CHAPTER 9

Network Security

When constructing a Windows XP Professional network, security must be managed on two fronts: at the local computer level and at the network level. This chapter examines both areas, first with a discussion of Windows XP Professional, and then with a discussion of server security.

WINDOWS XP PROFESSIONAL SECURITY FEATURES

Windows XP Professional keeps your system safe and secure in a number of ways. Not only are there tried-and-true security measures that are holdovers from earlier versions of Windows, there are also new features that enhance security. We'll talk about managing local security policies, logging, Internet Connection Firewall Security Logs, security templates, the logon process, and finally security configuration and analysis. Not only can these tools be used for managing Windows XP Professional security, but some can be used for managing security settings in a domain as well.

First, however, let's start with an overview of Windows XP Professional's security improvements.

What's New in Windows XP Professional

Windows security is a moving target. That is, whenever a new version of Windows is released, you can expect that it will include significant security improvements as part of the upgrade. Windows XP Professional is no exception.

Windows XP Professional still carries over most of the popular security features found on Windows NT and Windows 2000, but it offers new features, including these:

- **Administrative ownership** In earlier versions of Windows, any resources created by the administrator (such as files and folders) were shared by the entire group. However, in Windows XP Professional, these resources belong to the individual administrator who created them.
- **Encrypting File System (EFS) recovery agent** In Windows 2000, if you try to configure an EFS recovery policy with no recovery agent certificates, then EFS is automatically disabled. In Windows XP Professional, you can encrypt files without a Data Recovery Agent (DRA).
- **Printer installation** Only administrators and power users are able to install local printers. Administrators have this ability, by default, but power users must be granted this privilege.
- **Blank password limitation** Windows XP Professional users can use blank passwords; however, they are only able to log in, physically, at the local computer.
- **Software restriction** Windows XP Professional security policies can be assigned to specified applications based on a file path, Internet zone, or certificate.

- **Fast user switching** On Windows XP Professional machines that are not connected to a domain, the computer can switch from one user to another without having to log off or close applications.
- **Password Reset Wizard** In the event a user forgets his or her password, that user can use a reset disk to access his or her local account.

The following sections examine some of these topics in more depth, whereas others are self-explanatory and occur on the Windows XP Professional system by default.

Local Security Policy

The ability to create and manage security policies on a local computer is accomplished via a snap-in to the MMC. The snap in will allow you to not only view the local security policy, but also make changes to it.

Viewing

To view the security policy settings on a Windows XP Professional computer, select Start | Control Panel | Performance and Maintenance | Administrative Tools. Double-click Local Security Policy. The resulting screen is shown in Figure 9-1.

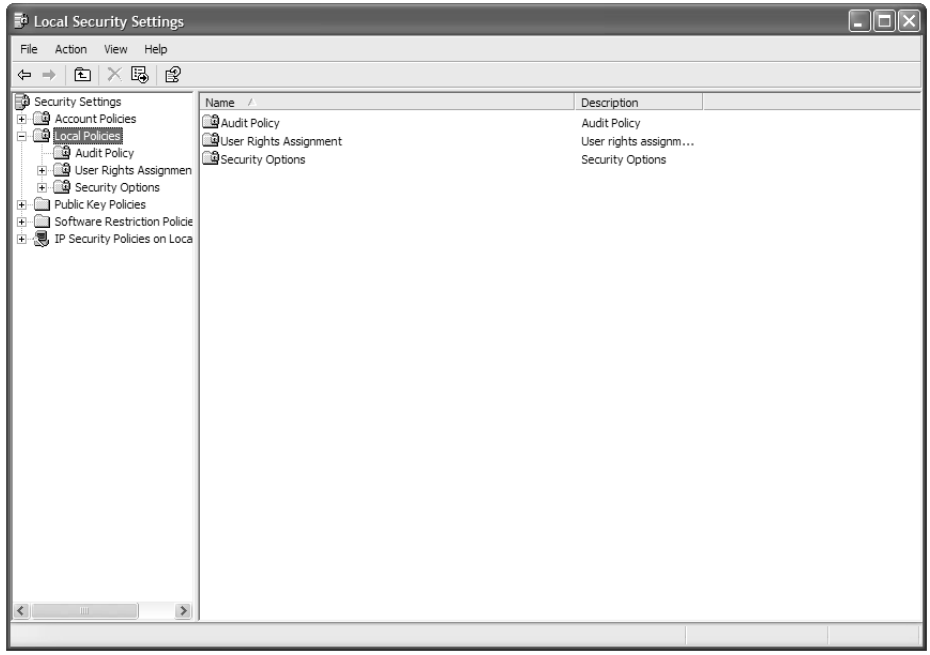

Figure 9-1. Viewing local security policy

NOTE You can also start this tool from the command line by entering **secpol.msc**.

Managing Local Policies

To view individual security policies, double-click the icon of the security topic you wish to examine. For example, the following steps illustrate how to manage security settings under the Security Options folder. Once you've double-clicked Security Options, a list of security settings appears, as shown in Figure 9-2.

Next, click the setting Devices: Unsigned driver installation behavior. As Figure 9-3 shows, there are three choices for this setting's behavior.

- Silently succeed
- Warn, but allow installation
- Do not allow installation

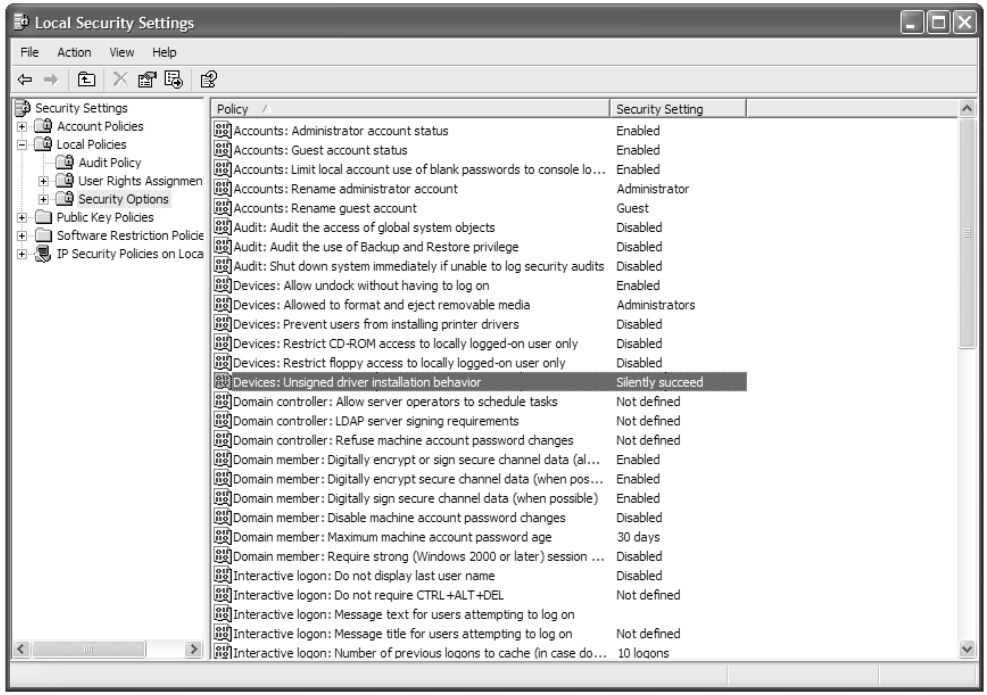

Figure 9-2. Security settings contained in the Security Options local policy folder

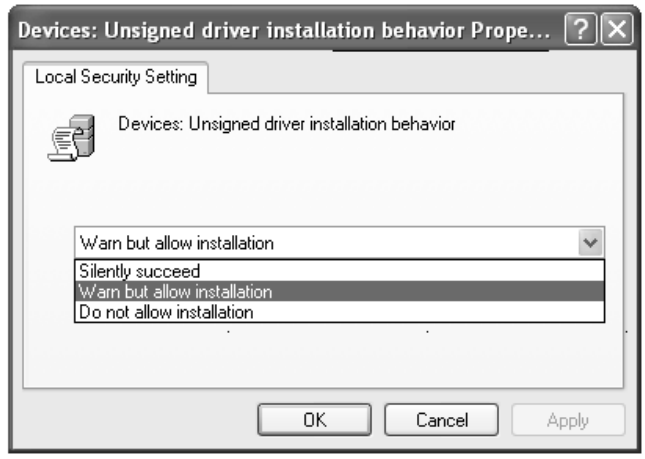

Figure 9-3. Expanded setting details

ICF Security Logging

In Chapter 5, we talked about the basic usage and management of Windows XP Professional's Internet Connection Firewall (ICF). Several additional security features in the realm of logging will make your ICF experience more useful.

The ICF security log allows you to generate a list of your firewall's activity—namely, whether traffic is permitted or rejected by ICF. You can customize your ICF's actions by managing different Internet Control Message Protocol (ICMP) rules. For example, ICMP enables you to manage whether or not you wish to allow the following:

- Incoming echo requests
- Incoming timestamp requests
- Incoming router requests
- Redirects

Based on your ICMP rules, various bits of information will be maintained in the ICF security log. The ICMP rules in Windows XP Professional's ICF are helpful in that they don't totally shut off your network from the outside world, although they severely limit access.

The ICF Log File

ICF logs have their own unique format. First is a header listing the version of ICF used, the name of the security log, a note that all log entries are in local time, and a list of fields available for log entries. Table 9-1 explains the entries you are likely to see in an ICS security log.

The ICF security log is useful in that, when used judiciously, you are able to examine it and see if anyone is trying to hack into your network. By examining the action, src-ip, and dst-ip fields, you should be able to tell if anyone is trying to do harm to your network in general, or a specific device in particular.

Now that you know what your security log will contain, let's take a closer look at how you can enable logging and manage various housekeeping functions that can make ICF easier to administer.

Field	Description
action	The operation trapped by the firewall. Entries include: OPEN CLOSE DROP INFO-EVENTS-LOST (this specifies a number of events that occurred, but were not stored in the log).
date	The date of the file entry, stored in the format YY-MM-DD.
dst-ip	The IP address of the packet's destination.
dst-port	The port number of the packet's destination.
icmpcode	A number representing the code field of the ICMP message.
icmptype	A number representing the type field of the ICMP message.
info	An information entry for the event that depends on the type of action.
protocol	The protocol for the communication. When the protocol is not TCP, UDP, or ICMP, then this entry will be a number.
size	The packet's size.
src-ip	The IP address of the packet's source.
src-port	The port number of the packet's source.
tcpack	The TCP acknowledgment number of the packet.
tcpflags	The TCP flag at the beginning of the packet, which can be one of the following: A—Ack (denotes that the acknowledgment field is significant) F—Fin (denotes the last packet) P—Psh (denotes the push function) S—Syn (denotes the synchronize sequence numbers) U—Urg (denotes that the urgent pointer field is significant).
tcpsyn	The TCP sequence number of the packet.
tcpwin	The TCP window size, in bytes.
time	The time of the file entry, stored in the format HH:MM:SS.

Table 9-1. Entries Found in the ICF Security Log

Enabling and Disabling Logging

Because ICF logging is not activated by default when you install ICF, it is necessary to enable it. To open ICF logging, follow these steps:

1. Select Start | Control Panel.
2. Click Network and Internet Connections, and then click Network Connections.
3. Click the connection that is using ICF, and then under Network Tasks click Change settings of this connection.
4. On the Advanced tab, click Settings.
5. On the Security Logging tab (shown in Figure 9-4), you can choose one or both available options.
   - **Log dropped packets** This makes a log entry whenever inbound connections are attempted, but rejected.
   - **Log successful connections** This makes a log entry whenever outbound connection attempts are successful.

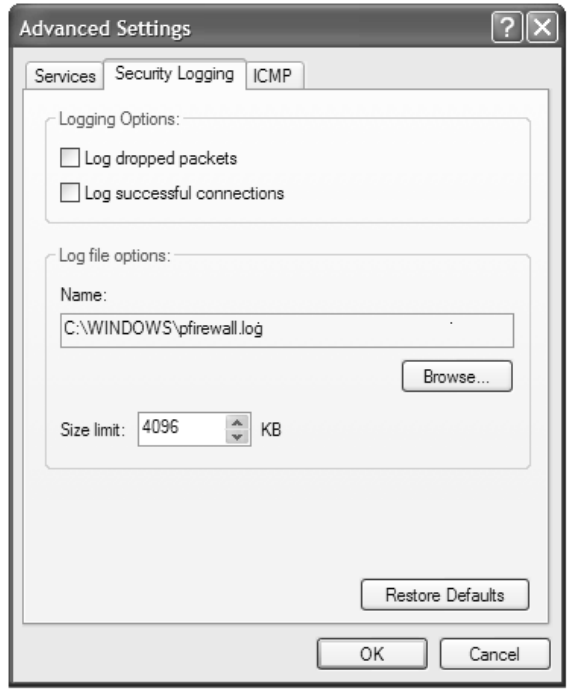

Figure 9-4. ICF logging options

Conversely, if you decide you no longer wish to track your ICF's activity, you can disable logging. To do so, simply follow the preceding steps, clearing the check boxes next to Log dropped packets and Log successful connections.

ICF Logging File Management

You can also decide to give your ICF log a different filename, and store it on a different path than the default file. This is useful when you wish to generate multiple reports (time of day, day of the week, and so forth). To change the path or filename, under the Security Logging tab (as shown earlier in Figure 9-4), under Log file options, click Browse, and navigate to the file where you want to maintain the log file. Enter the filename of your choice in File name, and then click Open.

NOTE If you leave File name blank, Windows XP Professional will give the log file the default name of pfirewall.log.

Like other ICF tasks, viewing your ICF log is fairly straightforward. On the Security Logging tab, under Log file options, and Name, click Browse, and then find the log. If you haven't saved the log with your own filename, it is stored under the default name of pfirewall.log. Right-click the desired log file, and then select Open to view the contents.

Changing the ICF Log File Size

You might discover that the ICF logging file is too small for your needs. Your file size needs will be based on the size of your organization, how many log entries are made, and how long ICF logging is enabled. If you determine that your log file needs to be beefed up (or toned down, if your log file is sucking up too much hard drive space), you can do it simply by accessing the Security Logging tab, as explained previously. Next, under the Log file options, in Size limit, use the arrow buttons to change the log file size limit.

The default size of a log file is 4MB, and the maximum size is 32MB.

NOTE If you fill up a log file, for instance the default file, logging won't stop. Rather, additional log files will be generated. Once pfirewall.log is maxed out, pfirewall.log.1 is created, and so forth.

Security Templates

Using the Security Templates snap-in for the MMC, you can create text-based files that include all the security settings of the security areas supported by local security policy. These are useful for tweaking the multitudes of security details possible in Windows XP Professional. This section shows you how to create a template, modify an existing template, and then finally apply the template to your Windows XP Professional system.

Creating a Template

To run the Security Templates snap-in to view security policy settings, follow these steps:

1. Open the MMC.
2. On the File menu, click Add/Remove Snap-in, and then click Add.
3. In Available Standalone Snap-ins, pick Security Templates.
4. Click Add, and then click Close.
5. Click OK. The Security Templates snap-in is shown in Figure 9-5.
6. In the left pane, click the + (plus) sign to expand Security Templates.
7. Expand C:\Windows\security\templates (in this example, C: is the letter of the drive where Windows is stored).
8. To create a template, double-click Security Templates, right-click the default templates folder, and then click New Template.

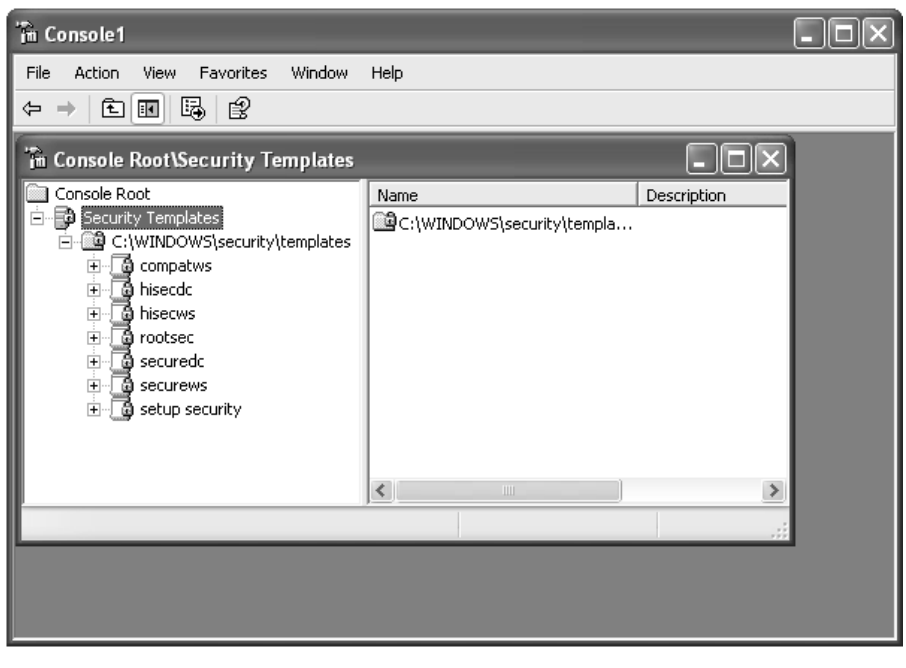

Figure 9-5. Security Templates snap-in

This will generate a blank template that you can fill with whichever security policies best suit your organization. To save the template, simply open the File menu and click Save As.

Editing Existing Templates

Microsoft has included a number of starter templates along with Windows XP Professional. These give a nice foundation on which to build your own security policies. Also, you might have existing security policies you want to fiddle with and apply later.

To open and edit any of these templates, simply double-click them in the left windowpane of the MMC Security Template snap-in.

NOTE Although the Security Template snap-in includes predefined templates, it's a smart idea to check out these templates and make sure they suit the needs of your organization before applying them.

There are four basic types of templates that can be used, depending on your needs:

- Basic
- Secure
- High Secure
- Miscellaneous

These templates represent a range of security needs from standard (Basic) up to strict (High Secure). Furthermore, the Miscellaneous templates provide security settings for some categories that don't easily fall within the Basic, Secure, or High Secure hierarchy. They add security settings for such optional components as Terminal Services and Certificate Services. Some of the templates within each category are listed here:

- **Basicsv** Establishes a basic level of security for file and print servers
- **Securews** Establishes the medium level of security for workstations
- **Hisecdc** Establishes the highest level of security for domain controllers
- **Ocfiless** Establishes security policies for file servers

Any of the ten sample templates are good places to start for network security. However, if you do change a template, it is a very good idea to save it using a new name, so that the old template is not overwritten.

Applying Security Templates

Creating or editing an existing template does not make changes to your security settings. In order for those changes to be made, you must apply the template to your computer. To apply your newly created or edited template, do the following:

1. Using the Group Policy snap-in, double-click Computer Configuration and expand Windows Settings.
2. Right-click Security Settings, and then click Import Policy (this is shown in Figure 9-6).
3. Choose the template you wish to use.
4. Click OK.

Auditing Security

Since computer networks are constantly being configured, tuned, and reconfigured, it's possible that established, functional security settings will not work properly after changes have been made. In order to keep your finger on the pulse of your network's security issues, it's a good idea to use the security auditing tools provided in Windows XP Professional.

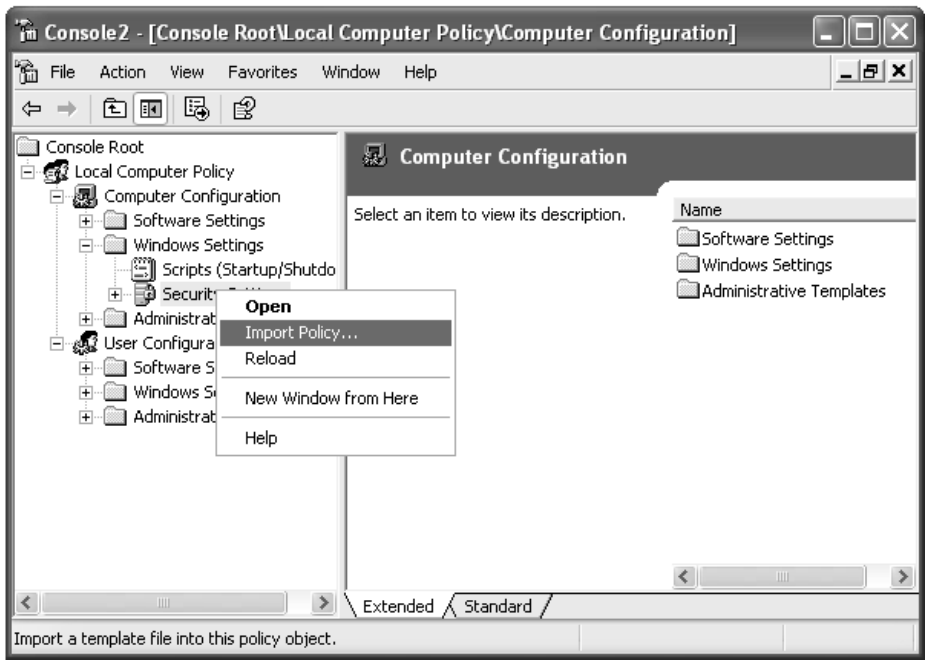

Figure 9-6. Applying security templates

There are a number of useful auditing tools in Windows XP Professional, including the following:

- Event Viewer (which was covered in Chapter 8)
- Audit policies
- The Security Configuration and Analysis snap-in

Auditing is performed from the Group Policy snap-in to the MMC. You can examine the different items that can be audited in Windows XP Professional by viewing the Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy folder in the Group Policy snap-in.

What Can Be Audited

Account logon events make a log entry each time a user tries to log on. The entry might include failed or successful attempts. Failed attempts are further subdivided by whether a user's account has expired, the user is trying to log on locally, the password is invalid, or any other failed attempt has occurred. The following items can be audited:

- **Account management** Makes a log entry each time an account is managed.
- **Logon events** Makes a log entry for logon events over the network.
- **Object access** Makes a log entry each time a certain object (such as a printer or a file folder) is accessed.
- **Policy changes** Makes a log entry whenever a policy is successfully changed on your network. This is useful if you need to reset a policy to a certain state and need reference material.
- **Use of privileges** Makes a log entry whenever a user tries to use special privileges. This entry is made whether or not the user is successful.
- **Process tracking** Makes a log entry each time the user starts a process. This can be used to monitor which applications a user is starting throughout the day.
- **System events** Makes a log entry each time a system event occurs, such as restarting the system.

Before jumping right into auditing, however, it is necessary to develop a solid plan that includes what you'll be auditing and how you can use that information to make positive changes. Auditing significantly taxes system resources, so you'll want to know exactly what you want to audit and what is just overkill.

For example, if you are experiencing performance problems with the network, using process tracking is a good place to start. By comparing the process tracking log to overall system performance, you might be able to tell if certain applications are responsible for a sluggish network. Also, if you are going through toner left and right, you can use object tracking to see which users are using the printer, and for which jobs. Auditing the printer in this way can help you determine if certain users need their printer permissions managed more stringently.

Enabling

To enable auditing, follow these steps:

1. Right-click the object you wish to audit, and then click Properties.
2. On the Security tab, click the Advanced button.
3. This will spawn the Advanced Security Settings for Shared Documents page. Click the Auditing tab. (This is shown in Figure 9-7.)
4. Click the Add button. This will call up a list of users and groups. Select the user or group whose activity you wish to audit.
5. You can select multiple users and groups to monitor. For each one, select whether you want to track successes, failures, or both. (This is shown in Figure 9-8.)
6. Choose whether auditing will be for this object only, or if auditing will include child objects. For instance, if you select the Documents folder, which also contains Administration Documents and Accounting Documents as subfolders,

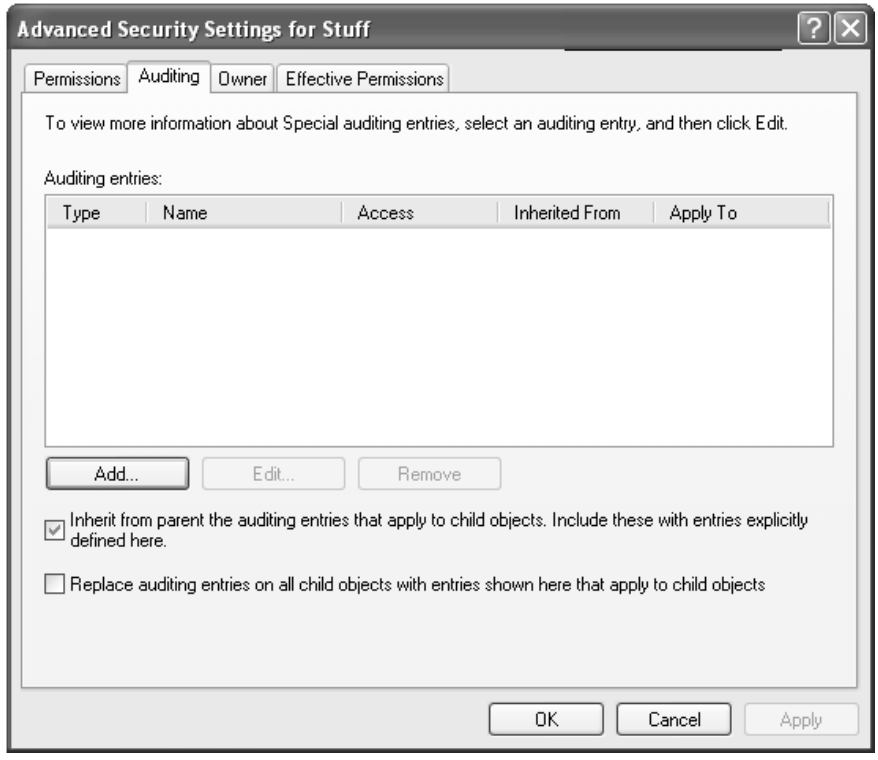

Figure 9-7. Auditing a folder in Windows XP Professional

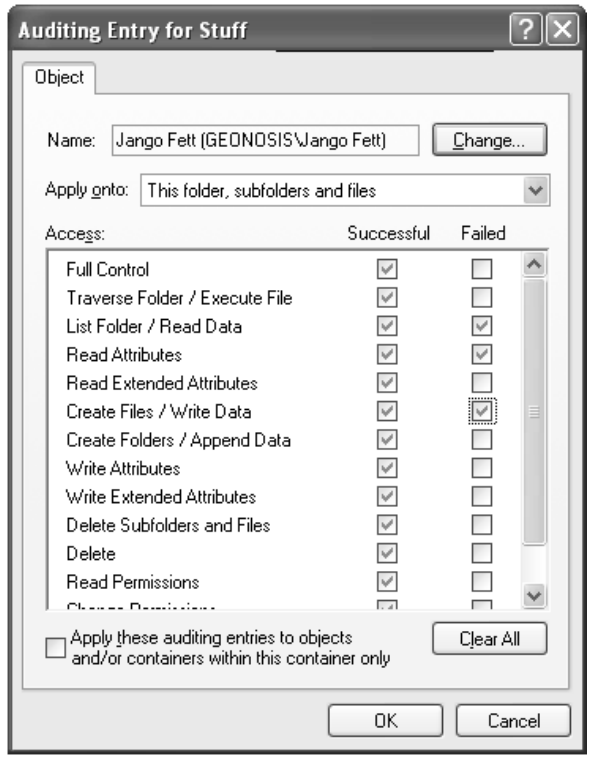

Figure 9-8. Selecting which items to track

and you wish to monitor their use, select the option Apply these auditing entries to objects and/or containers within this container only.

7. Complete any settings you wish to make for the users, computers, and groups you're monitoring, and then click OK.
8. Open the Group Policy snap-in to the MMC. Navigate to Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy.
9. Double-click Audit object access.
10. Check or clear boxes for success, failure, or both, as your auditing needs require.
11. Click OK.

Auditing can be a time- and resource-intensive task. However, by deciding which properties you need to audit and developing a solid plan for their analysis, you can make sure your system's security settings are what you need.

Security Configuration and Analysis Snap-In

The Security Configuration and Analysis snap-in for the MMC is a good tool to use to analyze your current security settings and compare them against a baseline security template. With the myriad security settings that can be made in a Windows XP Professional environment, it can be difficult to keep track of all the settings, let alone keep track of how they actually function in practice. Performing an analysis will allow you to find any security holes, test the impact of system wide security changes without having to implement them, and identify any deviations from a policy that are present on your system.

For instance, if you have established a security template, and want to compare that template (your ideal security settings) against what is already in place on your system, use the Security Configuration and Analysis tool. If your security template is more restrictive than what is already in place on your system, it will identify which areas need to be beefed up to accommodate the new settings. Furthermore, it will tell you what will happen to your system if those new settings are established.

To start the Security Configuration and Analysis tool, do the following:

1. At the command line, enter **MMC /s**.
2. Under the File menu, click Add/Remove Snap-in.
3. Click Add.
4. In Available Standalone Snap-ins, scroll down to Security Configuration and Analysis and double-click it.
5. Click Close, and then OK.

Now, you will have the Security Configuration and Analysis tool (as shown in Figure 9-9) available, but you still need to perform more configuration steps.

Creating a Database

The Security Configuration and Analysis tool is *database driven*. That means in order to use this tool, you need a security database. You won't have to go so far as to create an Access database; the tool will allow you to create a security configuration and analysis database (also known as a local computer policy database). This database is specific to your computer.

Initially, a database is created when Windows XP Professional is installed. This database contains the default security configurations of your system. If you choose, immediately after installation you can export this database and keep it on hand in case you want to restore your initial settings at some future point.

This database defines the security policy in place for your computer, and your computer runs with the configuration defined in the security policy. However, your security policy might not be sufficient to define the entire configuration. As a result, there will be some holes in your security policy. For example, you might not have

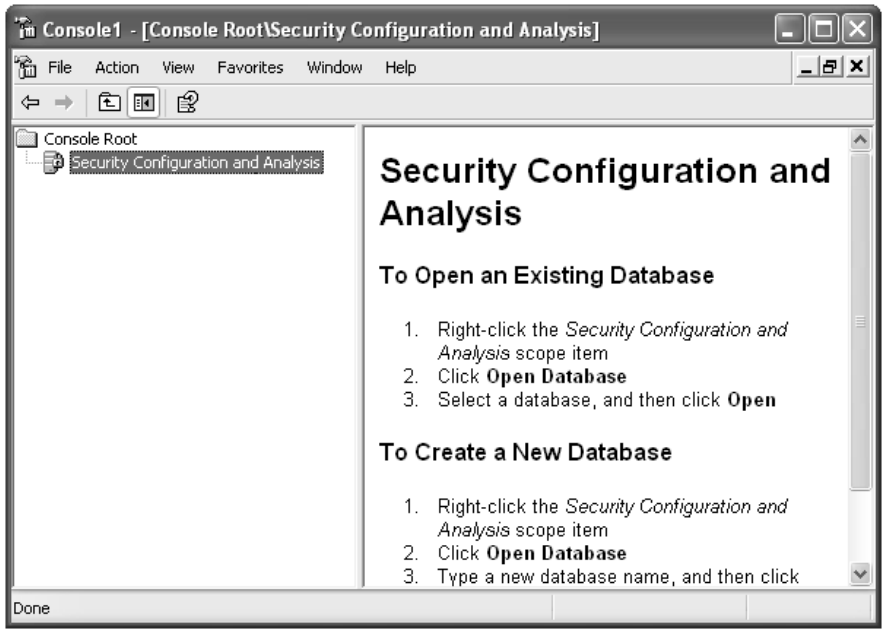

Figure 9-9. The Security Configuration and Analysis tool

security definitions in place for particular files or folders. By running the Security Configuration and Analysis tool, you can find these sorts of security discrepancies.

You can create as many security databases as you like. To create a new security configuration database, do the following:

1. In the left pane of the MMC, right-click Security Configuration and Analysis.
2. Click Open Database.
3. In the Name dialog box, enter the name you wish to use for the new database, and then click Open.
4. Pick an existing security template to import into the database.
5. Click Open.

Analyzing a Database

To analyze a security configuration database, follow these steps:

1. In the left pane of the MMC, right-click Security Configuration and Analysis.

2. Click Analyze Computer Now.
3. In the Error log file path dialog box that pops up, enter the location where you want to send the results of the analysis—for instance, c:\logs\securitylog.log.
4. Click Open, and then click OK. As the tool checks your computer's security settings, a status window will show the progress of the work.

Once the tool has completed its task, you can review the results of the analysis as follows:

1. In the left pane of the MMC, right-click Security Configuration and Analysis.
2. Click View, and then click Customize.
3. Select the description bar to show the database you're working on, and then click OK.
4. In the left pane, click Security Configuration and Analysis.
5. In the right pane, double-click any entry to get a detailed explanation of what was found. This is shown in Figure 9-10.

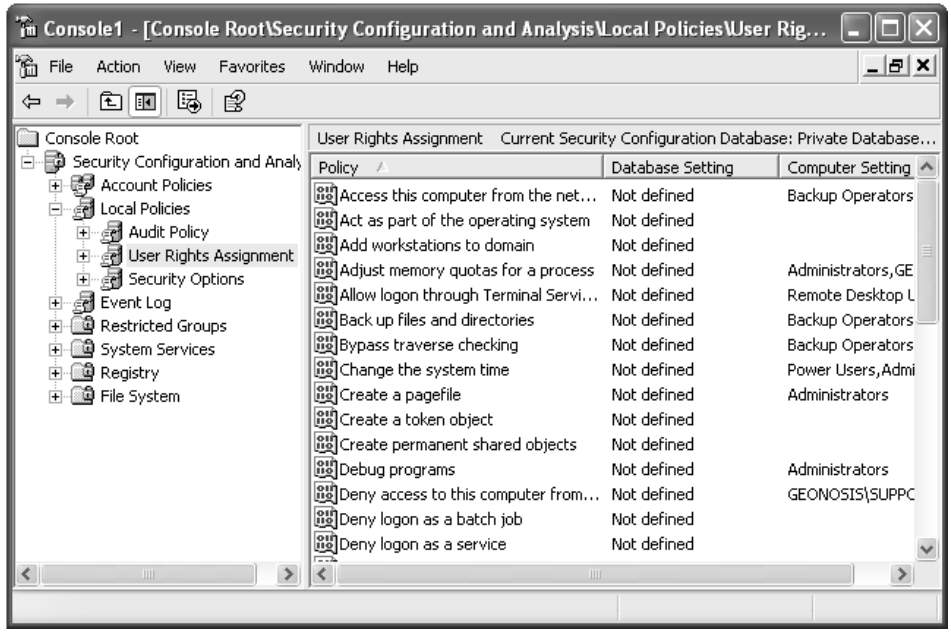

Figure 9-10. Examining the analysis results

Configuration results are shown for the following areas:

- **Account policies** Displays password, account lockout, and Kerberos authentication policies (on Windows 2000 domain controllers only)
- **Event log** Displays audit policies, including object access, password changes, and logon/logoff operations
- **Local policies** Displays audit policies for user rights assignment and computer security options
- **Restricted groups** Displays group memberships for groups identified as sensitive
- **Object trees** With Windows 2000 domain controllers, displays directory objects, Registry subkeys and entries, along with the local file system

Other entries include system services, the Registry, and the file system. After reviewing your security analysis, you might decide to change a security setting. If you decide a setting is relevant, then check the Define this policy in the database check box when examining security details. If this check box is clear, then the policy will be removed from the configuration.

To use different configurations and analyses in the future, simply click the Edit Security Settings control to change the existing security definition maintained in the database.

SECURING SERVERS

Although Windows XP does not include a flavor specifically for servers, you should still undertake certain important security tasks on your server (be it Windows NT, 2000, or .NET) when constructing and configuring your Windows XP Professional network. There are also considerations to be made when connecting your server to Windows XP Professional clients. This section examines such server security issues as IP Security (IPSec), security protocols, Group Policy, authentication, and access control lists (ACLs).

IPSec

Windows XP Professional keeps the packets coursing across TCP/IP networks secure by adopting IPSec. IPSec can be used to create an end-to-end security solution that results in encrypted transmission of data. An IPSec solution can offer the following:

- **Confidentiality** Individuals cannot intercept a message and read it.
- **Authentication** Messages are sure senders are who they say they are.
- **Integrity** Messages are guaranteed not to be tampered with along the way.

- **Protection** By blocking certain ports or protocols, IPSec can prevent denial of service (DoS) attacks.

How IPSec Works

Figure 9-11 illustrates, schematically, how IPSec works. A host with an active security policy wants to communicate with another computer running a security policy.

1. Host Computer A attempts to send data. The IPSec driver on Host A communicates with the IPSec driver on Host B to set up a security association (or SA, which is covered in the next section).
2. The two computers conduct a secret key exchange establishing shared and secret keys.
3. Using the methods of security negotiated in the SA, Host A signs and encrypts packets destined for Host B.
4. Host B receives the packets and the IPSec driver checks the signature and key on the packets. If authenticated, the data is passed up the stack to Host B.

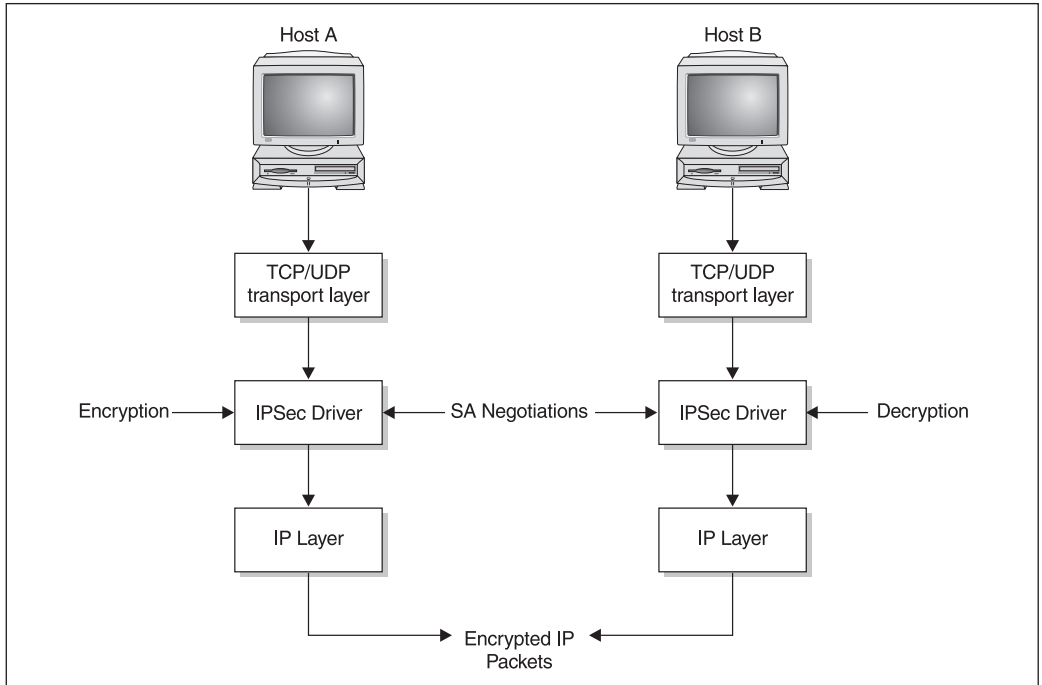

Figure 9-11. IPsec is set up between each communicating host pair.

Of course, the entire process occurs rapidly and without the knowledge of either user at Host A or B. However, additional CPU cycles are consumed encrypting and decrypting these packets.

IPSec Negotiation

An IPSec Policy Agent resides on each computer in a Windows XP/2000/.NET network. Whether it is active or not is up to the administrative policies in place. If the agent is active, it will retrieve the IPSec policy, which describes the local security association and enforces it on the local computer.

An SA is a contract between two communicating computers that is set up before any data is transferred. This negotiation determines specifics about how the two computers will communicate data including these items:

- **The IPSec protocol** Authentication Header, Encapsulating Security Payload
- **The Integrity Algorithm** Message Digest 5, Secure Hash Algorithm
- **The Encryption Algorithm** Data Encryption Standard (DES), Triple DES, 40-bit DES, or none

Establishing IPSec Policies

By default, Windows XP Professional provides three predefined security policies that will satisfy most cases of setting up a policy. You can also start with a predefined policy and customize it to fit your needs. These policies are described in the following list:

- **Client (Respond Only)** Instructs the computer to use IPSec when another computer requests it. It does not request IPSec when initiating communications with another computer. This policy is best for computers that contain little to no sensitive data.
- **Server (Request Security)** For servers that should use IPSec if possible, but won't deny communication if the client does not support IPSec. If total security is required, the Secure Server policy (explained next) should be used. However, this policy is useful in environments where not all the clients can use IPSec—for example, during a migration from Windows NT.
- **Secure Server (Require Security)** For servers containing sensitive data, this policy requires all clients to use IPSec. All outgoing communications are secured and all unsecured requests from clients are rejected.

Choosing the right policy requires careful assessment of the nature of the data. Indiscriminately assigning the highest level of security for all users and servers will unnecessarily put a tremendous strain on the servers and client workstations. This is because of the overhead on the computer to encrypt and decrypt all network traffic. However, allowing any type of client to connect to a secure server opens enormous gates for unsecured information to flow through.

Creating and Applying IPSec Policies

The Microsoft Management Console (MMC) is used to create and configure IPSec policies. The IPSec Policy Management snap-in must be added to the MMC as shown in Figure 9-12.

NOTE Adding IPSec to your MMC is identical to other methods listed in this book for adding a snap-in to your MMC. When scrolling through the list of available snap-ins, select IP Security Policy Management.

When you add the IPSec snap-in to your MMC, you will be asked which computer this snap-in will manage. You can choose from these options:

- This computer
- The Active Directory domain controller of which this computer is a member
- Another Active Directory domain
- Another computer

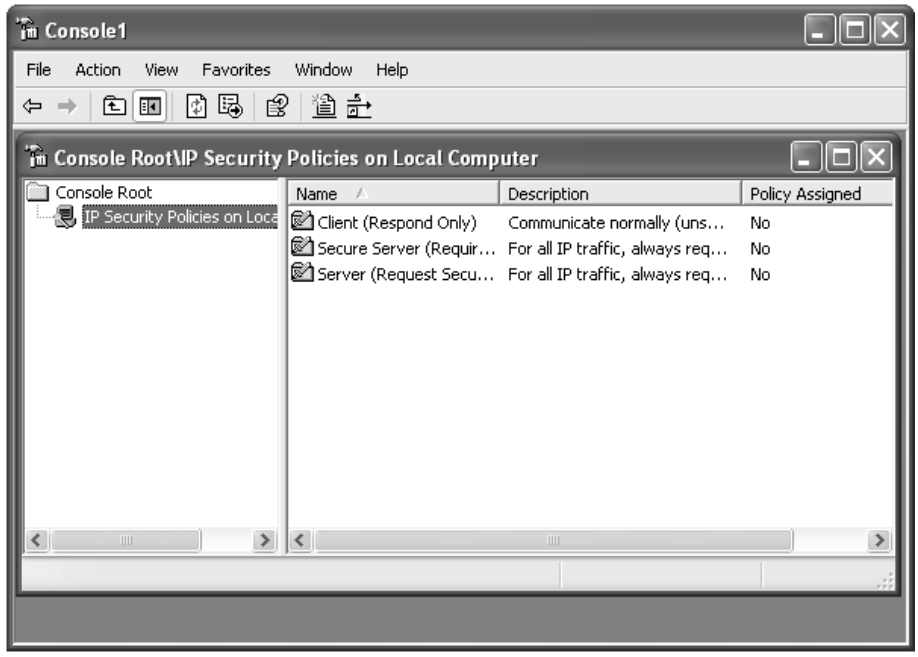

Figure 9-12. IPSec Policy Management snap-in

When the IPSec snap-in is first opened, the three default policies are present for you to alter as you see fit, or you can create your own using the IP Security Policy Wizard. This wizard is started by right-clicking the IPSec snap-in in the left window pane and then selecting Create IP Security Policy.

When the wizard starts, you will be prompted to enter the following information:

- The name and a description of the policy
- Whether this policy will respond to requests for secure communications
- The authentication method (Kerberos, certificate, or preshared key)

The detail of the resulting IPSec policy is shown in Figure 9-13.

You can also adjust settings pertaining to handling of keys and timeout values of shared information. For example, by double-clicking All IP Traffic, you can adjust specific settings for that particular feature. As Figure 9-14 shows, this specific IPSec detail allows you to decide whether you want the filtering rule to apply to all IP traffic, to ICMP traffic, or to both.

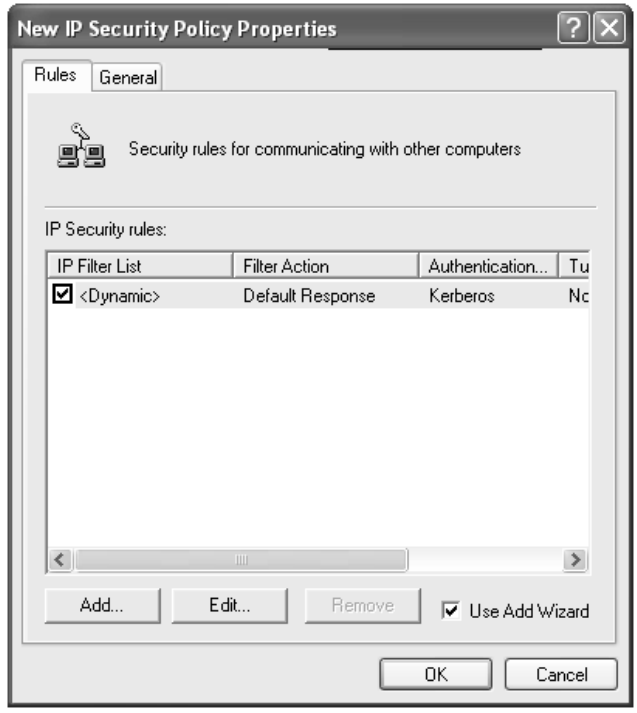

Figure 9-13. Configuring IPSec policies in the MMC

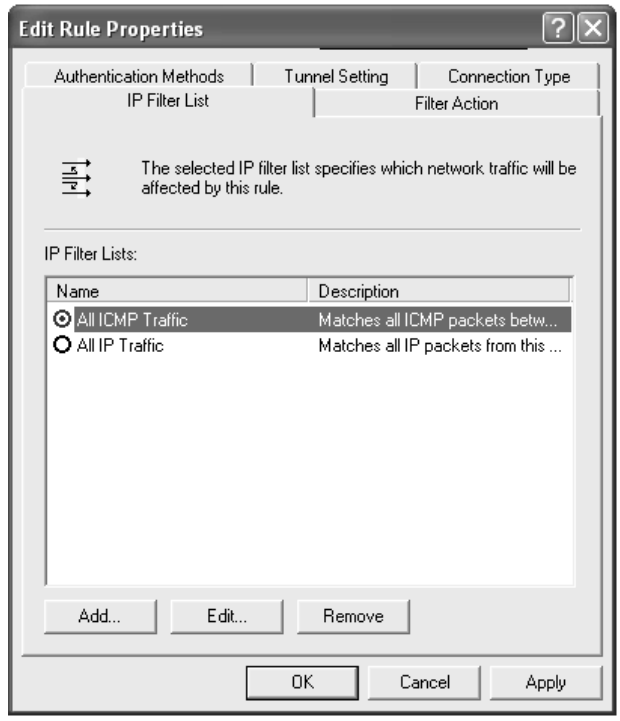

Figure 9-14. Editing IPSec rule properties

It is also possible to import other security methods as they become available so that you are not stuck using old technology. When you are finished making your changes, the policy is added to the default selections so you can alter or view its properties at a later time.

An IPSec policy can then be assigned to a Group Policy. There it will be applied to all member computers and users of the policy. Unlike many other policies, local policies take precedence over policies higher up the hierarchy. For example, the local Organizational Unit (OU) IPSec policy will override a policy included with the domain.

Logon

The first security step most users encounter is the logon process. When they sit down at their computers and press CTRL-ALT-DEL, they are prompted for their username and password. This section takes a closer look at what is involved with the Windows XP

Professional logon process and how you can switch between two different user accounts once Windows XP Professional has been started.

Types

When using Windows 2000 as a server, Windows XP Professional uses four types of logon processes:

- **Interactive** This logs on the user to a local computer.
- **Network** This logs the user onto the network. The Local Security Authority (LSA) of the client's workstation will try to authorize you with the LSA of the remote computer using the credentials employed for logon.
- **Service** Win32-based services log onto the local computer using the credentials of a local or domain user account or the LocalSystem account. When the LocalSystem account is used (with a Windows 2000 Server), the service would have unfettered access to Active Directory. On the other hand, if a service is running using the security privileges of a local user account, there would be no access to network resources.
- **Batch** This type of logon is rarely employed in Windows environments, and is used mainly for large batch jobs.

When logging onto Windows XP Professional using the interactive process, the user's credentials can be checked against either the local computer or the domain controller. The process is different, based on where the user's credentials are stored.

NOTE To log onto a Windows 2000 domain, Logon domain must appear in the dialog box. If it does not appear, click the Options button and select the domain, or enter your username in this format: *username@mycomputer.myorganization*.com.

Interactive Logon

To the end user, the logon process is fairly straightforward: Type your username and password, and then press ENTER. However, quite a lot goes on behind the scenes to make the interactive logon process happen. The following components all take a part in the logon process:

- **Winlogon** The process responsible for managing logon and logoff operations as well as starting the user's session.
- **Graphical Identification and Authentication (GINA)** A dynamic link library (DLL) file, called by Winlogon, containing username and password. This is the dialog box that appears at logon.
- **Local Security Authority (LSA)** The entity on the local device that checks the username and password for authentication.

- **Security Account Manager (SAM)** The entity that maintains a database of usernames and passwords. The SAM is maintained on both local computers and domain controllers.
- **Net Logon Service** This service is used in conjunction with NTLM (which is explained later in the chapter) to query a domain controller–based SAM.
- **Kerberos Key Distribution Center (KDC) service** This service is used when authentication is attempted to Active Directory.

Run As

If you log onto your Windows network, performing *all* your work using your administrator credentials, you open your network to some unnecessary risks. For instance, you could unwittingly download a virus that could propagate to the rest of the network. The best way to minimize the risk is to log on using user or power user rights, and then switch over to your administrator account only when administrative tasks need to be done.

Unfortunately, logging off as a user and relogging on as an administrator is time consuming and inefficient. As such, Windows XP Professional includes a tool called Run As. This allows a user to log on with one set of credentials, and then run an application using a second set of privileges. For example, using user credentials, you could perform your day-to-day work, visit Internet sites, and so forth. Then, if you had to manage a user group, you'd invoke Run As, perform your administrative tasks, and then close out Run As.

Run As allows you to start the following:

- Programs
- Program shortcuts
- MMCs
- Control Panel items

To start Run As, follow these steps:

1. Locate the item you wish to open in Windows Explorer, and then click it.
2. Press SHIFT, right-click the item, and select Run As.
3. In the resulting dialog box (as shown in Figure 9-15), click The following user radio button.
4. Enter your user name and password or the account you wish to use to access the item.
5. In the Domain box, you can do one of two things:
   - To use local administrator credentials, enter the name of your computer.
   - To use domain administrator credentials, enter the name of your domain.

Figure 9-15. The Run As dialog box

If Run As doesn't work, ensure that the Run As service is enabled by using the Services snap-in to the MMC.

Protocols

Although there are many protocols used for security, Windows XP Professional relies on two of the most prevalent protocols: Kerberos and NTLM. NTLM is used as the default logon protocol for Windows NT networks; Kerberos is used because it is the default protocol for Windows 2000 domains.

The only time Kerberos is employed is when both the domain controllers are using Windows 2000 or .NET and the clients are using Windows XP Professional. In all other scenarios, NTLM is used. The following sections examine what goes on with these security protocols.

Kerberos

We mentioned Kerberos earlier in this book. But because of its importance in Windows 2000 domains (and their connectivity with Windows XP Professional), it deserves further discussion here. Kerberos is the default authentication protocol used in Windows 2000 and Windows XP Professional.

Kerberos was created at the Massachusetts Institute of Technology in 1988. The protocol provides a fast, single logon to Windows network resources, along with other network operating systems that support the Kerberos protocol. Kerberos provides the following features:

- Faster logon authentication in a distributed computing environment
- Interoperability with non-Windows systems that use the Kerberos protocol
- Pass-through authentication for distributed applications
- Transitive trust relationships between domains

Kerberos is a shared-secret authentication protocol. This means the client and another computer (known as the Key Distribution Center, or KDC) know passwords, but no one else does. Kerberos is a faster authentication protocol because it shifts the burden of authentication away from the server and gives it to the client and the KDC.

NOTE The steps involved in a Kerberos logon were illustrated in Chapter 2.

NTLM

NTLM is a protocol that authenticates computers and users based on a challenge/response technique. When the NTLM protocol is initiated, a resource server must contact a domain controller to verify the user or computer's identity.

NOTE NTLM need not only be used in a domain environment; it can also be used in peer-to-peer and workgroup environments.

The following steps explain what occurs with an interactive NTLM logon:

1. The user initiates logon by pressing CTRL-ALT-DEL. This is called the Secure Attention Sequence (SAS).
2. Next, Winlogon calls the GINA DLL, which provides the logon dialog box.
3. Once the user enters his or her username and password, Winlogon sends the information to the LSA.

NOTE The LSA is the entity that receives the username and password from Winlogon and determines if the logon is to take place on the local computer or on the network.

---

4. If the user's account is stored on the local computer, the LSA uses the MSV1_0 authentication package, comparing the logon information with data in the computer's SAM database. If the user's account is stored on the network, the LSA uses MSV1_0 and Net Logon service to check the SAM on a Windows NT domain controller.
5. If the logon information is valid, the SAM tells the LSA, sending along the user's security identifier (SID). Furthermore, the SAM sends the SIDs of any groups to which the user belongs. This information is used by the LSA to generate an access token that includes the user's SID.
6. The user's session begins when Winlogon receives the token.

Authentication

Don't confuse logon with authentication. Whereas logon allows a user to access a computer (either locally or with network privileges), the process of authentication goes deeper, allowing users to have certain permissions and memberships in groups.

Creating, managing, and deleting *user accounts* and establishing and maintaining *security groups* are important tasks for security management. It is the establishment of these functions that governs what level of access your users will have and how they can use system resources.

User Accounts

Every user on your network has an account. Accounts can be established locally or as part of the larger domain. If a user has a local account, then he or she cannot access network resources (unless anonymous access is authorized on the network); if a user has a domain-based account, then network resources are available via the local computer.

When Windows XP Professional is installed, two user accounts are created:

- **Administrator** Used to configure and manage the system. Once Windows XP Professional has been installed and configured, this account is only needed for the occasional administrative task.

NOTE A good security practice is to log off the administrator account and log on with a user account for day-to-day tasks.

- **Guest** Allows users to log onto the computer without the need for a separate account for each user.

In addition to these accounts, Windows XP Professional allows a number of other types of accounts to be created. These accounts include the following:

- **Backup Operators** Members of this group can perform backup and restore operations on the computer, no matter which permissions are in place.
- **Help Services Group** Members of this group can use applications to help diagnose system problems.
- **Network Configuration Operators** Members of this group are able to provide limited administrative functions, such as assigning IP addresses.
- **Power Users** Members of this group lie somewhere between administrators and users. They can install and modify applications, have read and write functions, and can be granted permission to install local printers (if the administrator delegates that control to the power user).
- **Remote Desktop Users** Members of this group are allowed to log on remotely.

- **Replicator** Members of this group are allowed to replicate files across a domain.
- **Users** Members of this group have limited access to the system and have read and write permissions only to their own profile.

If a certain type of account (such as a user account) is needed for the local computer, the administrator will have to log on and create the account. No one else can create user accounts.

To create, manage, or delete a user account, follow these steps:

1. Select Start | Control Panel.
2. Click User Accounts. The resulting screen is shown in Figure 9-16.

You can also manage additional user traits, as explained in the following sections.

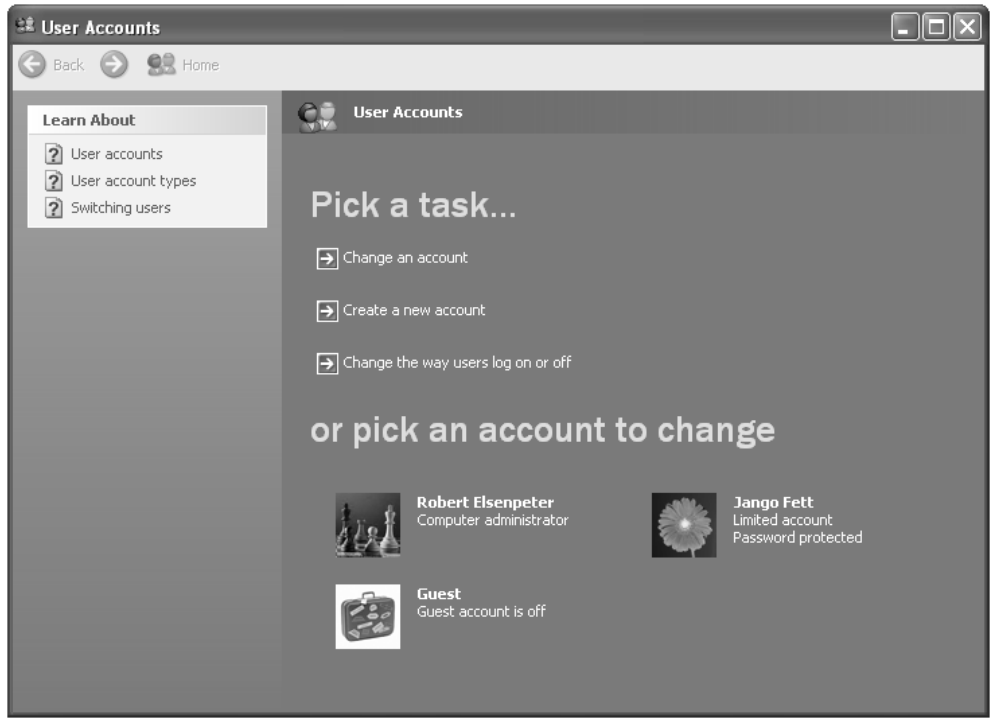

Figure 9-16. Managing user accounts

Password Management

Employees come, employees go (and some employees are *asked* to go). As such, Windows XP Professional provides a way to manage the passwords of your organization's employees. There are two ways in which passwords can be managed in Windows XP Professional:

- **User Accounts** Located in the Control Panel, this option is used when the computer is *not* part of a domain and passwords need to be managed locally.
- **Local Users and Groups** This snap-in to the MMC is used when the computer is part of a domain and passwords need to be managed across a number of computers.

Password Tasks

To change a user's password, follow these steps:

1. Select Start | Control Panel, and then double-click User Accounts.
2. In the resulting dialog box (shown in Figure 9-17), click the user's name, and then click Change Password.

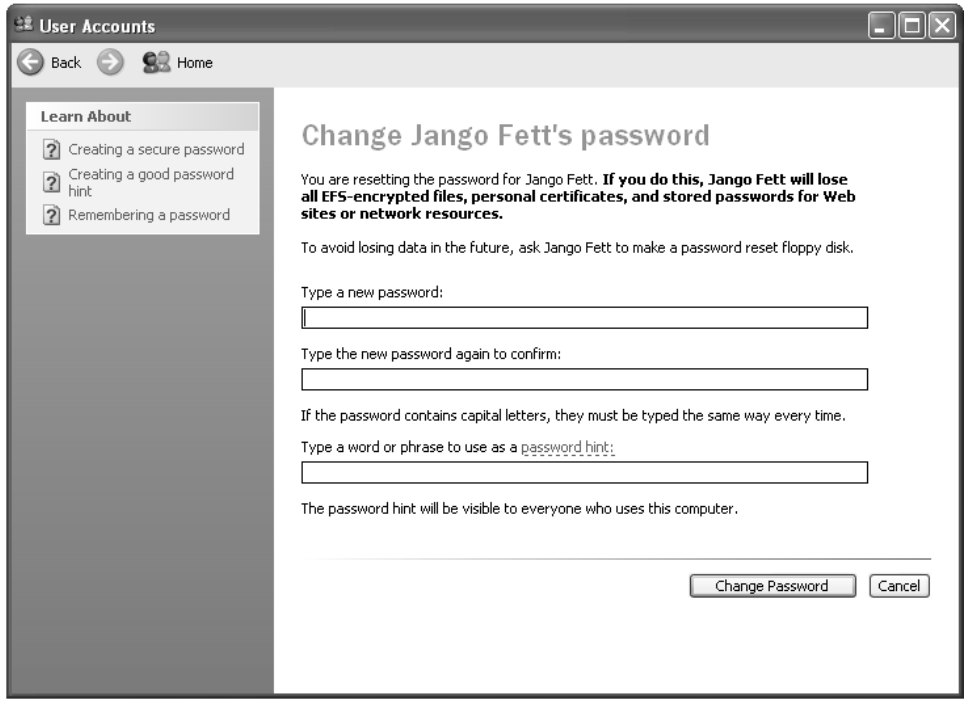

Figure 9-17. Changing a user's password

3. Type the new password twice in the Reset Password dialog box.
4. You can enter password hints, if you choose, that can help the user in case he or she forgets the password.

Windows XP Professional allows you to set certain rules for password management. For instance, you can make the user change his or her password the next time he or she logs on, you can disable an account, and so forth. To access these rules, follow these steps:

1. Open the MMC and add the Local Users and Groups snap-in.
2. Double-click the Users folder.
3. Right-click the name of the user whose account you wish to manage, and then select Properties.
4. On the Properties page (shown in Figure 9-18), you can establish the following rules.
   - User must change password at next logon.
   - User cannot change password.

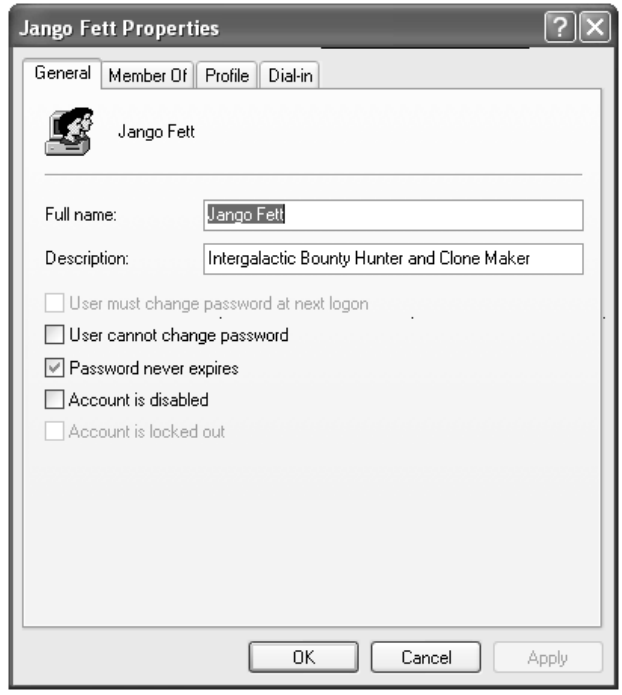

Figure 9-18. Managing password rules

- Password never expires.
- Account is disabled.
- Account is locked out.

NOTE If you need to establish even more sophisticated password rules, this can be accomplished through the Group Policy snap-in. You can set a minimum password length, or a predetermined time when passwords must be changed. Group Policy is discussed later in this chapter in the section "Group Policy."

Stored User Names and Passwords Depending on the complexity and design of your network, you might not want a user to have the same credentials for varying resources. For instance, a user might have power user access to the network, but only user-level access on the server. Whatever your needs, Windows XP Professional can keep track of the user's different credentials using Stored User Names and Passwords, located in the Control Panel.

NOTE Stored User Names and Passwords isn't limited to usernames and passwords. It can also keep track of certificates, smart cards, and Passport credentials.

If a user tries to access a password-protected network resource, his or her logon credentials are used. If those credentials are not sufficient, the Stored User Names and Passwords file is queried. If the requisite credentials are present, then the user can access the resource. If the credentials are not present, he or she is prompted to enter the correct credentials, which will be saved for later use.

To create a new username and password for a password-protected network resource, follow these steps:

1. Select Start | Control Panel, and then double-click User Accounts.
2. If you are part of a domain, click the Advanced tab, and then click Manage Passwords. On computers not part of a domain, click the icon similar to your user account, and then under Related Tasks, click Manage your stored passwords.
3. Click Add.
4. Enter the requested information.

Restoring Passwords If you've ever forgotten a password, you know how frustrating (and embarrassing) it can be to get it reset. To ameliorate this problem, Windows XP Professional includes a Password Reset Wizard, which allows a backup disk to be created that allows passwords to be reset.

NOTE The Password Reset Wizard works only on the local machine. It cannot be used for network accounts. Furthermore, the disk does not actually contain your password, rather it contains a public and private key pair. Since your password is not stored on the disk, it is not necessary to create a new password backup disk each time you change your password.

To back up a password, do the following:

1. Select Start | Control Panel.
2. Select User Accounts, and choose your own account from the list.
3. In the Related Tasks pane, click Prevent a forgotten password. This will invoke the Password Reset Wizard.
4. Click Next.
5. Put a floppy disk into your floppy disk drive.
6. In the Current User Account Password box, enter your password, and then click Next.
7. When the progress indicator shows the task is complete, click Finish, and then keep the disk somewhere safe.

NOTE It's a good idea *not* to put a label on the disk reading "Password Backup" or the like.

Now, if you enter the wrong pasword, Windows XP Professional will prompt you for your password backup disk. The wizard will ask you in which drive the backup disk is located, and then ask you to enter a new password.

Security Groups

User accounts are the building blocks of security groups. Groups can be established and managed based on your organizational needs. For example, you can place your organization's users into groups for upper management, middle management, and workers. This type of structure is helpful if you wish to give (or take away) a security permission to a specific user group, without giving it to the entire organization. For example, your organization might have just installed a kicked-up color printer, but you only want management to be able to access the printer. By giving that permission to the upper and middle management groups, you don't have to worry that the entire company will be using the printer. Furthermore, because you are able to assign the permission twice (once to each group), you aren't spending all day going through the network's user accounts and applying the permission over and over.

Security groups can be any size. They could govern a lone computer or user, an entire domain, or an entire forest. Windows XP Professional security groups fall into one of the following categories.

- **Computer local groups** These groups are specific to a local computer and not acknowledged anywhere else in the domain.
- **Domain local groups** Permissions are granted to devices only within the domain.
- **Global groups** These are used within a domain to combine user accounts that share a common access need, based on function within the organization.
- **Universal groups** Groups in this category are used in a multidomain setting to combine user accounts that share a common access need, based on function within the organization.

Though not a security group per se, yet sharing the same rules, built-in security principles apply to any account that is using a computer in a specified way. For example, built-in security principles could be set to apply to anyone who uses a dial-up connection to access the computer, or anyone logging onto a computer across a network.

Groups are determined largely by where in the network they are able to use permissions and the amount of traffic the group generates. Another bonus to using groups is that when they are well planned and implemented, network congestion decreases because there isn't as much domain controller replication required.

Whoami

No, Whoami is not an early 1980s world-class breakdancing group. Rather, it is a command-line tool used in Windows XP Professional that allows you to view the permissions and rights that apply to a user.

Whoami is on your Windows XP Professional CD-ROM in the Support/Tools directory. This tool returns the domain or computer name along with the username of the user who is currently logged onto the computer on which Whoami is run. It displays the username and security identifiers (SID), groups and their SIDs, privileges, and status.

To install Whoami, double-click the SETUP.EXE tool in the Support/Tools directory on your Windows XP Professional CD-ROM. Then, complete the steps in the Support Tools Setup Wizard to complete the Whoami installation.

To run Whoami, at the command prompt, enter **whoami**.

Depending on your needs, there are options you can add at the end of Whoami to garner the results you need, as listed here:

- **/all** Displays all the information in current access token.
- **/user** Displays the user associated with the current access token.
- **/groups** Displays the groups associated with the current access token.
- **/priv** Displays the privileges associated with the current access token.
- **/logonid** Displays the logon ID used for the current session.
- **/sid** Displays the SID associated with the current session. This argument must be added to the end of the /USER, /GROUPS, /PRIV, or /LOGONID options.

A couple of examples of Whoami follow.

```
C:\Documents and Settings\Robert Elsenpeter>whoami /user /priv
[User]     = "GEONOSIS\Robert Elsenpeter"

(X) SeChangeNotifyPrivilege         = Bypass traverse checking
(O) SeSecurityPrivilege             = Manage auditing and security log
(O) SeBackupPrivilege               = Back up files and directories
(O) SeRestorePrivilege              = Restore files and directories
(O) SeSystemtimePrivilege           = Change the system time
(O) SeShutdownPrivilege             = Shut down the system
(O) SeRemoteShutdownPrivilege       = Force shutdown from a remote system
(O) SeTakeOwnershipPrivilege        = Take ownership of files or other objects
(O) SeDebugPrivilege                = Debug programs
(O) SeSystemEnvironmentPrivilege    = Modify firmware environment values
(O) SeSystemProfilePrivilege        = Profile system performance
(O) SeProfileSingleProcessPrivilege = Profile single process
(O) SeIncreaseBasePriorityPrivilege = Increase scheduling priority
(X) SeLoadDriverPrivilege           = Load and unload device drivers
(O) SeCreatePagefilePrivilege       = Create a pagefile
(O) SeIncreaseQuotaPrivilege        = Adjust memory quotas for a process
(X) SeUndockPrivilege               = Remove computer from docking station
(O) SeManageVolumePrivilege         = Perform volume maintenance tasks
```

To display my SID, the /user and /sid switches are used in tandem:

```
C:\Documents and Settings\Robert Elsenpeter>whoami /user /sid
[User]     = "GEONOSIS\Robert Elsenpeter"  S-1-5-21-606747145-113007714-17085377
68-1003
```

Access Control Lists

In the last section we gave a quick, back-of-the-envelope sketch about user accounts and how those accounts are managed by their membership in a group. In order to manage your groups (add and remove both users and permissions, for instance), administrators use access control lists (ACLs).

Windows XP Professional uses two types of ACLs:

- **Discretionary access control lists (DACLs)** Used to identify the users and groups that are allowed (or denied) access
- **System access control lists (SACLs)** Control how access is audited

ACLs are a handy tool to examine who has access to a specific object, and they provide the means to edit those permissions. For instance, if you determine that an object, such as a new turbo laser printer, isn't to be used by anyone but the marketing department, then an ACL can be used to set and enforce those limits.

Viewing

To view an ACL, right-click a particular object's icon (folder, printer, and so forth), then select Properties. Click the Security tab, and you'll see the groups and users that have access to this object, along with a summary of the permissions granted to that group.

NOTE Computers running Windows XP Professional in stand-alone or workgroup environments won't be able to see the Security tab if simple sharing has been enabled. To disable Simple Sharing, open My Computer. Under the Tools menu, click Folder Options. Next, click the View tab, and then clear the Use simple file sharing (Recommended) check box.

On the Security tab, there are two windows:

- **Group or user names** This box lists the users or groups that have the requisite permissions for this object.
- **Permissions** This box lists the permissions granted or denied for the user or group selected in the Group or user names box.

NOTE Only users who have permissions for a particular object are able to view the ACL for the object.

The Add and Remove buttons do as their names suggest: They allow you to add or remove users or groups from the list.

Advanced Settings

By clicking the Advanced button, you can examine more details of particular user and group settings. On the Advanced Security Settings page, you can establish more advanced features for granting permissions, including:

- Managing special permissions for a user or group
- Managing access inheritance options from the object to any child objects
- Viewing attempts to access the object
- Managing the ownership information of an object

When the Advanced Security Settings page appears, it automatically starts on the Permissions tab. This shows the permissions that have been *explicitly* established for this object. A second permissions tab labeled Effective Permissions allows you to examine all the permissions that apply to a user or group for an object, including the permissions that come as being part of a particular group or those established for a particular user.

Group Policy

One of the most powerful administrative tools in Windows XP Professional is Group Policy. Judicious use of this tool can reduce the Total Cost of Ownership (TCO) by locking down users' systems and thus reducing the probability that a user will somehow screw things up. Group Policy is a snap-in for the MMC and can be applied to almost any object. You might, for example, create and apply a Group Policy to a domain, OU, and group within the OU. The policies follow the hierarchy of the domain tree. Therefore, if a policy higher up the tree is in conflict with a lower-level policy, the higher-level policy takes precedence by default.

NOTE By and large, Group Policy is used for Active Directory domains. However, to manage your local computer using Group Policy, you use Local Group Policy. You implement Local Group Policy in the same general way you do Group Policy. However, when you initiate the Group Policy snap-in, you are asked which computer you wish to manage. Rather than a network computer or domain, select Local Computer.

The Snap-In

The Group Policy snap-in, shown in Figure 9-19, includes two major groups: Computer Configuration and User Configuration. These correspond to the System Policy Editor and User Policies, respectively. Each contains three major policy containers.

- **Software Settings** Installs software on specific computers or on users' systems
- **Windows Settings** Sets security settings and runs scripts at startup or shutdown
- **Administrative Templates** Controls how Windows and applications look and behave

Once you have selected the particular policy you want to alter, right-click it and select Properties. You have the choice of disabling or enabling the policy. In this example, we have enabled the Remove Documents menu from Start Menu policy. Now no users in the domain will have the Documents item in their Start menus.

Group Management

If you were in an enterprise with thousands of employees, it would be impossible to manage each user account individually. That's where groups become useful (and necessary). You can apply attributes for a broad range of users with a couple clicks of the mouse.

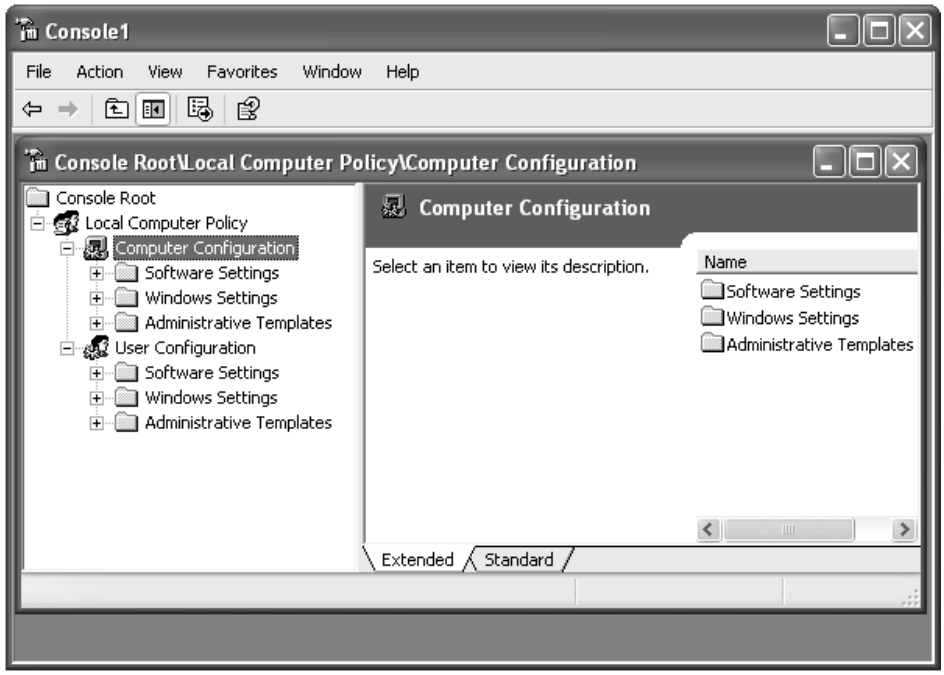

Figure 9-19. The Group Policy snap-in

Creating a Group The first step is to create an OU. This can be done from either the Windows 2000 or .NET server, or using the Windows .NET Server Administration Tools Pack mentioned in Chapter 6 and the appendix. OUs are the basic building block of Active Directory. Open the Active Directory Users and Computers tool by selecting Start | Administrative Tools | Active Directory Users and Computers. Select the domain where you want to locate the OU. Now, choose Action | New | Organizational Unit. Enter the name of your new OU and click OK.

To add a user to your newly created OU, go back to the Active Directory Users and Computers snap-in and pick the OU into which you want to place the user. From the toolbar, choose Action | New | User.

This summons a New Object–User box into which you will enter the necessary user information, and then click Next. You'll be asked for the user's password (which can be changed by the user at the next logon).

Adding a group to your OU follows the same basic steps as adding a user. Again, use the Active Directory Users and Computers snap-in, select Action | New | Group, and follow the dialog boxes to establish your group and its attributes.

You need to pay special attention to where you are creating the new object because it is conceivable to add a new object just about anywhere in the hierarchy. It is possible and encouraged to create OUs within other OUs. If this is what you intend to do and you actually create the new OU under the domain, the results are completely different and will impact all members of that OU. The same can be said for users and groups—the placement of these objects in the Active Directory hierarchy have a dramatic impact on their properties. For example, creating a new user under the domain will give this new user rights over all objects beneath it in the hierarchy, including all member OUs. This is quite different from creating a new user in an OU that has very restricted rights.

NOTE You can easily move users, groups, and OUs around the domain tree using this snap-in. Be aware that a simple move might impact many users.

Editing a Group Groups rarely keep the same information from the time they're created. Active Directory supplies the necessary tools to edit your group and its attributes. Use the Active Directory Users and Computers snap-in, right-click the user or group account, and select Properties. This provides a Properties box containing all the pertinent attributes of your user or group.

As Group Policy shows, security management in Windows XP Professional networks can be rather detailed. Understanding how to manage security can be an important task, and not one that should be taken lightly.