DATA SECURITY MANAGEMENT

Security Configuration and Analysis for Windows NT 4.0 and Windows 2000

Roberta Bragg

INSIDE

How to Use the Tool; What an Organization Can Do; Automating Security Configuration Without Active Directory; A Tool That Can Analyze Current Configuration Against Policy; When to Use SCA and When to Use Group Policy

Looking for an inexpensive tool to assist in configuring security settings on Windows NT 4.0 and Windows 2000? Look no further. Microsoft provides, free of charge, tools for both products at the least cost — free. For Windows NT 4.0, one will need to make sure that systems are at least at level service pack 4 and then install the Security Configuration Manager from the service pack 4 CD-ROM. (It is not installed when one applies the service pack.) A Windows 2000 default installation (Professional, Server, and Advanced Server) provides the Security Configuration and Analysis (SCA) Microsoft Management Console (MMC) snap-in. Both tools work in a similar manner; in fact, the Windows NT tool is a back port of technology developed for Windows 2000. This article examines the use of SCA on Windows 2000. There are minor differences in the use under Windows NT.

PAYOFF IDEA

Both Windows NT and Windows 2000 provide a tool for configuring security settings. The Security Configuration and Analysis (SCA) tool can free administrators from the tedium of visiting systems, adjusting Local Security Policy, or making individual registry and file system settings. It also adds additional configurations and can be used to ensure that standardization is carried out through the use of a template, not by pointing-and-clicking in an interface on each machine. In an Active Directory Setting, SCA allows automated analysis of current host settings, a way of determining if Group Policy settings are being applied, and whether or not they have been modified. This article discusses how to use the Security Configuration and Analysis (SCA) Microsoft Management Console (MMC).

© 2001 CRC Press LLC

FIRST THINGS FIRST: HOW TO USE THE TOOL

To use the tool, there are two choices: a GUI interface or the secedit command line tool. Use the GUI to learn the ropes and examine analyses of host systems. Use the command line in scripts to carry out analysis and implementation in the background and to force refreshes of policy.

To start:

1. Open an MMC console by typing MMC from the Start button Run command.
2. From the console menu, select the "Add/Remove Snap-In."
3. From the Add/Remove Snap-In dialog box, click the Add button.
4. From the Add Standalone Snap-In button, select "Security Configuration and Analysis" (see Exhibit 1) and click the Add button.
5. Click the Close button and then the OK button to return to the console with the snap-in loaded.
6. Right-click the "Security Configuration and Analysis" item under the "Console Root."
7. Click "Open Database."
8. Enter a new database name and click the Open button (any name is OK; one is creating a new database).
9. Select a security template to import and then click the Open button (for definitions of templates provided, see Exhibit 2).

Microsoft provides several security templates for use with SCA. Template files can be located in the %system root%\Security\Templates folder. One can examine them more easily by loading the snap-in to an MMC console. Follow instructions similar to loading SCA, but add the Security Templates snap-in. One can copy templates in this interface and modify them to one's own security policy expectations. Then use them to apply or analyze security on a system. One can even import them into Group Policy objects. Templates are described in Exhibit 2.

Before beginning the analysis, examine the template. Each different template presents a level of security settings predefined by Microsoft. However, one can change the settings anyway one wants. In fact, this is how one sets a written security policy into a framework, which can then be either applied to the computer or compared to the current computer settings.

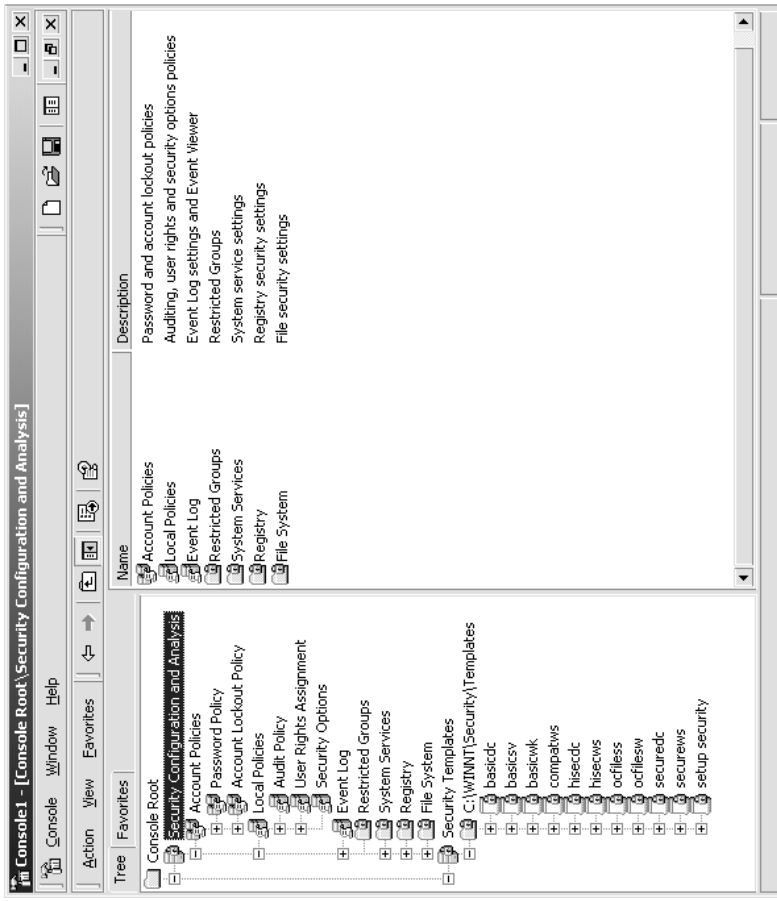
To configure the local system with the chosen policy:

1. Right-click the "Security Configuration and Analysis"
2. Select "Configure Computer Now."
3. One can change the location of the default log file; then press OK.

To analyze the local system against a security policy:

© 2001 CRC Press LLC

EXHIBIT 1 — Security Configuration and Analysis Screen



© 2001 CRC Press LLC

EXHIBIT 2 — Security Templates

Template File Name	Purpose	Use For
basicsv.inf	Similar to installation defaults	Server, Advanced Server
basicwk.inf	Similar to installation defaults	Server, Advanced Server
compatws.inf	File , registry, etc, permission settings similar to Window's NT 4.0. This represents a relaxation in security from the default settings and should only be used if necessary on systems running legacy software.	Professional
hisecdc.inf	High Security domain controller; high security settings mostly to do with network; domain level security.	Server DCs, Advanced Server DCs
hisecws.inf	High Security — settings mostly to do with network and network communications.	Professional, Server, Advanced Server
notssid.inf	Terminal server internet user security.	Server, Advanced Server used as a Terminal Server.
ocfiless.inf	Security settings for optional components like certificate services.	Server, Advanced Server
ocfilesw.inf	Secuirty settings for optional components.	Professional
securedc.inf	Medium level security settings for DCs	Server DCs, Advanced Server DCs
securews.inf	Medium level security settings for non-DCs	Server, Advanced Server, Professional

1. Open a new database, or right-click "Security Configuration and Analysis" and select the template.
2. Right-click the "Security Configuration and Analysis"
3. Select "Analyze Computer Now."
4. Examine the results by selecting items in the right-hand window. Items that do not match the selected template are marked with a red x.

PART TWO: WHAT AN ORGANIZATION CAN DO

If an organization has installed Windows 2000 and the installation includes the deployment of Windows 2000 domains, there is an excellent directory-based security configuration tool, Group Policy. Group Policy can be applied at the site (physical organization of Windows systems), domain (logical organization of windows systems), or organizational unit (sub-domain administrative unit) level. Group Policy propagates from a central administrative configuration to appropriate Windows 2000 servers and workstations — an excellent way to centrally control security settings as well as other administrative configurations.

However, Windows 2000 systems that are not joined in a domain exist without the benefits of Active Directory and propagatable security poli-

© 2001 CRC Press LLC

cies. Each Windows 2000 system does have a Local Security Policy, a GUI interface that can be configured for each individual computer. The Security Configuration and Analysis (SCA) tool can free administrators from the tedium of visiting systems, adjusting Local Security Policy, or making individual registry and file system settings. It also adds additional configurations and can be used to ensure that standardization is carried out through the use of a template — not by pointing-and-clicking in an interface on each machine. In an Active Directory Setting, SCA allows automated analysis of current host settings, a way of determining if Group Policy settings are being applied and whether or not they have been modified. Information system security and auditors, as well as administrators, can benefit from the use of the tool in either situation.

Automating Security Configuration Without Active Directory

Consider the types of settings that SCA allows (Exhibit 1). Settings fall into broad categories.

- *Account Policies:* Password Policy and Account Lockout Policy
- *Local Policies:* Audit Policy, User Rights Assignment, and Security Options
- *Event Log:* log size, retention policy, crash on audit fail
- *Restricted Groups:* preset membership in groups to prevent local administrators from changing
- *System Services:* determine boot status — start, stop, or disabled
- *Registry:* configure permissions on registry keys
- *File System:* configure permissions on file folders and files

Some of these categories may be unfamiliar to non-Windows aficionados; thus, an explanation is in order.

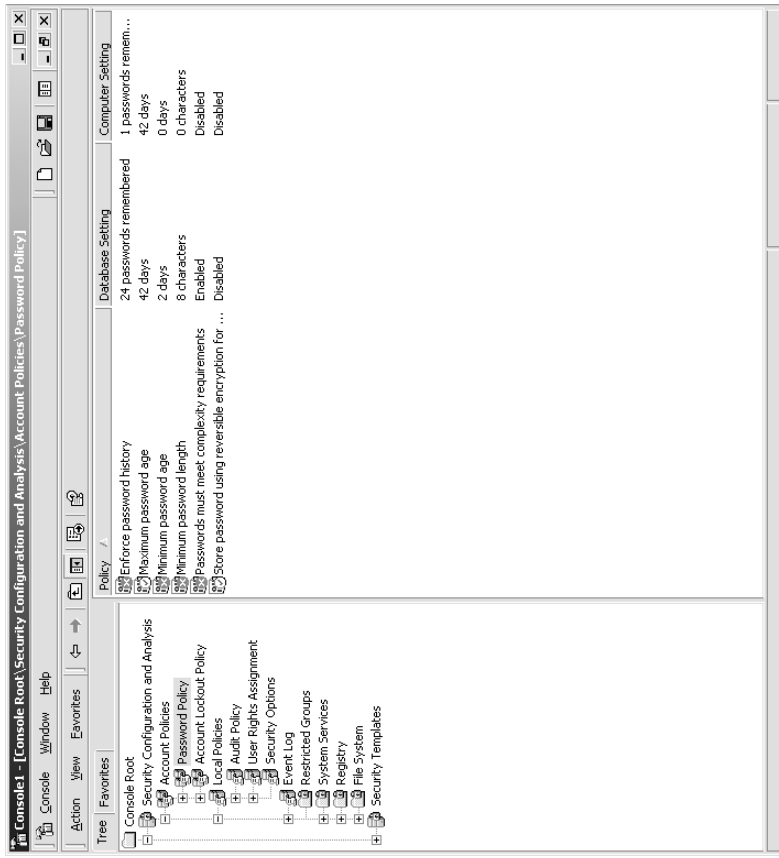
Account Policies. Typical Windows settable password policies cover password length, history, complexity, frequency of reset, and maximum and minimum time between password changes (see Exhibit 3). Account Lockout Policy covers the number of tries before an account is locked out, how long it is locked out, and when the lockout count is reset.

Local Policies. Audit Policy is, by default, turned off and must be set. Categories are broad and include object access, logon, policy change, privilege use system events, and process tracking. After turning on object access audit, audit can be configured separately for any file, folder, printer, or Active Directory object. Audit can be configured using the Registry and File Systems settings within SCA.

User Rights Assignment includes such defaults as “logon locally,” “access this computer from a network,” and shutting down the system.

© 2001 CRC Press LLC

EXHIBIT 3 — Password Policy Screen



© 2001 CRC Press LLC

Windows standard groups such as Administrators, Account Operators, and Users have default rights. Additional restrictions or allowances can be made.

Security Options (see Exhibit 4) covers a broad range of special security settings, several of which allow hardening of the Windows OS. These types of settings include many of those recommended in various publications as the list of registry settings that should be made to lock down Windows NT. Now they can be set without delving into the intricacies and dangers of direct registry editing.

Event Log. The Windows Event Logs capture event messages, including informational, warning, and errors. There are three basic logs: System, Application, and Security. Security, of course, is where audit messages are stored once auditing is turned on.

When a user account is given membership in the Administrators group, one of the privileges assigned is the right to add other users to groups, including the Administrators group. If this is not the intention of the assignment (i.e., an Administrator is needed, but one does not want to have them placing users in certain groups, then use Restricted Groups to define only the members allowed in each group. Each group to be so delineated must be included here and the membership listed. If an attempt is made to add a user to any Restricted Group in the normal manner (using Active Directory Users and Computers, or Computer Management consoles), the added account will be automatically removed from the Restricted Group.

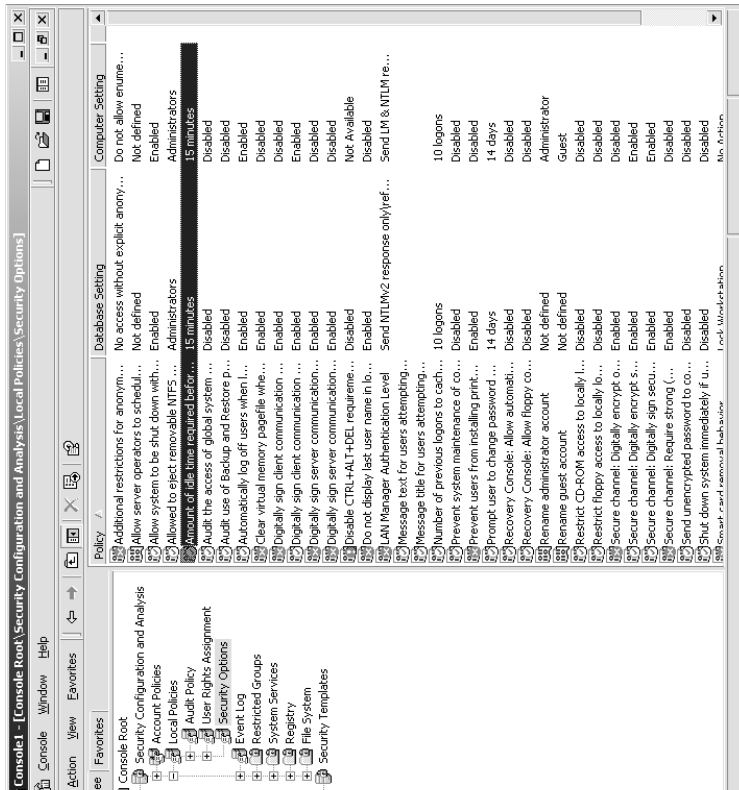
System Services. System Services are integral to the operation of Windows 2000. Services are used by various running background programs such as Net Logon (necessary for authentication), DHCP client (ability to obtain IP address), or DHCP server (ability to dynamically assign IP address), etc. Here is where one might wish to disable the Telnet service, disable the browser service, or ensure that other services will always start automatically if the system is rebooted.

Registry. The Windows 2000 Registry is a repository of information. It includes system configuration and user settings. It also includes the local account database (administrator account, encrypted password, etc.). Default access permissions are set quite a bit stronger in Windows 2000 than in Windows NT. However, one may want to apply different settings, or apply settings to registry keys added after installation. In addition, one can configure access auditing. Use this area of SCA to ensure that settings remain the way one wants them.

File System. The File System likewise has areas that should be maximally protected. Default system file protection in Windows 2000 is stron-

© 2001 CRC Press LLC

EXHIBIT 4 — Security Options Screen



© 2001 CRC Press LLC

ger than in Windows NT. Use the File System area of SCA to include other folders and files, to further tighten defaults, and to set auditing on file system access.

Security Templates. Without SCA, the above settings can be accomplished using various tools on each computer. Computer Management, Local Security Policy, Windows Explorer, and regedt32.exe can be used to configure security. However, configuration involves the use of all tools, and is a labor-intensive approach to setting system security. SCA allows the administrator to develop templates for security. Different templates can be developed for different classes of systems (servers, workstations, database servers, file servers, etc.) and different security levels, or base levels provided by Microsoft can be utilized. Each template is a text-based file and can easily be modified using SCA or by directly editing the file. Templates can be stored and applied to appropriate systems, either through the GUI or the use of the command line tool "secedit." Secedit can be used in a script and thus the process of applying or analyzing systems can be automated.

Finally: A Tool That Can Analyze Current Configuration Against Policy

How does one audit Windows systems? How does one ensure that all of the development effort devoted to the hard work at developing implementation specifics that enforce an organization's security policy is actually being applied? And how does one make sure that it has not been modified?

It would be nice to believe that, once designed, security implementation and enforcement are carried out like the application of regular break times and lunches for all employees. (In other words, regularly and without fail). However, a number of elements can prevent this ranging from error, (both human and computer) misdirection, and malfeasance. SCA provides a tool that can be used to determine if settings that should be made, have been made. Analysis is carried out against the current settings but does not change them. In the interface, current settings are listed alongside the desired policy. Exhibit 5 shows an example. For any difference between the desired policy and the actual settings, a red x is displayed. To examine the differences, open these folders for inspection. Exhibit 5 shows the Security Options section after analysis. Alternatively, use the Action menu/Export list select to export the results into a tab-delimited text file, and then import this file into Microsoft Access, Microsoft Excel, or another tool to print reports or for further analysis or archival purposes. Exhibit 5 also shows the Security Options section after analysis and being imported into Excel. The log produced during the analysis also lists each section analyzed and the results.

© 2001 CRC Press LLC

EXHIBIT 5 — Security Options Section Analyzed and Imported into Excel

Microsoft Excel - fig3a.xls

File Edit View Insert Format Tools Data Window Help

Arial 10

B2 = No access without explicit anonymous permissions

	A	B	C	D	E
1	Policy	Database Setting	Computer Setting		
2	Additional restrictions for anonymous connections	No access without explicit anonymous permiss	Do not allow enumeration of SAM acc		
3	Allow server operators to schedule tasks (domain controllers only)	Not defined	Not defined		
4	Allow system to be shut down without having to log on	Enabled	Enabled		
5	Allowed to eject removable NTFS media	Administrators	Administrators		
6	Amount of idle time required before disconnecting session	15 minutes	15 minutes		
7	Audit the access of global system objects	Disabled	Disabled		
8	Audit use of Backup and Restore privilege	Disabled	Disabled		
9	Automatically log off users when logon time expires (local)	Enabled	Enabled		
10	Clear virtual memory pagefile when system shuts down	Enabled	Disabled		
11	Digitally sign client communication (always)	Enabled	Disabled		
12	Digitally sign client communication (when possible)	Enabled	Enabled		
13	Digitally sign server communication (always)	Enabled	Disabled		
14	Digitally sign server communication (when possible)	Enabled	Disabled		
15	Disable CTRL+ALT+DEL requirement for logon	Disabled	Not Available		
16	Do not display last user name in logon screen	Enabled	Disabled		
17	LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLI	Send LM & NTLM responses		
18	Message text for users attempting to log on				
19	Message title for users attempting to log on				
20	Number of previous logons to cache (in case domain controller is not available)	10 logons	10 logons		
21	Prevent system maintenance of computer account password	Disabled	Disabled		
22	Prevent users from installing printer drivers	Enabled	Disabled		
23	Prompt user to change password before expiration	14 days	14 days		
24	Recovery Console: Allow automatic administrative logon	Disabled	Disabled		
25	Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	Disabled		
26	Rename administrator account	Not defined	Administrator		
27	Rename guest account	Not defined	Guest		
28	Restrict CD-ROM access to locally logged-on user only	Disabled	Disabled		
29	Restrict floppy access to locally logged-on user only	Disabled	Disabled		
30	Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled	Disabled		
31	Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Enabled		
32	Secure channel: Digitally sign secure channel data (when possible)	Enabled	Enabled		
33	Secure channel: Require strong (Windows 2000 or later) session key	Enabled	Disabled		
34	Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled		
35	Shut down system immediately if unable to log security audits	Disabled	Disabled		
36	Smart card removal behavior	Lock Workstation	No Action		
37	Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Enabled		

fig3a

Ready

© 2001 CRC Press LLC

To automate the collection of information, one must write a script. Use the secedit tool. Of course, someone still has to review the information for its meaning and determine a plan of action.

WHEN TO USE SCA AND WHEN TO USE GROUP POLICY

Group Policy is a utility available with Windows 2000 Active Directory. Unless one implements Windows 2000 domains, one will not have an Active Directory and cannot utilize its power. The local component of this process is called Local Security Policy. This GUI presents security policy configuration information for the current local system.

- Use Group Policy where Windows 2000 domains have been implemented.
- Use Local Security Policy for small numbers of Windows 2000 systems and one only wants to make changes to a single system (or where one incorporates its use with Group Policy Objects in a hierarchy). The Local Security Policy interface does not allow one to import templates, or analyze security settings against a baseline. All configuration is point-and-click.
- Use Security Configuration and Analysis to apply a policy template to a system using a minimum number of keystrokes and to apply uniform policy across multiple systems, albeit one at a time. (To do so most efficiently, one will need to write a script and use secedit commands.)
- Use Security Configuration and Analysis to analyze current settings on a machine-by-machine basis. (Again, one can script an efficient process to automate this.)
- Group Policy does not provide analysis capability. One can use SCA to analyze the results of Group Policy on security settings at the local machine level.
- Use Group Policy (domains) or Computer Management (no Windows 2000 domain) to configure settings other than those described as available via SCA.
- Group Policy does not affect Windows NT 4.0. Use The Security Configuration Manager tool to configure and analyze security on Windows NT 4.0 systems.
- Remember: Group Policy is hierarchical. Policies set at different levels may push policy down to lower levels, and higher level policy may be overwritten by that which exists closer to the system in question. Policy configured local, using Local Security Policy or Security Configuration and Analysis, can be overwritten by Group Policy. To use SCA in a domain setting requires a thorough understanding of security templates, SCA, and Group Policy.

© 2001 CRC Press LLC

CONCLUSION

Both Windows 2000 and Windows NT provide a tool for configuring security settings. The Security Configuration and Analysis tool can free administrators from the tedium of visiting systems, adjusting Local Security Policy, or making individual registry and file system settings. It also adds additional configurations and can be used to ensure that standardization is carried out through the use of a template — not by pointing-and-clicking in an interface on each machine. In an Active Directory Setting, SCA allows automated analysis of current host settings, a way of determining if Group Policy settings are being applied and whether or not they have been modified. This article discusses how to use the Security Configuration and Analysis (SCA) Microsoft Management Console (MMC). If one has not investigated the uses of SCAin Windows 2000 or SCM in Windows NT, one should. One will be pleasantly surprised by the results.

Roberta Bragg, MCSE, MCT, CTT, CISSP, is a veteran of over 20 years of IT experience. Her company, Have Computer Will Travel, Inc., keeps her writing, teaching, and consulting, primarily on Windows (NT and 2000) security. She is a contributing editor and security columnist for *Microsoft Certified Professional Magazine* (www.mcpmag.com) and the author of two books. She is an online instructor in Seattle Pacific University's MCSE program (www.spu.edu\prolearn).

© 2001 CRC Press LLC