18

Windows Server 2003 Security Management

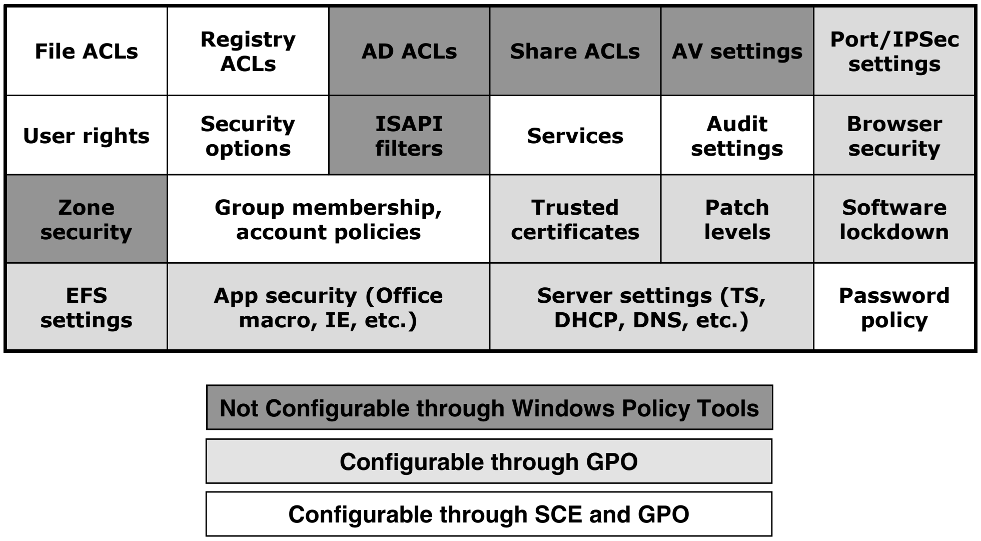
Security management is a critical security service that guarantees that the security settings and software on computer platforms and security infrastructure servers can be configured and maintained in an easy and coherent way. The security configuration together with the software that's allowed to run on a computer system are defined in a security policy. Computer platforms can become trusted platforms if the security policy is audited—this means checked for compliance by a trusted entity—at regular intervals. This is the goal of security-related auditing.

In what follows, we discuss how Microsoft supports security management in Windows Server 2003 in the following three key areas: security policy management, security patch management, and security-related auditing. This chapter specifically focuses on Microsoft security management solutions. A deeper coverage of third-party (non-Microsoft) security management solutions is beyond the scope of this book.

18.1 Security policy management

The security policy for a computer platform defines all security-related configuration settings for that platform. It includes all the configuration settings listed in Figure 18.1. As Figure 18.1 shows, Microsoft does not offer a single tool to deal with the configuration all security-related settings. Most of the settings can be configured using Group Policy Object (GPO) settings; others can be configured though the Security Configuration Editor; and some cannot be configured using a Microsoft security policy configuration tool.

Next we introduce the security policy life cycle. The other sections contain an overview of the different security policy management tools available in the Windows Server 2003 and Windows XP platforms. We discuss



□ File ACLs	□ Registry ACLs	▓ AD ACLs	▓ Share ACLs	▓ AV settings	▒ Port/IPSec settings
□ User rights	□ Security options	▓ ISAPI filters	□ Services	□ Audit settings	▒ Browser security
▓ Zone security	□ Group membership, account policies		▒ Trusted certificates	▒ Patch levels	▒ Software lockdown
▒ EFS settings	▒ App security (Office macro, IE, etc.)		▒ Server settings (TS, DHCP, DNS, etc.)		□ Password policy

▓ Not Configurable through Windows Policy Tools

▒ Configurable through GPO

□ Configurable through SCE and GPO

Figure 18.1 *Coverage of security-related configuration settings by Windows security policy management tools.*

Group Policy Objects (GPOs), the Security Configuration Editor and Analysis tool (SCE-SCA), the Security Configuration Wizard (SCW), and the Microsoft Baseline Security Analyzer (MBSA). We also look at third-party security policy management tools that can supplement the Microsoft tools.

18.1.1 The security policy life cycle

The life cycle of a Windows security policy can be split into several different phases:

- Policy creation: During this phase, security administrators define the security configuration of a Windows platform. Typically, a different security policy is defined for each machine type in the enterprise: workstations, file servers, and mail servers.
- Analysis: During this phase, security administrators validate the security configuration of a Windows platform against the settings defined in the security policy.
- Enforcement: During this phase, the security settings defined in the security policy are enforced on the different Windows platforms.
- Reporting: This phase deals with the generation of security policy compliance reports.

- Monitoring: This phase deals with the generation of real-time alerts when a machine's security settings are changed.

18.1.2 Group Policy and Group Policy Objects

Group Policy refers to a group of software technologies that allow centralized configuration and change management of user and computer environments. Through its tight integration with Active Directory, Group Policy Objects (GPOs) are highly scalable and extensible. Microsoft introduced Group Policy in Windows 2000.

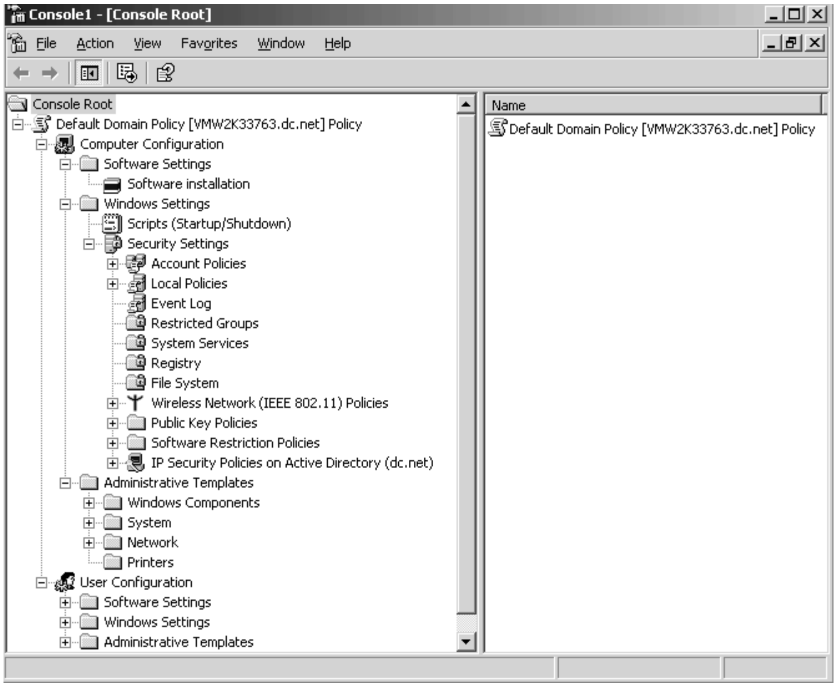
Group Policy covers six major system management areas: registry setting management, software deployment, folder redirection, scripts, software restriction policy, and security settings management. Software restriction policies were added in Windows Server 2003 (and discussed in detail in Chapter 11).

The basic unit of Group Policy is a Group Policy Object (GPO), a collection of policy configuration settings that can be linked to an Active Directory container (a domain, site, or OU) or to a local machine. The latter GPO type is referred to as a Local GPO (LGPO). The administrative interface for GPO management is the MMC Group Policy snap-in, also known as the Group Policy Editor (GPE), which is illustrated in Figure 18.2.

Windows 2000 and Windows Server 2003 come with two predefined GPOs: the default domain controllers and the default domain policy GPO.

- The default Domain Policy GPO is the GPO that is automatically applied to every user and computer object in a Windows 2000 or Windows Server 2003 domain. It is linked to an AD domain object. The default domain policy is the only policy that can be used to control the security settings (password quality, account lockout, and so forth) of AD account objects (also known as global accounts)
- The default Domain Controllers GPO is the GPO that is automatically applied to every Windows 2000 and Windows Server 2003 domain controller. It is linked to the Domain Controllers Organizational Unit (OU) container.

Next we briefly introduce the major GPO changes in Windows Server 2003. Afterward we look at how you can use GPOs for security policy management. For more information on GPOs and GPO settings and to learn more about the GPO design and the GPO application process, see the information contained in the Microsoft Technet library or Chapter 7 of my previous book, *Mission-Critical Active Directory.*


Console1 - [Console Root]
File Action View Favorites Window Help
Name

- Console Root
  - Default Domain Policy [VMW2K33763.dc.net] Policy
    - Computer Configuration
      - Software Settings
        - Software installation
      - Windows Settings
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - IP Security Policies on Active Directory (dc.net)
      - Administrative Templates
        - Windows Components
        - System
        - Network
        - Printers
    - User Configuration
      - Software Settings
      - Windows Settings
      - Administrative Templates

Default Domain Policy [VMW2K33763.dc.net] Policy

Figure 18.2 *GPE and different containers and settings.*

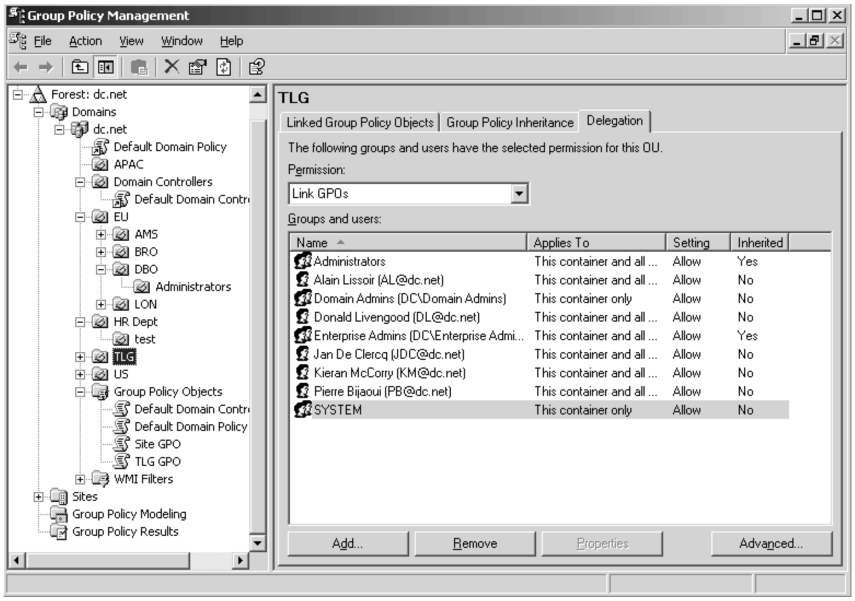
Key Windows Server 2003 Group Policy changes

Windows Server 2003 includes important GPO enhancements that improve administrators' ability to design, manage, and troubleshoot GPOs. The following sections provide an overview of the key enhancements. We will not come back to software restriction policies, which were covered extensively in Chapter 11.

Group Policy Management Console

The Group Policy Management Console (GPMC) provides a unified view (illustrated in Figure 18.3) of GPOs, sites, domains, and OUs in an enterprise and can be used to manage either Windows Server 2003 or Windows 2000 domains. Because GPMC supports the new forest trust type, administrators can use it to manage GPOs in multiple forests from a single console. Until the release of GPMC, enterprises had to look at third-party tools to obtain a unified Group Policy management interface. A good example is FullArmor's FAZAM 2000 software.

GPMC comes with an HTML-based reporting feature and provides GPO backup, restore, and copy support. GPMC also provides a set of



TLG

The following groups and users have the selected permission for this OU.

Permission: Link GPOs

Groups and users:

Name	Applies To	Setting	Inherited
Administrators	This container and all ...	Allow	Yes
Alain Lissoir (AL@dc.net)	This container and all ...	Allow	No
Domain Admins (DC\Domain Admins)	This container only	Allow	No
Donald Livengood (DL@dc.net)	This container and all ...	Allow	No
Enterprise Admins (DC\Enterprise Admi...	This container and all ...	Allow	Yes
Jan De Clercq (JDC@dc.net)	This container and all ...	Allow	No
Kieran McCorry (KM@dc.net)	This container and all ...	Allow	No
Pierre Bijaoui (PB@dc.net)	This container and all ...	Allow	No
SYSTEM	This container only	Allow	No

Figure 18.3
GPMC interface.

scripts that can be used to automate GPO operations at the command line. Among its most powerful features are GPO results and modeling support. GPMC exposes the Resultant Set of Policy (RSoP) data. RSoP makes it easy for administrators to determine the resulting set of policies for a user or computer in both actual and what-if scenarios.

GPMC runs on Windows XP Professional SP1 and Windows Server 2003. In Windows XP Professional, you must have Service Pack 1 and the .NET Framework installed before installing the GPMC. The tool can be downloaded from the Microsoft downloads Web site.

WMI filters

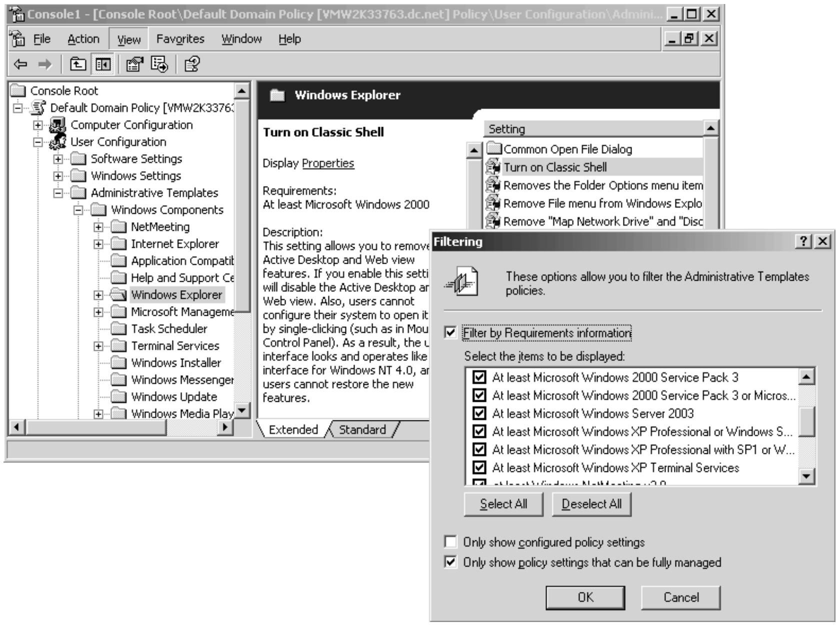
Windows 2000 supports a GPO feature, known as GPO filtering, that allows you to define to which users and computers a GPO will be applied. This can be done by modifying the permissions on the GPO. In Windows XP and Windows Server 2003, Microsoft adds an additional filtering mechanism based on the Windows Management Instrumentation (WMI) interface.

A WMI GPO filter lets you dynamically determine the application scope of a GPO based the on properties of the target computer or user. You can, for example, create a WMI filter that only applies the GPO if the target computer is running Windows XP Service Pack 1. When using a WMI filter, the GPO is only applied if the result of the WMI query is true. WMI filters use the WMI Query Language (WQL), a WMI-specific SQL-like query language.

Administrative template changes

Administrative templates drive the configuration of Windows registry settings using GPOs. Windows Server 2003 provides a great deal of additional information about the different registry settings: Every setting now comes with an explain text. The text contains information about OS requirements and details about the effect of enabling or disabling the setting. The explain text is visible from the Extended GPO view or by double-clicking a setting and going to the Explain tab.

Not every administrative template setting can be applied to every Windows version. Windows Server 2003 GPO includes new features to expose this template versioning system in the interface. Under the hood, this versioning system builds on the supported keyword in administrative template files (*.adm). To filter the administrative template settings based on the Windows version requirements, right-click an administrative templates container, and then in the View menu, select Filtering (as illustrated in Figure 18.4).



Turn on Classic Shell

Display Properties

Requirements:
At least Microsoft Windows 2000

Description:
This setting allows you to remove Active Desktop and Web view features. If you enable this setti will disable the Active Desktop ar Web view. Also, users cannot configure their system to open it by single-clicking (such as in Mou Control Panel). As a result, the u interface looks and operates like interface for Windows NT 4.0, ar users cannot restore the new features.

Filtering

These options allow you to filter the Administrative Templates policies.

☑ Filter by Requirements information

Select the items to be displayed:

☑ At least Microsoft Windows 2000 Service Pack 3
☑ At least Microsoft Windows 2000 Service Pack 3 or Micros...
☑ At least Microsoft Windows Server 2003
☑ At least Microsoft Windows XP Professional or Windows S...
☑ At least Microsoft Windows XP Professional with SP1 or W...
☑ At least Microsoft Windows XP Terminal Services

☐ Only show configured policy settings
☑ Only show policy settings that can be fully managed

Figure 18.4
Administrative template changes.

Command-line support

Administrators can now refresh policy settings from the command line using gpup*date, which replaces the Windows 2000 secedit /refreshpolicy.

Windows Server 2003 includes a new tool called dcgpofix.exe to restore the default domain and the default domain controllers GPOs to their original state—meaning their default state after a fresh Windows Server 2003 installation.

Using GPOs for security policy management

The GPO security policy management portion includes configuration options for the following security policy areas (Table 18.1 contains an overview):

- Account policies to configure password, account lockout, and Kerberos settings.
- Local policies to configure auditing, user rights, and security options.
- Event log settings to configure the properties of the application, system, and security logs.
- Restricted group settings to configure the membership of security sensitive groups.
- System services settings to configure security and startup settings for services.
- Registry settings to configure security permissions on registry keys.
- File system settings to configure security permissions on files and folders.
- Wireless network settings to configure wireless network access policies.
- Public key policies to configure EFS recovery agents, trusted root CAs, user and machine certificate autoenrollment settings, and Certificate Trust Lists (CTLs).
- Software restriction policies to configure malicious mobile code protection rules.
- IP security policies to configure IPsec-related settings.

All of these settings can be configured from the Windows Settings\Security Settings GPO container (as illustrated in Figure 18.2). To configure local security policy settings on member servers, workstations, and stand-alone machines, you must use the local security policy settings MMC snap-in (illustrated in Figure 18.5). The wireless network settings and software restriction policies settings are new to Windows Server 2003. Only the soft-

Table 18.1 *GPO Security Settings Containers and Equivalent NT4 Administration Tool*

GPO Security Settings Subcontainer (Windows 2000,Windows XP, and Windows Server 2003)	Equivalent NT4 Administration Tool (NT4)
Account policies	
Password policy	User manager => Policy/Account Policy
Account lockout	User manager => Policy/Account Policy
Kerberos policy*	N/A
Local policies	
Audit policy	User manager => Policy/Audit Policy
User rights assignment	User manager => Policy/User Rights
Security options	N/A
Event log*	Event Viewer => Log/Event Log Settings
Restricted groups*	N/A
System services*	Control Panel => Services
Registry	N/A
File system*	N/A
Wireless network policies*	N/A
Public key policies	N/A
Encrypting File System	N/A
Automatic Certificate Request Settings*	N/A
Trusted Root Certification Authorities*	N/A
Enterprise Trust*	N/A
Software restriction policies	N/A
IP security policies	N/A

* Not configurable on workstations, member servers, and stand-alone machines.

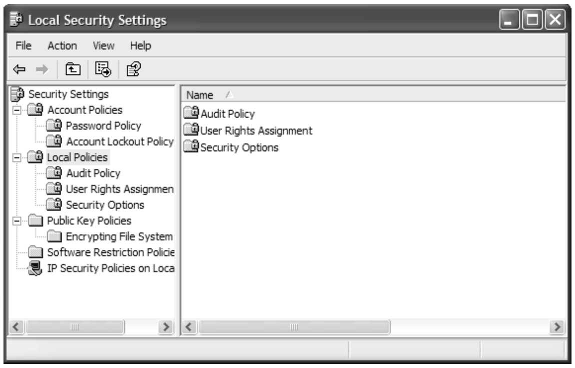


Figure 18.5 *Local security policy configuration tool.*

ware restriction policies and public key policies can be configured in both the user- and machine-portion of the GPOs; the other settings can only be configured in the machine-portion of the GPO.

In the GPO security policy management portion, Microsoft brought together the configuration of several security settings that before, in NT4, were spread across different administration tools. Table 18.1 gives an overview of the different security setting categories configurable through the Windows 2000, Windows XP, and Windows Server 2003 GPO security settings and their NT4 administration tool counterpart.

The Account policies in the GPO security policy management container deserve a bit more explanation. Account policies can refer to local accounts or domain accounts. Account policies for domain accounts can only be set in the Default Domain Policy. This means that password, account lockout, and Kerberos policies for domain accounts can only be defined once: on the domain level using the Default Domain Policy. Account policies that are set in other GPOs will not affect the domain account policy but local account policies. Local account policies means policies linked to accounts stored in the SAM (the local security database).

A very interesting category of GPO security settings is the Security Options, located in the Local Policies container. Windows Server 2003 comes with a lot of additional Security Options; they are listed in Table 18.2. I strongly advise you to look closely at these new security options. Administrators can also add additional security-related registry configuration settings to the Security Options. How to do this is explained in the Microsoft Knowledge Base article Q214752.

GPO security policy management is closely related to the Security Configuration Editor and Analysis tool (SCE/SCA), which is discussed later in

Table 18.2 *New Windows Server 2003 Security Options*

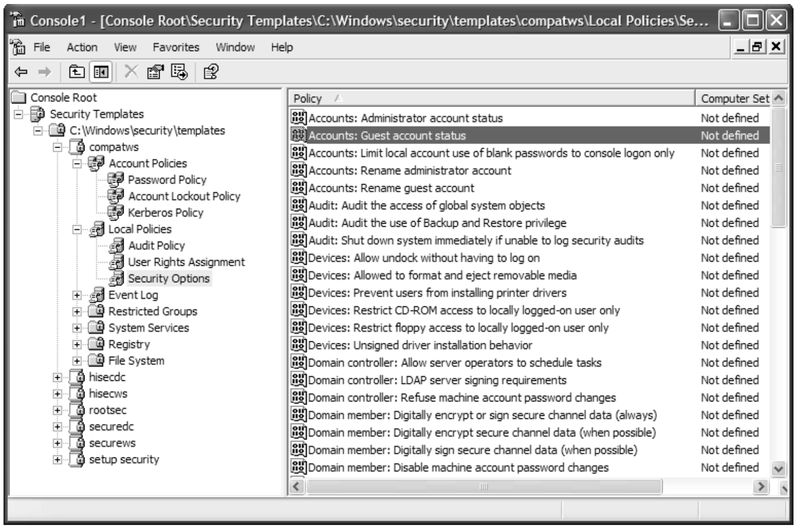
Security Option	Values
Guest account status	Enabled/Disabled
Limit local account use of blank passwords to console logon only	Enabled/Disabled
Allow undock without having to log on	Enabled/Disabled
Allowed to format and eject removable media	Administrators/Administrators and Power Users/ Administrators and Interactive Users
LDAP server signing requirements:	None/Require Signing
Refuse machine account password changes	Enabled/Disabled
Maximum machine account password age	x days
Require strong (Windows 2000 or later) session key	Enabled/Disabled
Require domain controller authentication to unlock workstation	Enabled/Disabled
Require smart card	Enabled/Disabled
Allow anonymous SID/Name translation	Enabled/Disabled
Do not allow anonymous enumeration of SAM accounts	Enabled/Disabled
Do not allow anonymous enumeration of SAM accounts and shares	Enabled/Disabled
Administrator account status	Enabled/Disabled
Do not allow storage of credentials or .NET Passports for network authentication	Enabled/Disabled
Let Everyone permissions apply to anonymous users	Enabled/Disabled
Remotely accessible registry paths	Names of registry paths
Remotely accessible registry paths and subpaths	Names of registry paths and subpaths
Restrict anonymous access to Named Pipes and Shares	Enabled/Disabled
Shares that can be accessed anonymously	share names
Sharing and security model for local accounts	Classic: local users authenticate as themselves / Guest: local users authenticate as Guest
Do not store LAN Manager hash value on next password change	Enabled/Disabled

Table 18.2 *New Windows Server 2003 Security Options (continued)*

Security Option	Values
LDAP client signing requirements	None/Negotiate Signing/Require Signing
Minimum Session Security for NTLM SSP-based (including secure RPC) clients	Require message integrity/Require message confidentiality/Require NTLMv2 session security/Require 128-bit encryption
Minimum Session Security for NTLM SSP-based (including secure RPC) servers	Require message integrity/Require message confidentiality/Require NTLMv2 session security/Require 128-bit encryption
Allow automatic administrative logon	Enabled/Disabled
Use Certificate rules on Windows executables for SRPs	Enabled/Disabled
Force strong key protection for user keys stored on the computer	User input is not required when new keys are stored and used/User is prompted when the key is first used/User must enter password each time they use a key
Use FIPS compliant algorithms for encryption, hashing, signing	Enabled/Disabled
Default owners for object created by members of the Administrators group	Administrators group/Object creator
Allow floppy copy and access to all drives and all folders	Enabled/Disabled
Require case-insensitivity for non-Windows subsystems	Enabled/Disabled
Optional subsystems	Subsystem names (Posix)

this chapter. GPOs complement the SCE/SCA by making it possible to enforce security policy settings on the domain, OU, and site level. Both the SCA and GPO security management use the same client-side extensions for security policy enforcement: the scecli.dll on Windows client platforms and the scesrv.dll on Windows servers. Both also use the same local security configuration database: secedit.sdb.

Both the GPO- and SCE-rooted security policy management support security configuration templates (*.inf files). These are security configuration-specific templates that can be easily exchanged between different GPOs and machines. The templates are stored in the %systemdrive%\winnt\security\templates directory. Like the administrative templates used for registry configuration (*.adm), the security configuration templates are customizable. To edit security configuration templates, you use a plaintext



Policy	Computer Set
Accounts: Administrator account status	Not defined
Accounts: Guest account status	Not defined
Accounts: Limit local account use of blank passwords to console logon only	Not defined
Accounts: Rename administrator account	Not defined
Accounts: Rename guest account	Not defined
Audit: Audit the access of global system objects	Not defined
Audit: Audit the use of Backup and Restore privilege	Not defined
Audit: Shut down system immediately if unable to log security audits	Not defined
Devices: Allow undock without having to log on	Not defined
Devices: Allowed to format and eject removable media	Not defined
Devices: Prevent users from installing printer drivers	Not defined
Devices: Restrict CD-ROM access to locally logged-on user only	Not defined
Devices: Restrict floppy access to locally logged-on user only	Not defined
Devices: Unsigned driver installation behavior	Not defined
Domain controller: Allow server operators to schedule tasks	Not defined
Domain controller: LDAP server signing requirements	Not defined
Domain controller: Refuse machine account password changes	Not defined
Domain member: Digitally encrypt or sign secure channel data (always)	Not defined
Domain member: Digitally encrypt secure channel data (when possible)	Not defined
Domain member: Digitally sign secure channel data (when possible)	Not defined
Domain member: Disable machine account password changes	Not defined

Figure 18.6
Security Templates MMC snap-in.

editor (like Notepad) or the Security Templates MMC snap-in, illustrated in Figure 18.6.

Microsoft provides two basic categories of security configuration templates: default and incremental security templates:

- Default security templates contain the default Windows security settings, as they are applied to a Windows system during a normal installation.
- Incremental security templates define higher or lower security levels; they can be used to bring a machine from the default security level to a higher or lower security level. The compatws.inf template, for example, loosens security on a Windows machine to allow applications to write to more registry keys. The hisecdc.inf template, on the other hand, tightens the security of a Windows domain controller. An incremental template should never be applied without first applying a default template. Microsoft defines three levels: compatible, secure, and high secure.

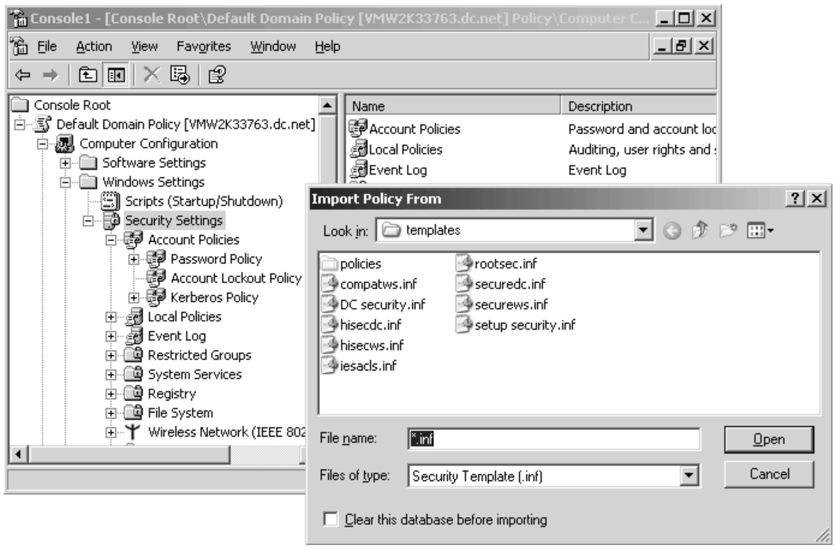
Each of these categories contains specific templates for a Windows workstation, server, and domain controller. The security configuration templates available in Windows are listed in Table 18.3.

To load a template in the GPO interface, right-click the security settings container and select import policy (as illustrated in Figure 18.7). The security settings are the only GPO settings that can be copy-pasted or imported-

Table 18.3 *Windows XP and Windows Server 2003 Security Templates*

Security Template Category	Template Name	Meaning
Default templates	DC security.inf	The default template for a Windows domain controller
	Setup security.inf	The default template for a Windows workstation
Incremental templates	Compatws.inf	Compatible incremental template for a Windows workstation. Relaxes security settings to deal with noncertified applications.
	Rootsec.inf	Applies default root permissions introduced in Windows XP to the OS partition and propagates them to child objects that are inheriting from the root.
	Securedc.inf	Secure incremental template for a Windows domain controller
	Securews.inf	Secure incremental template for a Windows workstation
	Hisecdc.inf	High Secure incremental template for a Windows domain controller
	Hisecws.inf	High Secure incremental template for a Window workstation

Figure 18.7 *Importing security templates for a GPO's security settings.*



Look in: templates

File name: *.inf

Files of type: Security Template (.inf)

☐ Clear this database before importing

exported between different GPOs.To export the security settings defined in a GPO, you must use the secedit tool with the /export switch.

18.1.3 Security Configuration Editor

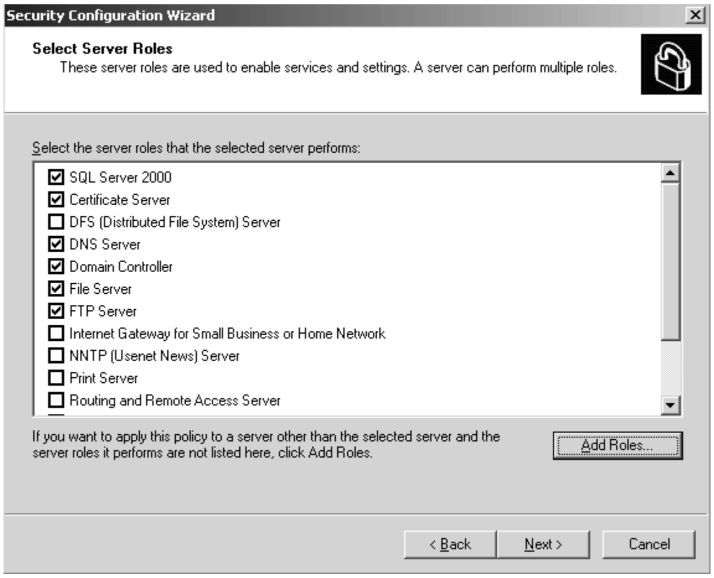
The Security Configuration Editor and Analysis (SCA) tool can be used to edit and analyze the security settings on a Windows 2000, Windows XP, or Windows Server 2003 computer. SCA was introduced in SP4 for NT4; an updated version is provided with Windows 2000, Windows XP, and Windows Server 2003.

Using the SCA, an administrator can validate a computer's security settings against the values defined in a security template. He or she can also enforce the settings following the values defined in a security template. The security templates used by SCA are the ones used by the GPO security policy management section; they were explained in the previous section.

Like the GPO security policy management section, SCA uses the secedit.sdb security database. The SCA engine can be run from the Security Configuration and Analysis MMC snap-in or from the command prompt, using the secedit executable. Table 18.4 shows the secedit switches. Note that the secedit /refreshpolicy switch that was available in Windows 2000 to refresh GPOs has been replaced in Windows Server 2003 by the gpupdate tool.

Table 18.4 *Secedit Switches*

Secedit Switch	Meaning
`/analyze`	Analyze the security settings on a computer against the values defined in a security template.
`/configure`	Configure the security settings on a computer based on the values defined in a security template.
`/export`	Export security settings stored in secedit database.
`/import`	Import a security template into the secedit database.
`/validate`	Validate the syntax of a security template.
`/generaterollback`	Generate a rollback template with respect to a particular security template. When applying a security template to a computer, you have the option of creating a rollback template which, when applied, resets the security settings to the values before the configuration template was applied.



Security Configuration Wizard

Select Server Roles

These server roles are used to enable services and settings. A server can perform multiple roles.

Select the server roles that the selected server performs:

- ☑ SQL Server 2000
- ☑ Certificate Server
- □ DFS (Distributed File System) Server
- ☑ DNS Server
- ☑ Domain Controller
- ☑ File Server
- ☑ FTP Server
- □ Internet Gateway for Small Business or Home Network
- □ NNTP (Usenet News) Server
- □ Print Server
- □ Routing and Remote Access Server

If you want to apply this policy to a server other than the selected server and the server roles it performs are not listed here, click Add Roles.

Figure 18.8 *Security Configuration Wizard.*

18.1.4 Security Configuration Wizard

The Security Configuration Wizard (SCW or secwiz.exe) allows administrators to easily create a baseline security policy for a Windows server based on the server's organizational role. SCW does not provide a complete Windows security policy coverage: instead it focuses on the network-related security policy settings. These include service configuration, and TCP and UDP port usage. The goal of the SCW is to help maximize the security of Windows server systems without sacrificing their required functionality. Microsoft refers to the SCW as a policy authoring tool, whose primary goal is to reduce the Windows attack surface.

The SCW constructs XML-formatted security policies for their different types of servers. These policies can be applied directly to a server using the wizard, or they can be transformed[1] into native scripts or security templates (*.inf) that can then be deployed on individual machines or via Group Policy. The SCW is linked to a database that's referred to as the SCW knowledge base. It is made up of different xml-formatted files. These files are stored in the %windir%/security/ssr/KBs folder (ssr refers to the initial name of the tool: secure server roles) and hold the preferred security policy

[1] At the time of writing, the tool to transform the SCW's XML files to an *.inf file was not yet available.

configuration settings for different server roles. If you want you can add your own SCW knowledge base extensions.

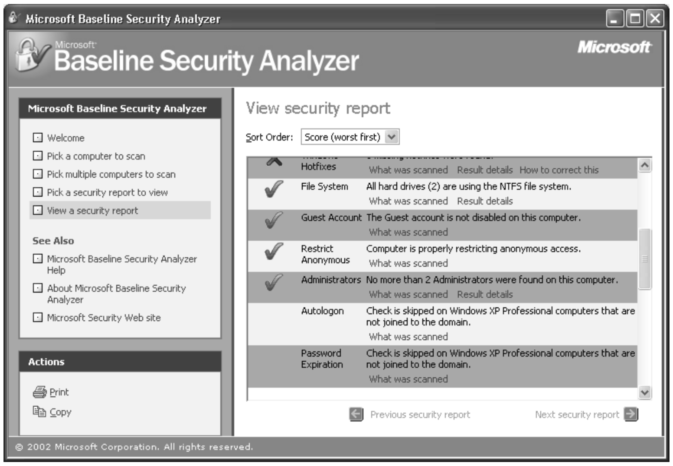
Microsoft makes the Security Configuration Wizard (see Figure 18.8) available as a part of Service Pack 1 (SP1) for Windows Server 2003. SCW supports Windows 2000 and Windows Server 2003.

18.1.5 Microsoft Baseline Security Analyzer

You can use the Microsoft Baseline Security Analyzer (MBSA- mbsa.exe) tool to perform a security scan on NT4 and later Windows systems. The tool can be installed on any Windows 2000 or later system. Although the MBSA tool cannot be installed on an NT4 system, it can be run against an NT4 system that has at least NT4 Service Pack 4 installed. The tool's installation program (an *.msi file) can be downloaded for free from the Microsoft Web site. At the time of writing the latest MBSA release was version 1.1.1.

MBSA is a tool that can be run from both the Windows GUI and the command prompt (mbsacli.exe). It can analyze both the local and remote systems. It can scan for common security misconfigurations in the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS) 4.0, 5.0, and 6.0 SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000 and XP. MBSA can also scan for missing security patches for Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, IIS 4.0, 5.0 and 6.0, SQL Server 7.0 and 2000, Exchange 5.5 and 2000, IE 5.01 and later, and Windows Media Player 6.4 and later. Once a system is analyzed using MBSA, you must use other tools to deploy missing patches to the system (as explained in Section 18.2). More information on the MBSA tool is available in the following Microsoft Knowledge Base article: http://support.microsoft.com/default.aspx?scid=kb;en-us;q320454.

Running a security check against a system using the tool is as simple as starting the tool by double-clicking the desktop shortcut, clicking "Scan a computer," entering the IP address of the computer you want to scan, selecting the scan options (check for Windows vulnerabilities, weak passwords, IIS vulnerabilities, and so forth), and clicking "Start scan." Figure 18.9 shows a report as it is automatically generated by the MBSA tool at the end of a security scan. The MBSA reports are stored in an XML format in the %userprofile%\Securityscans file system folder. To run MBSA, the user must have local administrator access to the computer.


Microsoft Baseline Security Analyzer
Microsoft Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
Previous security report
Next security report

View security report

Sort Order: Score (worst first)

	Hotfixes	What was scanned Result details How to correct this
✓	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
✓	Guest Account	The Guest account is not disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
	Autologon	Check is skipped on Windows XP Professional computers that are not joined to the domain. What was scanned
	Password Expiration	Check is skipped on Windows XP Professional computers that are not joined to the domain. What was scanned

© 2002 Microsoft Corporation. All rights reserved.

Figure 18.9 *Microsoft Security Baseline Analyzer.*

18.1.6 Third-party security policy management tools

Microsoft currently lacks the tools to centralize security policy management and to provide advanced management features such as real-time alerting. Table 18.5 provides a nonexhaustive overview of other third-party management tools that can provide such functionality for the Windows platform.

18.1.7 Security policy management: Overview

Table 18.6 provides an overview of the security policy management tools explained previously and the security policy life cycle phases for which they can be used. A fundamental engine that is called on for most of the security

Table 18.5 *Third-Party Security Policy Management Tools (Nonexhaustive)*

Third-Party Tool	More Information Is Available At…
Bindview Policy Compliance Center, Bindview Bv-Control	http://www.bindview.com/Products/PolicyComp/index.cfm
HP Openview Security Management	http://www.openview.hp.com
NetIQ VigilEnt Policy and Compliance Management	http://www.netiq.com/solutions/security/policy.asp

Table 18.6 *Security Policy Management: Overview*

Security Policy Life Cycle Phase	Tools
Policy Creation	■ Security Configuration and Analysis (SCA) tool ■ Security Configuration Wizard (SCW) ■ Microsoft Baseline Security Analyzer (MBSA) ■ Security Configuration Engine and database
Analysis	■ Security Configuration and Analysis tool (SCA) ■ Microsoft Baseline Security Analyzer (MBSA) ■ Security Configuration Engine and database
Enforcement	■ Group Policy (GPO) ■ Local Security Policy tool ■ Security Configuration Wizard (SCW) ■ Security Configuration Engine and database
Reporting	■ Security Configuration and Analysis tool (SCA) ■ Microsoft Baseline Security Analyzer (MBSA) ■ Security Configuration Engine and database
Monitoring	■ Third-party tools (NetIQ, Bindview, HP Openview)

policy life cycle phases is the security configuration engine and database. This engine and database are available on every Windows 2000, Windows XP, and Windows Server 2003 installation.

18.2 Security patch management

Keeping your systems up-to-date from a security patch point of view is a critical security requirement. Microsoft provides several tools to help with efficient security patch management: the Microsoft Baseline Security Analyzer (MBSA), Windows Update, the Software Update Services (SUS), SUS Feature Pack for SMS 2.0, and the qchain tool. All tools are discussed in more detail next.

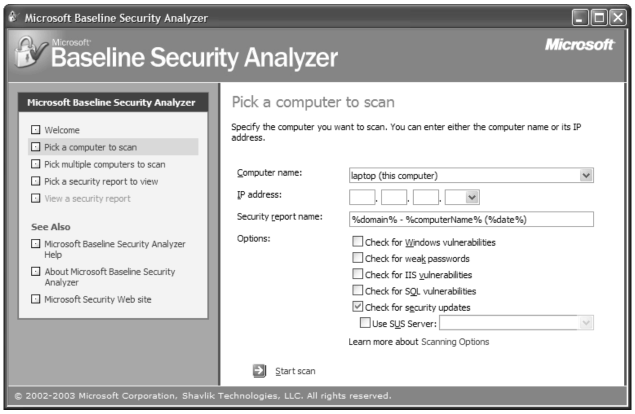
All of these tools rely on the Security Patch Bulletin Catalog (mssecure.xml) to decide upon which security patches are already installed and which patches are required on a system. Every time a patch is installed, all of the tools call on hfnetchk.exe (explained below) to download the latest version of mssecure.xml from the Microsoft Web site.

18.2.1 Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MBSA) was discussed earlier in Section 18.1.5. It also provides security patch scanning functionality. When starting a scan from the MBSA GUI, you have the option to check for security updates (as illustrated in Figure 18.10). When running MBSA from the command line (using mbsacli.exe), you must use the /hf switch to scan a machine's security patch status. Once a system is analyzed using MBSA, you must use other tools to deploy the missing patches to the system. To do so, you can use one of the tools explained next.

The command-line version of MBSA (mbsacli.exe) builds on an earlier MS scan tool, HFnetchk.exe, for its security patch management functionality. HFnetchk.exe is also known as the hotfix network checker. This tool was developed for Microsoft by a company called Shavlik. Microsoft does not provide updates to HFnetchk anymore; however, an up-to-date version of the tool can be downloaded from the Shavlik Web site at http://www.shavlik.com. Shavlik also provides an advanced version of the HFnetchk tool, called HFnetchkPro. This is a GUI tool that allows for the distribution and installation of missing security patches after an HFnetchk scan (something that cannot be done with MBSA).

MBSA can be integrated with the Microsoft Software Update Services (SUS)—SUS is explained in more detail in Section 18.2.3. This means that MBSA can check the enterprise SUS server for security updates instead of going to the Microsoft Web site. MBSA will automatically call upon the enterprise SUS server when its location has been configured in the system


Microsoft Baseline Security Analyzer
Microsoft Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Start scan

Pick a computer to scan

Specify the computer you want to scan. You can enter either the computer name or its IP address.

Computer name: laptop (this computer)

IP address: . . .

Security report name: %domain% - %computerName% (%date%)

Options:
☐ Check for Windows vulnerabilities
☐ Check for weak passwords
☐ Check for IIS vulnerabilities
☐ Check for SQL vulnerabilities
☑ Check for security updates
☐ Use SUS Server:

Learn more about Scanning Options

© 2002-2003 Microsoft Corporation, Shavlik Technologies, LLC. All rights reserved.

Figure 18.10 *Checking for security updates from the MBSA.*

registry (this can be done using GPOs; see SUS section below). You can also force MBSA to go to a particular SUS server by typing the following at the command line:

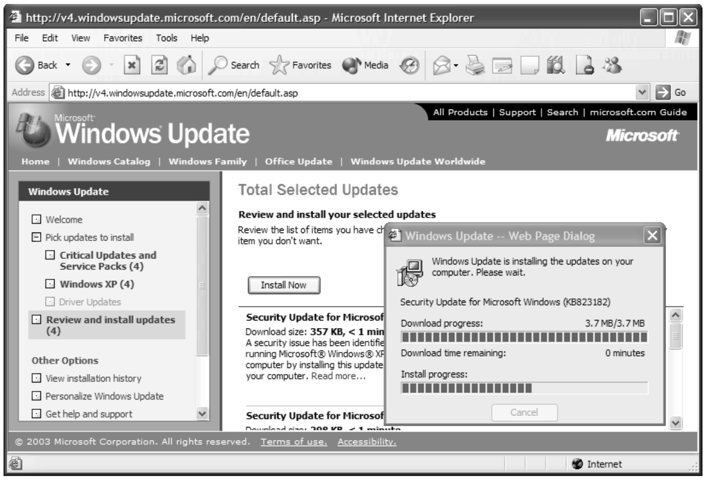
```
Mbsacli.exe /hf /sus "http://<SUS_server_FQDN>".
```

The key difference with using MBSA without SUS is that SUS-rooted MBSA scans will only include enterprise-level approved security updates as they are available on the SUS server rather than all available updates available on the Windows Web site.

MBSA is also compatible with the SMS SUS feature pack (explained in Section 18.2.4). SMS can be used to push mbsacli.exe to all clients and perform a local security patch scan. SMS can then distribute all missing security patches to the clients.

18.2.2 Windows Update

The Windows Update service allows Windows 98, Windows 2000, Windows Me, Windows XP, and Windows Server 2003 users to easily download and install the latest Microsoft security patches. User can manually initiate a Windows Update sequence by selecting Windows Update from the Windows Start Menu, by going to the http://windowsupdate.microsoft.com URL in Internet Explorer or by running wupdmgr.exe from the command line. Windows Update will then connect to the Microsoft Windows Update Web site (illustrated in Figure 18.11) on the Internet. On this Web site, users must run through a set of steps to update their system: Initiate a scan



http://v4.windowsupdate.microsoft.com/en/default.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://v4.windowsupdate.microsoft.com/en/default.asp Go
All Products | Support | Search | microsoft.com Guide
Microsoft Windows Update
Microsoft
Home | Windows Catalog | Windows Family | Office Update | Windows Update Worldwide
Windows Update
Welcome
Pick updates to install
Critical Updates and Service Packs (4)
Windows XP (4)
Driver Updates
Review and install updates (4)
Other Options
View installation history
Personalize Windows Update
Get help and support
Install Now
Windows Update -- Web Page Dialog
Cancel
© 2003 Microsoft Corporation. All rights reserved. Terms of use. Accessibility.
Internet

Total Selected Updates

Review and install your selected updates

Review the list of items you have ch
item you don't want.

Security Update for Microsof
Download size: 357 KB, < 1 min
A security issue has been identifie
running Microsoft® Windows® XP
computer by installing this update
your computer. Read more...

Security Update for Microsof

Windows Update is installing the updates on your computer. Please wait.

Security Update for Microsoft Windows (KB823182)

Download progress: 3.7 MB/3.7 MB

Download time remaining: 0 minutes

Install progress:

Figure 18.11
Windows Update.

(by clicking "Scan for updates"), pick the updates to install, review them, and then install the updates. Windows Update provides a patch classification system: Users must make sure they always install at least the critical patches.

Because Windows Update is a Web-based tool, it can only work if the following conditions are met:

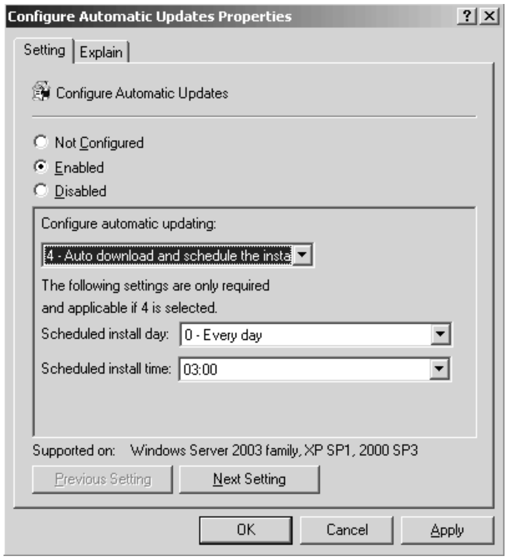
- Internet Explorer must support cookies. IE cookie-related behavior is configured from the Privacy tab in the IE Internet Options.
- Internet Explore must allow ActiveX controls. IE ActiveX-related behavior is configured in the IE Security Zone properties.
- The user initiating a Windows Update sequence must be a member of the local Administrators group.

Windows Update can also be configured to run automatically at predefined intervals. This feature is referred to as automatic patch updating and is only available on Windows 2000 Service Pack 3 and later, Windows XP, and Windows Server 2003 systems. Automatic patch updating can be configured in different ways:

- From the properties of the My Computer object in Windows XP, Windows 2000, and Windows Server 2003. These properties are also accessible from the System Control Panel applet.
- From the Automatic Updates Control Panel applet in Windows 2000 Service Pack 3 or later
- From the system registry
- From the GPO settings (as illustrated in Figure 18.12) in Windows Server 2000 and Windows Server 2003

In all four cases, you have the option to enable or disable automatic patch updating. If you enable it, the Windows Update can notify users for both patch download and install, notify only for install, or automatically perform both the patch download and install.

To configure automatic updates from the registry (e.g., in non-AD environments), use the keys listed in Table 18.7. These keys are all located in the HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate registry container. When automatic update has been configured for notification when installing only (AUOptions value 3), a dialog box similar to the one in Figure 18.13 will be presented to the user.



Configure Automatic Updates

○ Not Configured
● Enabled
○ Disabled

Configure automatic updating: 4 - Auto download and schedule the insta

The following settings are only required and applicable if 4 is selected.

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

Supported on: Windows Server 2003 family, XP SP1, 2000 SP3

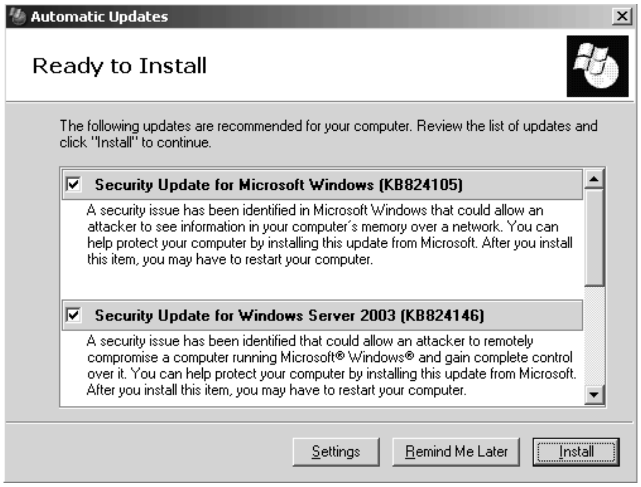
Figure 18.12 *Configuring automatic patch updates using GPO.*

18.2.3 Software Update Services

Software Update Services (SUS) builds on the Windows Update service. It gives enterprise administrators the ability to provide Windows Update–based security patch services in a controlled and secure manner. SUS can be used to set up an enterprise Windows Update server from which internal

Table 18.7 *Automatic Update Registry Keys*

Registry Key	Values and Meaning
NoAutoUpdate (REG_DWORD)	1: Automatic updates are enabled.
AUOptions (REG_DWORD)	2: Notify for download and install 3: Notify for install only 4: Automatically perform download and install following a predefined schedule
ScheduledInstallDay (REG_DWORD)	Specifies day for scheduled automatic update. 0 means every day, 1 means Sunday, … , 7 means Saturday.
ScheduledInstallTime(REG_DWORD)	Specifies time for scheduled automatic update. Holds a value ranging from 0 to 23.



Ready to Install

The following updates are recommended for your computer. Review the list of updates and click "Install" to continue.

☑ **Security Update for Microsoft Windows (KB824105)**

A security issue has been identified in Microsoft Windows that could allow an attacker to see information in your computer's memory over a network. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

☑ **Security Update for Windows Server 2003 (KB824146)**

A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft® Windows® and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Figure 18.13
Automatic updates dialog box.

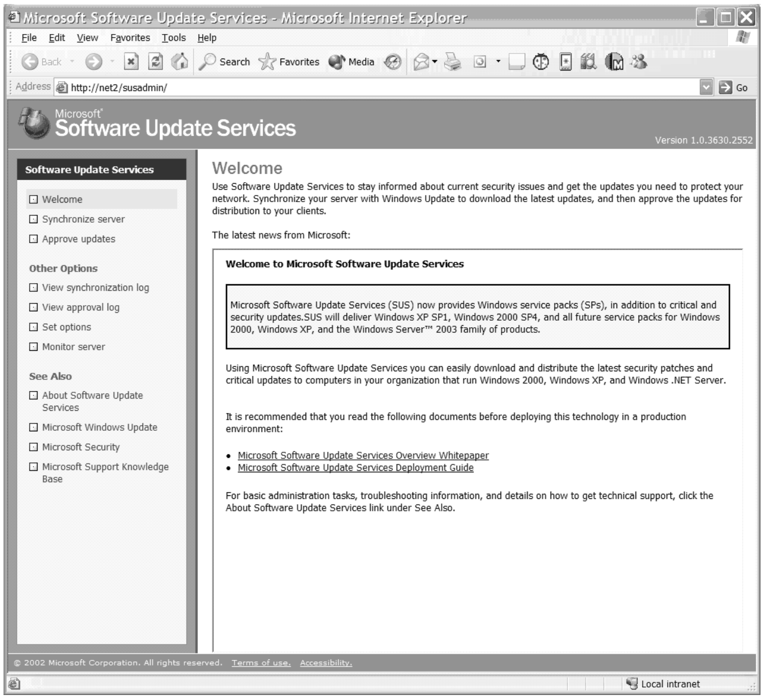
Windows clients can download the latest patches. To receive security patch updates, the internal Windows Update server obviously links up to the MS Windows Update infrastructure.

The SUS software is a free download available from http://www.microsoft.com/downloads/recommended/susserver. SUS requires IE 5.5 or later, IIS 5.0 or IIS 6.0, Windows 2000, or Windows Server 2003 and cannot be installed on a domain controller. It can distribute patches to Windows 2000, Windows XP, and Windows Server 2003 platforms.

SUS configuration and administration options are accessible from the SUS Administration Web page (http://<SUSServerName>/susadmin). To set configuration options, click the Set Options hyperlink (illustrated in Figure 18.14). To update the SUS server patch data, click the Synchronize Server hyperlink.

SUS also provides a security patch staging solution: It allows the SUS administrator to define which security patches are approved for distribution to its Windows clients. To approve patches, click the Approve Updates hyperlink on the SUS Administration Web page. Unlike the SUS Feature Pack for SMS 2.0 (explained next), SUS cannot define which client gets which updates. Every client that connects to the SUS server gets all approved security patches.

The SUS server used by a Windows client can be configured using GPO settings (Computer Configuration\Administrative Templates\Windows Components\Windows Update\Specify intranet Microsoft update



Microsoft Software Update Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://net2/susadmin/
Go
Microsoft
Software Update Services
Version 1.0.3630.2552

Software Update Services

- □ Welcome
- □ Synchronize server
- □ Approve updates

Other Options

- □ View synchronization log
- □ View approval log
- □ Set options
- □ Monitor server

See Also

- □ About Software Update Services
- □ Microsoft Windows Update
- □ Microsoft Security
- □ Microsoft Support Knowledge Base

Welcome

Use Software Update Services to stay informed about current security issues and get the updates you need to protect your network. Synchronize your server with Windows Update to download the latest updates, and then approve the updates for distribution to your clients.

The latest news from Microsoft:

Welcome to Microsoft Software Update Services

Microsoft Software Update Services (SUS) now provides Windows service packs (SPs), in addition to critical and security updates.SUS will deliver Windows XP SP1, Windows 2000 SP4, and all future service packs for Windows 2000, Windows XP, and the Windows Server™ 2003 family of products.

Using Microsoft Software Update Services you can easily download and distribute the latest security patches and critical updates to computers in your organization that run Windows 2000, Windows XP, and Windows .NET Server.

It is recommended that you read the following documents before deploying this technology in a production environment:

- Microsoft Software Update Services Overview Whitepaper
- Microsoft Software Update Services Deployment Guide

For basic administration tasks, troubleshooting information, and details on how to get technical support, click the About Software Update Services link under See Also.

© 2002 Microsoft Corporation. All rights reserved. Terms of use. Accessibility.

Figure 18.14 *SUS administration interface.*

service location). In non-AD environments, you can configure the Windows clients' SUS server using the registry keys illustrated in Table 18.8. These keys are all located in the HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate registry container.

18.2.4 SUS Feature Pack for SMS 2.0

The SMS Software Update Services (SUS) Feature Pack is Microsoft's most advanced security patch management tool. It provides the ability to determine security patch status, distribute patches, install patches, and generate

Table 18.8 *SUS Client Registry Keys*

Registry Key	Values and Meaning
UseWUServer (REG_DWORD)	1: use a SUS server
WUServer (REG_SZ)	Contains URL of SUS server
WUStatusServer (REG_SZ)	Contains URL of SUS statistics server

reports on the patch status. Unlike any of the other patch management tools discussed so far, the SMS SUS Feature Pack allows an administrator to identify and target specific computers for security patch updates. For example, it allows for the deployment of a specific set of patches to a subset of the machines in an enterprise.

SMS SUS Feature Pack also provides security patch update facilities for Windows platforms other than Windows XP, Windows 2000, and Windows Server 2003. Unlike SUS, SMS can also distribute and install service packs (SPs). Microsoft recommends using SMS and the SMS SUS Feature Pack when distributing patches to more than 5,000 computers. The SUS Feature Pack is specifically made for SMS version 2.0 Service Pack 3 or later. The complete Feature Pack's functionality will be an integral part of the SMS 2003 release.

The SMS SUS Feature Pack consists of four major components: the Security Update Inventory tool (uses MBSA 1.1), the MS Office Inventory tool, the Distribute Software Updates wizard, the Software Updates Installation Agent and the SMS Web Reporting tool. The SUS Feature Pack can be downloaded for free from http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/. This URL also includes pointers to the SUS Feature Pack deployment guide.

18.2.5 Qchain

Qchain allows you to install multiple security patches in a single installation run. This eliminates the need for several system reboots. Qchain works for NT 4.0, Windows 2000, Windows XP, and Windows Server 2003. The tool evaluates all of the patch components (DLLs, executables, and so forth) and makes sure that only the most recent versions of the components are installed. The following is a sample batch file script that can be used to install two security patches using qchain:

```
@echo off
setlocal
set PATHTOFIXES=c:\systemfixes
%PATHTOFIXES%\Q123456_w2k_sp1_x86.exe -z -m
%PATHTOFIXES%\Q123457_w2k_sp1_x86.exe -z -m
%PATHTOFIXES%\qchain.exe
```

In this command the –z switch prevents reboots, and the –m switch enables unattended installation. More information on the tool is available in MS Knowledge Base article Q296861.

Table 18.9 *Third-Party Security Patch Management Software*

Company	Product	URL
Altiris, Inc.	Altiris Patch Management	http://www.altiris.com
BigFix, Inc.	BigFix Patch Manager	http://www.bigfix.com
BMC Software	Patrol	http://www.bmc.com/patrol
Computer Associates	Unicenter	http://www.ca.com/unicenter
Configuresoft, Inc.	Security Update Manager	http://www.configuresoft.com
Ecora, Inc.	Ecora Patch Manager	http://www.ecora.com
GFI Software, Ltd.	GFI LANguard Network Security Scanner	http://www.gfi.com
Gravity Storm Software, LLC	Service Pack Manager 2000	http://www.securitybastion.com
Hewlett-Packard	Openview	http://openview.hp.com
IBM	Tivoli	http://www.ibm.com/tivoli
LANDesk Software, Ltd	LANDesk Patch Manager	http://www.landesk.com
Novadigm, Inc.	Radia Patch Manager	http://www.novadigm.com
PatchLink Corp.	PatchLink Update	http://www.patchlink.com
Shavlik Technologies	HFNetChk Pro	http://www.shavlik.com
St. Bernard Software	UpdateExpert	http://www.stbernard.com

18.2.6 Third-party security patch management tools

Table 18.9 gives an overview of third-party security patch management tools. It is beyond the goals of this book to cover these products in more detail.

18.3 Security-related auditing

The auditing system of an operating system keeps track of all activities that occur on a computer system. It gathers not only security-related information, but also application- and system service-related information.

18.3.1 The Event Viewer and the Event Logs

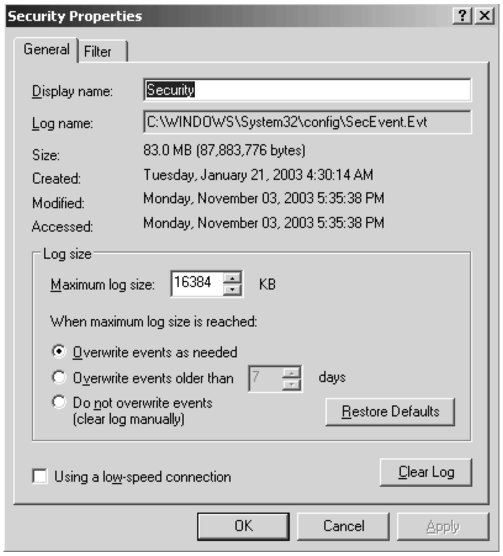
When discussing auditing in Windows Server 2003, we must address two topics: Event Logs and the Event Viewer. Windows Server 2003 gathers all events in Event Log files. By default, these files (*.evt) are located in the <%systemdirectory%>\config\ subdirectory. The default log files are named Appevent.evt, Secevent.evt, Sysevent.evt, ntds.evt, dnsevent.evt, and ntfrs.evt. The Event Logs are governed and fed by a system's Local Security Authority (LSA); see Chapter 2 for information on the LSA.

The Event Viewer is Windows' primary Event Log viewer. The Event Viewer also allows you to filter the Event Logs and display only certain categories of events. For every Event Log entry, the Event Viewer shows an event description, the account that caused the event, the event type (warning, error, or information), the event ID, the source of the event (originating service), and the date and time of the event. From a troubleshooting point of view, the event description and the event ID are the most important fields. The event ID allows you to uniquely identify the event so you can, for example, look up its meaning in the Microsoft Knowledge Base. Earlier chapters of this book contain examples of event IDs related to specific security processes. For example, for logon-related event IDs, see Chapter 4.

You may have some difficulty locating the Event Viewer in the Windows 2000, Windows XP, and Windows Server 2003 interface. It is now integrated with the Computer Management MMC snap-in. You can also view it from the Event Viewer MMC snap-in. As in NT4, you can launch the event viewer from the command prompt by typing eventvwr.

Compared to its NT4 predecessor, the Event Viewer has been extended: It includes a set of new folders to gather auditing information related to OS core services such as the Directory Service, the DNS Service, and the File Replication Service. Also, the description portion of the events has been extended, facilitating troubleshooting. Some events even include an HTTP pointer to the Microsoft online support site. Last but not least, the event logs can now also be accessed using a WMI (Windows Management Instrumentation) management interface.

Like NT4, the Event Viewer includes an application (to log application-specific information), security (to log security events), and system log (to log system-related events). The application log entries are fixed and set by the application developer. The system log entries are fixed as well and set by the OS. By default, no security entries are logged. The security entries that are logged can be configured by an administrator, as is explained in the next section. An important exception to this in Windows Server 2003 is domain controllers: They now have security auditing enabled by default for successful account logon and logon events.



Display name: Security

Log name: C:\WINDOWS\System32\config\SecEvent.Evt

Size: 83.0 MB (87,883,776 bytes)

Created: Tuesday, January 21, 2003 4:30:14 AM

Modified: Monday, November 03, 2003 5:35:38 PM

Accessed: Monday, November 03, 2003 5:35:38 PM

Log size

Maximum log size: 16384 KB

When maximum log size is reached:

● Overwrite events as needed

○ Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection

Figure 18.15 *Security event log properties.*

The Windows Server 2003 Event Log files have, like their NT4 and Windows 2000 predecessors, a limited size. In Windows Server 2003, the default log file size has been increased to 32 Mb; In earlier Windows versions (including Windows 2000 and Windows XP), this was 512 Kb. The maximum log size has been increased to 4 Gb. The size of a log file can be set per individual event viewer container, as illustrated in Figure 18.15 for the Security event log container. Because all event logs are permanently kept open in system memory, the practical maximum log file size limit is around 300 Mb.

To cope with this limited size, different retention policies can be set per individual container:

- Overwrite events as needed: When this option is set, the oldest events will automatically be overwritten with newer events when the log file fills up. Keeping in mind the above practical log file size limit (300 Mb each), "overwrite events as needed" is the recommended retention policy. This is not true for systems that have the crashonauditfail security policy option enabled (this option is explained below).
- Overwrite events older than X days: When this option is set, only events older than X days will be overwritten. If all events older than X days are overwritten, no more events are logged. Logging will start again from the moment some older events expire (or reach the X days limit).

- Do not overwrite events: When this option is set, no events are overwritten. When the log is full, logging stops. Logging can only be started again by manually clearing the logs.

A critical event log file is the security log. To read and clear the security logs of a Windows system of a Windows system, a user must have the "Manage auditing and security log" user right (SeSecurityPrivilege). By default, this privilege is given only to members of the Administrator group. To write to the security log, you must have the "Generate security audits" user right (SeAuditPrivilege). In addition to using these two user rights, you can also modify the access control permissions on the security event log file (secevent.evt) to better protect against unauthorized access to the security event log.

Both the Security Configuration and Analysis (SCA) tool and the security portion of the Windows Server 2003 GPOs include important event logging-related configuration settings. The settings are listed in Table 18.10, together with their corresponding registry entry. The first four settings can be set for the application, security, and system log and are set from the Event Log container in the Security Settings. The last three can be set from the Security Options in the Security Settings' Local Policies container. Table 18.11 lists the recommended values for these settings for Windows Server 2003 Domain Controllers and Member Servers.

Table 18.10 *Event Logging-Related Registry Hacks*

Setting	Registry Entry:
	HKLM\System\CurrentControlSet\Services\Eventlog\<log name>
Maximum log size	MaxSize (REG_DWORD)
Restrict local guests group from accessing log	RestrictGuestAccess (REG_DWORD)
Retain log	Retention (REG_DWORD)
Retention method for log	Retention (REG_DWORD)
	HKLM\System\CurrentControlSet\Control\LSA\
Audit: Audit the access of global system objects	Auditbaseobjects (REG_DWORD)
Audit: Audit the use of Backup and Restore privilege	Fullprivilegeauditing (REG_BINARY)
Audit: Shut down system immediately if unable to log security audits	CrashOnAuditFail (REG_DWORD):

Table 18.11 *Event Logging-Related Registry Hacks Recommended Settings*

Setting	Recommendation for Domain Controllers	Recommendation for Member Servers
Maximum log size	32 Mb for System, Application, and Security logs; make sure that no log data are lost by backing up the log files at regular intervals	16,384 Kb for System, Application, and Security logs; make sure that no log data are lost by backing up the log files at regular intervals
Restrict local guests group from accessing log	Enabled for System, Application, and Security logs	Enabled for System, Application, and Security logs
Retain log (Retention method for log)	Overwrite as needed for System, Application and Security logs.	Overwrite as needed for System, Application and Security logs.
Audit: Audit the access of global system objects	Disabled	Disabled
Audit: Audit the use of Backup and Restore privilege	Enabled	Disabled
Audit: Shut down system immediately if unable to log security audits	Depends on importance of AD data	Disabled

RestrictGuestAccess and CrashOnAuditFail are two critical parameters from a security point of view. RestrictGuestAccess prohibits members of the Guests group to view the information in one of the event log containers.

CrashOnAuditFail prevents that unauthorized actions can occur when they cannot be logged in the security log. When it is enabled, Windows will crash the computer if it is unable to write an event to the event logs. The system crash occurs as a blue screen that contains a STOP error code and displays {Audit Failed} along with a description of why the audit failed. When the computer crashes, the CrashOnAuditFail value is automatically changed from 1 to 2 and the type of CrashOnAuditFail registry entry is changed from REG_DWORD to REG_NONE. After a CrashOnAuditFail-initiated crash, only a local administrator or a member of the Domain Admins group can log in. Before other users are allowed to log back in, the CrashOnAuditFail registry value must be deleted and readded to the system registry as a REG_DWORD with a value of either 0 or 1.

18.3.2 Setting up security-related auditing

The security auditing system in Windows Server 2003 is very closely related to the access control system. Like access control settings, auditing settings can be set on individual objects and are stored in an object's security descriptor. Each time an object is accessed, its auditing settings are checked to see whether this type of access needs to be audited. Next we will focus on how to set up security-related auditing in Windows Server 2003.

To set up security event logging, you must define a security audit policy and set auditing properties for several event categories on the object level. Once set up, Windows will log the security-related events to the security container of the Event Viewer. To look at the content of this container, you must be a local administrator on the system.

A Windows Server 2003 audit policy defines which categories of audit events will be recorded in a computer's local security log. It is defined through Group Policy Object settings on the domain, site, or OU level. You can find the audit policy in the GPO computer configuration, underneath Windows Settings\Security Settings\Local Policies\Audit Policy. You can also set the audit policy locally using the Local Security Policy configuration tool.

Table 18.12 shows the event categories that can be logged. For all categories, you can set auditing for both successful and failed attempts. Table 18.13

Table 18.12 *Audit Policy Categories*

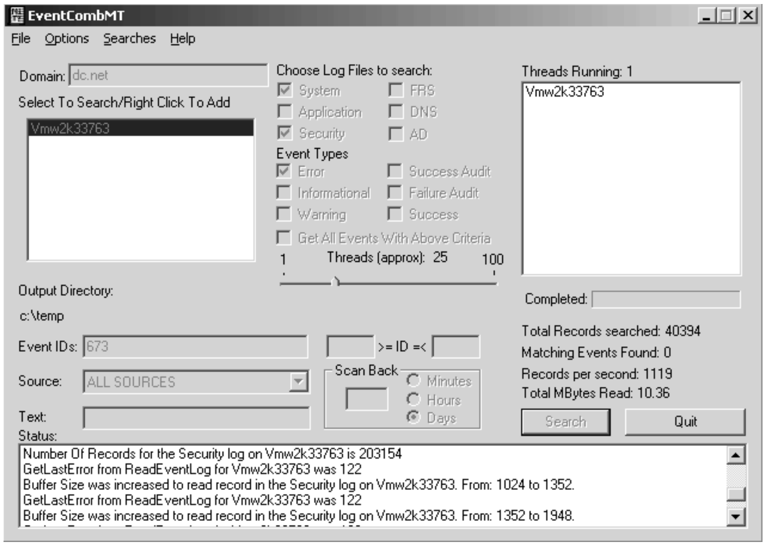
Audit Policy Category	Meaning
Audit Account Logon Events	Monitors logon attempts against a Windows security database (SAM or AD).
Audit Account Management	Monitors creation, deletion, and modification of security principals (user, computer, and group accounts).
Audit Directory Service Access	Monitors administrative access to AD objects in the configuration and schema naming contexts. The domain naming context is covered by the "Audit Account Management" category.
Audit Logon Events	Logs events at the machine where the authentication takes place. During an interactive logon this is at the local computer. During a network login, this is at the machine where the resource is located.
Audit Object Access	Monitors access to all objects that have a system ACL (SACL).
Audit Policy Change	Logs events for audit policy changes.
Audit Privilege Use	Logs events when a security principal exercises a user right.
Audit Process Tracking	Logs events for attempts to create and end processes.
Audit System Events	Logs events for changes to the computer's operating environment. This includes changing the system time, clearing the security event log, and shutting down the computer.

Table 18.13 *Recommended Audit Policy for Domain Controllers and Members Servers*

Audit Policy Category	Domain Controller Configuration	Member Server Configuration
Audit Account Logon Events	Success, Failure	Success, Failure
Audit Account Management	Success, Failure	Success, Failure
Audit Directory Service Access	Failure	Failure
Audit Logon Events	Success, Failure	Success, Failure
Audit Object Access	Success, Failure	Success, Failure
Audit Policy Change	Success, Failure	Success, Failure
Audit Privilege Use	Failure	Not enabled
Audit Process Tracking	Not enabled	Not enabled
Audit System Events	Success, Failure	Success, Failure

shows the recommended audit settings for Windows Server 2003 domain controllers and member servers.

To set up auditing on the object level, right-click the object and select properties; then open up the Security tab, click Advanced, and select the Auditing tab. You will see that you can set up auditing based on the account or group performing an action and the type of action being performed (as



Domain: dc.net
Select To Search/Right Click To Add
Vmw2k33763

Choose Log Files to search:
☑ System ☐ FRS
☐ Application ☐ DNS
☑ Security ☐ AD

Event Types
☑ Error ☐ Success Audit
☐ Informational ☐ Failure Audit
☐ Warning ☐ Success
☐ Get All Events With Above Criteria

1 Threads (approx): 25 100

Threads Running: 1
Vmw2k33763

Output Directory:
c:\temp

Event IDs: 673
>= ID =<
Source: ALL SOURCES
Text:

Scan Back
○ Minutes
○ Hours
● Days

Completed:
Total Records searched: 40394
Matching Events Found: 0
Records per second: 1119
Total MBytes Read: 10.36

Status:

```
Number Of Records for the Security log on Vmw2k33763 is 203154
GetLastError from ReadEventLog for Vmw2k33763 was 122
Buffer Size was increased to read record in the Security log on Vmw2k33763. From: 1024 to 1352.
GetLastError from ReadEventLog for Vmw2k33763 was 122
Buffer Size was increased to read record in the Security log on Vmw2k33763. From: 1352 to 1948.
```

Figure 18.16 *The eventcombmt tool.*

illustrated in Figure 18.16). As with authorization, Microsoft included some important object auditing changes in Windows 2000 and Windows Server 2003:

- Windows 2000 and Windows Server 2003 permit a much finer granularity for object and property auditing than NT4. Just as with access control, auditing settings can be defined based on object types and object properties.
- Windows 2000 and Windows Server 2003 include the capability to define auditing setting inheritance between parent and child objects.
- The object auditing administration interface has been extended to reflect the changes mentioned previously and is integrated with the new ACL editor.

18.3.3 Event log–related tools

To archive the log file content, you can rely on your standard backup utility. To make sure that no log entries are lost, you must align the log settings described earlier with the archival procedure. To dump the content of the event log, you can use command-line tools such as Microsoft's dumpel.exe or Systinternals' psloglist.exe. The first one can be downloaded from the MS Downloads Web site. The second one is available from the Sysinternals Web site. The following dumpel command will dump all events in the security log on a server named Myserver to a file named security.xls:

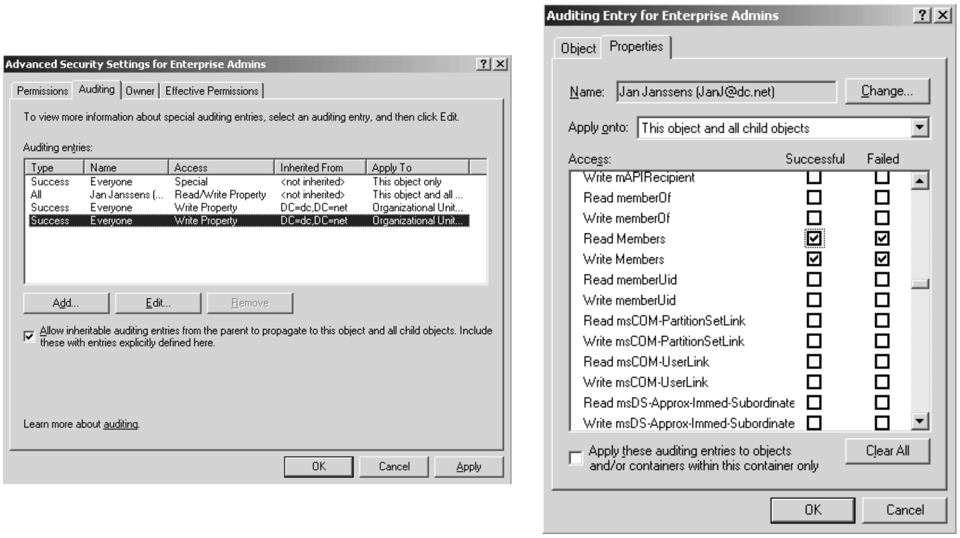
```
dumpel -f security.xls -s myserver -l security
```

Dumpel can also filter out certain event types when it dumps the event log content. For example, to filter out event ID 528 in the above example, type:

```
dumpel -f security.xls -s myserver -l security -e 528
```

A great resource kit tool to query the local and remote event logs is the eventcombmt.exe (illustrated in Figure 18.17) Resource Kit utility. It allows an administrator to look for occurrences of a single event ID, multiple event IDs, a range of event IDs, specific event types or sources, or a specific event message text. The eventcombmt tool drops the results of its query in the eventcombmt.txt file in a system's temporary folder.

A brand-new tool is the Microsoft Audit Collection System (MACS), which provides a security log collection service. MACS facilitates role separation between Windows system administrators and IT system auditors. Before MACS, Microsoft customers had to turn to products like Sentry or



To view more information about special auditing entries, select an auditing entry, and then click Edit.

Auditing entries:

Type	Name	Access	Inherited From	Apply To
Success	Everyone	Special	<not inherited>	This object only
All	Jan Janssens (...	Read/Write Property	<not inherited>	This object and all ...
Success	Everyone	Write Property	DC=dc,DC=net	Organizational Unit...
Success	Everyone	Write Property	DC=dc,DC=net	Organizational Unit...

☑ Allow inheritable auditing entries from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

Learn more about auditing.

Name: Jan Janssens (JanJ@dc.net)

Apply onto: This object and all child objects

Access:	Successful	Failed
Write mAPIRecipient	☐	☐
Read memberOf	☐	☐
Write memberOf	☐	☐
Read Members	☑	☑
Write Members	☑	☑
Read memberUid	☐	☐
Write memberUid	☐	☐
Read msCOM-PartitionSetLink	☐	☐
Write msCOM-PartitionSetLink	☐	☐
Read msCOM-UserLink	☐	☐
Write msCOM-UserLink	☐	☐
Read msDS-Approx-Immed-Subordinate	☐	☐
Write msDS-Approx-Immed-Subordinate	☐	☐

☐ Apply these auditing entries to objects and/or containers within this container only

Figure 18.17 *Setting up auditing.*

Microsoft MOM to provide this kind of functionality. MACS is made up of a client (the MACS agent) and a server component (the MACS collector). The MACS server stores the security log data in a SQL Server or MSDE database. Transport of the log data happens in a secure way. MACS agents locate the MACS collector using a DNS SRV record (named _adtserver). Here MACS agents can authenticate to the MACS collector using Kerberos or SSL (in non-domain environments). MACS provides an API that can be used by application developers to build host-based intrusion detection systems (IDSs). MACS is an add-on service to Windows Server 2003. The first release of the service will be made available as a free Web download; later releases may be integrated with the Microsoft Operations Manager (MOM). At the time of writing, MACS was planned to run on Windows 2000, Windows XP, and Windows Server 2003.