSAccess)			
Audit Logon events	No auditing	Failure	Success/Failure
(AuditLogonEvents)			
Audit object access	No auditing	No auditing	Success/Failure
(AuditObjectAccess)			
Audit policy change	No auditing	Success/Failure	Success/Failure
(AuditPolicyClaange)			
Audit privilege use	No auditing	Failure	Success/Failure
(AuditPrivilegeUse)			
Audit process tracking	No auditing	No auditing	No auditing
(AuditProcessTracking)			
Audit system events	No auditing	No auditing	Success/Failure
(AuditSystemEvents)			
User Rights			
Access this computer from the network	Not defined	Not defined	Not defined
Add workstations to the domain	Not defined	Not defined	Not defined
Backup Files & Directories	Not defined	Not defined	Not defined
Bypass traverse checking	Not defined	Not defined	Not defined
Change system time	Not defined	Not defined	Not defined
Create a Token Object	Not defined	Not defined	Not defined
Create Pagefile	Not defined	Not defined	Not defined
Create Permanent Shared Objects	Not defined	Not defined	Not defined
Debug Programs	Not defined	Not defined	Not defined
Force shutdown from a remote system	Not defined	Not defined	Not defined
Generate security audits	Not defined	Not defined	Not defined

Increase Quotas	Not defined	Not defined	Not defined
Increase Scheduling Priority	Not defined	Not defined	Not defined
Load Device Drivers	Not defined	Not defined	Not defined
Lock Pages in Memory	Not defined	Not defined	Not defined
Log on Locally	Not defined	Not defined	Not defined
Logon as a batch job	Not defined	Not defined	Not defined
Logon as a service	Not defined	Not defined	Not defined
Manage auditing & security log	Not defined	Not defined	Not defined
Modify firmware environment variables	Not defined	Not defined	Not defined
Profile a single process	Not defined	Not defined	Not defined
Profile system performance	Not defined	Not defined	Not defined
Replace a process level token	Not defined	Not defined	Not defined
Restore files & directories	Not defined	Not defined	Not defined
Shut down the system	Not defined	Not defined	Not defined
Take ownership of files & other objects	Not defined	Not defined	Not defined
Security options			
Additional restrictions for anonymous connections COMPUTER\System\CurrentControlSet\Control\Lsa\RestrictAnonymous	None: Rely on default permissions	Do not allow enumeration of SAM accounts and shares	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only) COMPUTER\System\CurrentControlSet\Control\Lsa\SubmitControl	Not defined	Not defined	Not defined
Allow system to be shut down without having to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon	Disabled	Not defined	Not defined
Allowed to eject removable NTFS media COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD	Administrators	Administrators	Administrators
Amount of idle time required before disconnecting session COMPUTER\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoDisconnect	15 minutes	15 minutes	15 minutes
Audit the access of global system objects COMPUTER\Systern\CurrentControlSet\Control\Lsa\AuditBaseObjects	Disabled	Disabled	Disabled
Audit use of Backup and Restore privilege COMPUTER\System\CurrentControlSet\Control\Lsa\AuditBaseObjects	Disabled	Disabled	Disabled

Automatically log off users when logon time expires COMPUTER\System\CurrentControlSet\Control\Lsa\Services\LanManServer\Parameters\EnableForcedLogOff	Not defined	Not defined	Not defined
Automatically log off users when Logon time expires (local) [Not in the Registry]	Enabled	Enabled	Enabled
Clear virtual memory pagefile when system shuts down COMPUTER\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown	Disabled	Disabled	Enabled
Digitally sign client communication (always) COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature	Disabled	Disabled	Enabled
Digitally sign client communication (when possible) COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature	Enabled	Enabled	Enabled
Digitally sign server communication (always) COMPUTER\System\CurrentControlSet\Services\LanManServer\Parameteres\RequireSecuritySignature	Disabled	Disabled	Enabled
Digitally sign server communication (when possible) COMPUTER\System\CurrentControlSet\Services\LanManServer\Parameteres\EnableSecuritySignature	Disabled	Enabled	Enabled
Disable Ctrl+Alt+Del requirement for to logon COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD	Disabled	Disabled	Disabled
Do not display last username in logon screen COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName	Disabled	Disabled	Enabled
LAN Manager Authentication Level COMPUTER\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel	Send LM & NTLM responses	Send NTLM response only	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText			

Message title for users attempting to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption			
Number of previous logons to cache (in case domain controller is not available) COMPUTER\Software\Microsft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount	10 logons	10 logons	10 logons
Prevent system maintenance of computer account password COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange	Disabled	Disabled	Disabled
Prevent users from installing printer drivers COMPUTER\System\CurrentControlSet\Control\PrintProviders\LanMan Print Services\Servers\AddPrinterDrivers	Enabled	Enabled	Enabled
Prompt user to change password before expiration COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpireWarning	14 days	14 days	14 days
Recovery Console: Allow auto-matic administrative logon COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel	Disabled	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand	Disabled	Disabled	Disabled
Rename administrator account [Not in the Registry]	Not defined	Not defined	Not defined
Rename guest account [Not in the Registry]	Not defined	Not defined	Not defined
Restrict CD-ROM access to locally logged-on user only COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms	Disabled	Disabled	Disabled
Restrict floppy access to locally logged-on user only COMPUTER\Software\Microsoft\Windows	Disabled	Disabled	Disabled

NT\CurrentVersion\Winlogon\AllocateFloppies			
Secure channel: Digitally encrypt or sign secure channel data (always) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignorSeal	Disabled	Disabled	Enabled
Secure channel: Digitally encrypt secure channel data (when possible) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel	Enabled	Enabled	Enabled
Secure channel: Digitally sign secure channel data (when possible) COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel	Enabled	Enabled	Enabled
Secure channel: Require strong (Windows 2000 or later) session key COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey	Disabled	Disabled	Enabled
Secure system partition (for RISC platforms only) [Not in the Registry]	Not defined	Not defined	Not defined
Send unencrypted password to connect to third-parry SMB servers COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword	Disabled	Disabled	Disabled
Shut down system immediately if unable to log security audits COMPUTER\System\CurrentControlSet\Control\Lsa\CrashonAuditFail	Disabled	Disabled	Disabled
Smart card removal behavior COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption	No Action	Lock Workstation	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links) COMPUTER\System\CurrentControlSet\Control\Session Manager\ProtectionMode	Enabled	Enabled	Enabled
Unsigned driver installation behavior COMPUTER\Software\Microsoft\Driver Signing\Policy	Not defined	Warn but allow installation	Do not allow installation
Unsigned non-driver installation behavior COMPUTER\Software\Microsoft\Non-Driver Signing\Policy	Not defined	Silently succeed	Silently Succeed
Event Log			

Settings for Event Logs			
Maximum application log size (MaximumLogSize)	512 kilobytes	Not defined	Not defined
Maximum security log size (MaximumLogSize)	512 kilobytes	5120 kilobytes	10240 kilobytes
Maximum system log size(MaximumLogSize)	512 kilobytes	Not defined	Not defined
Restrict guest access to application log (RestrictGuestAccess)	Disabled	Enabled	Enabled
Restrict guest access to security log (RestrictGuestAccess)	Disabled	Enabled	Enabled
Restrict guest access to system log(RestrictGuestAccess)	Disabled	Enabled	Enabled
Retain application log (RetentionDays)	7 days	Not defined	Not defined
Retain security log (RetentionDays)	7 days	Not defined	Not defined
Retain system log (RetentionDays)	7 days	Not defined	Not defined
Retention method of application log (AuditLogRetentionPeriod)	By days	Not defined	Not defined
Retention method for security log (AuditLogRetentionPeriod)	By days	As needed	As needed
Retention method for system log (AuditLogRetentionPeriod)	By days	Not defined	Not defined
Shut down the computer when the security audit log is full (CrashOnAuditFull)	Not defined	Not defined	Not defined

Table 4.5 Domain Controller Security Policy Templates

4.4 Author's Recommended Security Policy

Based on the policies from the default Windows 2000 templates and made a couple of changes of his own. The next sections will describe the recommended settings.

4.4.1 Author's Recommended Account Policy

The table below lists the author's recommended account policy.

	Author's Recommended Workstation / Server	***Author's Recommended Domain Controller***
Account Policies		
Password Policy		
Enforce password history	24 passwords remembered	24 passwords remembered
(PasswordHistorySize)		
Maximum password age	45 days	45 days
(MaximumPasswordAge)		
Minimum password age	1 days	1 days
(MinimumPasswordAge)		

Minimum password length	8 characters	8 characters
(MinimumPasswordLength)		
Passwords must meet complexity requirements (PasswordComplexity)	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled
Account Lockout Policy		
Account lockout duration	0	0
(LockoutDuration)		
Account lockout threshold (LockoutBadCount)	3 invalid Logon attempts	3 invalid Logon attempts
Reset account lockout counter after (ResetLockoutCount)	15 minutes	15 minutes
Local Policies		
Audit Policy		
Audit account logon events	Success/Failure	Success/Failure
(AuditAccountLogon)		
Audit account management	Success/Failure	Success/Failure
(AuditAccountManage)		
Audit directory services access	Success/Failure	Success/Failure
(AuditDSAccess)		
Audit Logon events	Success/Failure	Success/Failure
(AuditLogonEvents)		
Audit object access	Success/Failure	Success/Failure
(AuditObjectAccess)		
Audit policy change	Success/Failure	Success/Failure
(AuditPolicyClaange)		
Audit privilege use	Success/Failure	Success/Failure
(AuditPrivilegeUse)		
Audit process tracking	No auditing	No auditing
(AuditProcessTracking)		
Audit system events	Success/Failure	Success/Failure
(AuditSystemEvents)		
User Rights		
Access this computer from the network	Administrators, Authenticated Users	Administrators, Authenticated Users
Add workstations to the domain	None	None
Backup Files & Directories	Administrators, Backup Operators	Administrators, Backup Operators
Bypass traverse checking	None	None
Change system time	Administrators	Administrators

Create a Token Object	None	None
Create Pagefile	Administrators	Administrators
Create Permanent Shared Objects	None	None
Debug Programs	None	None
Force shutdown from a remote system	Administrators	Administrators
Generate security audits	None	None
Increase Quotas	None	None
Increase Scheduling Priority	Administrators	Administrators
Load Device Drivers	Administrators	Administrators
Lock Pages in Memory	None	None
Log on Locally	Administrators, Authenticated Users	Administrators, Backup Operators
Logon as a batch job	None	None
Logon as a service	As needed	As needed
Manage auditing & security log	Administrators	Administrators
Modify firmware environment variables	Administrators	Administrators
Profile a single process	Administrators	Administrators
Profile system performance	Administrators	Administrators
Replace a process level token	None	None
Restore files & directories	Administrators, Backup Operators	Administrators, Backup Operators
Shut down the system	Administrators, Authenticated Users	Administrators, Authenticated Users
Take ownership of files & other objects	Administrators	Administrators
Security options		
Additional restrictions for anonymous connections COMPUTER\System\CurrentControlSet\Control\Lsa\RestrictAnonymous	No access without explicit anonymous permissions	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only) COMPUTER\System\CurrentControlSet\Control\Lsa\SubmitControl	Disabled	Disabled
Allow system to be shut down without having to log on COMPUTER\Software\Microsoft\Winodws\CurrentVersion\Policies\System\ShutdownWithoutLogon	Disabled	Disabled

Allowed to eject removable NTFS media COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD	Administrators	Administrators
Amount of idle time required before disconnecting session COMPUTER\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoDisconnect	15 minutes	15 minutes
Audit the access of global system objects COMPUTER\Systern\CurrentControlSet\Control\Lsa\AuditBaseObjects	Disabled	Disabled
Audit use of Backup and Restore privilege COMPUTER\System\CurrentControlSet\Control\Lsa\AuditBaseObjects	Disabled	Disabled
Automatically log off users when logon time expires COMPUTER\System\CurrentControlSet\Control\Lsa\Services\LanManServer\Parameters\EnableForcedLogOff	Enabled	Enabled
Automatically log off users when Logon time expires (local) [Not in the Registry]	Enabled	Enabled
Clear virtual memory pagefile when system shuts down COMPUTER\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown	Enabled	Enabled
Digitally sign client communication (always) COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature	Enabled	Enabled
Digitally sign client communication (when possible) COMPUTER\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature	Enabled	Enabled

Digitally sign server communication (always) COMPUTER\System\CurrentControlSet\Services\LanManServer\Parameteres\RequireSecuritySignature	Enabled	Enabled
Digitally sign server communication (when possible) COMPUTER\System\CurrentControlSet\Services\LanManServer\Parameteres\EnableSecuritySignature	Enabled	Enabled
Disable Ctrl+Alt+Del requirement for to logon COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD	Disabled	Disabled
Do not display last username in logon screen COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName	Enabled	Enabled
LAN Manager Authentication Level COMPUTER\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel	Send NTLM response only	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	Disclaimer Text	Disclaimer Text
Message title for users attempting to log on COMPUTER\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	Disclaimer Caption	Disclaimer Caption
Number of previous logons to cache (in case domain controller is not available) COMPUTER\Software\Microsft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount	10 logons	10 logons

Prevent system maintenance of computer account password COMPUTER\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange	Disabled	Disabled
Prevent users from installing printer drivers COMPUTER\System\CurrentControlSet\Control\PrintProviders\LanMan Print Services\Servers\AddPrinterDrivers	Enabled	Enabled
Prompt user to change password before expiration COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpireWarning	14 days	14 days
Recovery Console: Allow auto-matic administrative logon COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand	Disabled	Disabled
Rename administrator account [Not in the Registry]	Not defined	Not defined
Rename guest account [Not in the Registry]	Not defined	Not defined
Restrict CD-ROM access to locally logged-on user only COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms	Enabled	Enabled

Restrict floppy access to locally logged-on user only COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies	Enabled	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always) COMPUTER\System\CurrentControlSet\Services\ Netlogon\Parameters\RequireSignorSeal	Enabled	Enabled
Secure channel: Digitally encrypt secure channel data (when possible) COMPUTER\System\CurrentControlSet\Services\ Netlogon\Parameters\SealSecureChannel	Enabled	Enabled
Secure channel: Digitally sign secure channel data (when possible) COMPUTER\System\CurrentControlSet\Services\ Netlogon\Parameters\SignSecureChannel	Enabled	Enabled
Secure channel: Require strong (Windows 2000 or later) session key COMPUTER\System\CurrentControlSet\Services\ Netlogon\Parameters\RequireStrongKey	Enabled	Enabled
Secure system partition (for RISC platforms only) [Not in the Registry]	Not defined	Not defined
Send unencrypted password to connect to third-parry SMB servers COMPUTER\System\CurrentControlSet\Services\ LanmanWorkstation\Parameters\EnablePlainText Password	Disabled	Disabled
Shut down system immediately if unable to log security audits COMPUTER\System\CurrentControlSet\Control\L sa\CrashonAuditFail	Disabled	Disabled

Smart card removal behavior COMPUTER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption	Force Logoff	Force Logoff
Strengthen default permissions of global system objects (e.g. Symbolic Links) COMPUTER\System\CurrentControlSet\Control\Session Manager\ProtectionMode	Enabled	Enabled
Unsigned driver installation behavior COMPUTER\Software\Microsoft\Driver Signing\Policy	Do not allow installation	Do not allow installation
Unsigned non-driver installation behavior COMPUTER\Software\Microsoft\Non-Driver Signing\Policy	Silently Succeed	Silently Succeed
Event Log		
Settings for Event Logs		
Maximum application log size (MaximumLogSize)	50560 kilobytes	50560 kilobytes
Maximum security log size (MaximumLogSize)	50560 kilobytes	50560 kilobytes
Maximum system log size(MaximumLogSize)	50560 kilobytes	50560 kilobytes
Restrict guest access to application log (RestrictGuestAccess)	Enabled	Enabled
Restrict guest access to security log (RestrictGuestAccess)	Enabled	Enabled
Restrict guest access to system log(RestrictGuestAccess)	Enabled	Enabled
Retain application log (RetentionDays)	Not defined	Not defined
Retain security log (RetentionDays)	Not defined	Not defined
Retain system log (RetentionDays)	Not defined	Not defined
Retention method of application log (AuditLogRetentionPeriod)	As needed	As needed
Retention method for security log (AuditLogRetentionPeriod)	As needed	As needed
Retention method for system log (AuditLogRetentionPeriod)	As needed	As needed

Shut down the computer when the security audit log is full (CrashOnAuditFull)	Not defined	Not defined

Table 4.6 Author's Recommended Security Policy

4.4.2 Author's Recommended Account Policy

There are not many differences between these settings and the high-security settings if the default templates were to be applied incrementally. Your security settings may be different depending on your organization's security policy. For instance the maximum password age may be increased if perhaps you may want to use a longer minimum password length.

You may choose a shorter lockout time duration if the invalid logon attempts were lowered. For the recommended policy the reset duration is set to 15 minutes instead 30 minutes, but the lockout duration is set to 0. The 0 setting will require an administrator to unlock the account every time.

4.4.3 Author's Recommended Local Policy

Auditing of system and security events are recommended on both the server and workstations. This allows for easy tracking of system problems on all computers if they were to occur.

For the user rights, it is recommended that limited access be granted. Notice that only Administrators, Authenticated Users, and Backup Operators occur in the user rights. The Everyone and Power Users groups have been stripped from these settings.

The security options remain almost the same as the Windows default high-security templates.

4.4.4 Author's Recommended Event Log Policy

It is recommended that a centralized audit consolidation program be used. Therefore it is recommended that the log size be increased to 50560 kilobytes. This setting along with the retention method set to as needed, allows events to be kept as logs as possible before they are cleared. This will allow for ample evidence collection. With a central audit consolidation program you can rely on the auditing program to pull the event logs off the computer and archive it before it is cleared off the computer. It is recommended that restriction of guest access be enabled. It is not recommended that the computer be shutdown if the security logs are full.

5 Conclusion

The Security Configuration Tool set is a set of very useful and powerful tools. With these tools, a security policy can be configured and implemented to a single or group of computers.

The Windows 2000 default security policies can be extremely useful in determining a security policy for your organization. The policies are meant to be applied incrementally. Applying a single default security policy will not provide the security that is needed. You will only utilize the full potential of the policy templates if they are used together.

With the Security Configuration Tool set however, you can modify the default security policy templates to correspond to your organization's security policy.

The file security settings and registry settings were not discussed in this document. In most cases the majority of the settings are limited to Administrators and System with FULL CONTROL rights, Power Users with limited rights, and Authenticated Users with READ rights. Depending on what programs your organization utilizes, the Authenticated Users may need more than READ access to certain parts of the registry and file system. In certain areas of the file system and registry, Authenticated Users may need FULL CONTROL This document emphasis security through password and local policy settings. These policies would need to be broken first before a person with malicious intent can access a computer. A file and registry policy should not be ignored. It is not recommended that a policy without a file or registry policy be implemented. File and registry policies are included with each Windows default security policy

6 List of References

Fossen, Jason. 2000. SANS Security Windows 2000 Course Books. Washington DC SANS Conference. December 2000.

Microsoft Windows Knowledge Base Article Q234926 – "Windows 2000 Security Templates are Incremental."

Microsoft Windows Knowledge Base Article Q216736 – "Methods Used to Apply Security Settings in an Enterprise."

Bragg, Roberta. 2001. Windows 2000 Security. Indianapolis, Indiana. New Riders Publishers. ISBN (0-7357-0991-2)

Internet Security Systems, Inc. 2000 Microsoft Windows 2000 Security Technical Reference. Redmond, Washington. Microsoft Press. ISBN (0-7356-0858-X)

Bartock, Paul. Brown, Karl. Cook, Melanie. Hanley, Julie. Parks, Hartley. Pasanen, York. Stephens, Robin. White, Martin. Guide to Securing Microsoft Windows NT Networks. FT Meade, MD. February 3, 2000.