Home Computer Security

Examples - Table of Contents

Introduction

The example provided here is a guide for how to do your task on a Microsoft Windows 2000 system. Please note that your computer might vary from the example. If so, you will still be able to do the task, but it might take some effort to get your version of Windows to do the same thing.

In the example, you'll find the notation **A→B→C**. This means that you need to use the left mouse button to select the A menu item, then use the left mouse button again to select the B menu item, and again to select the C menu item.

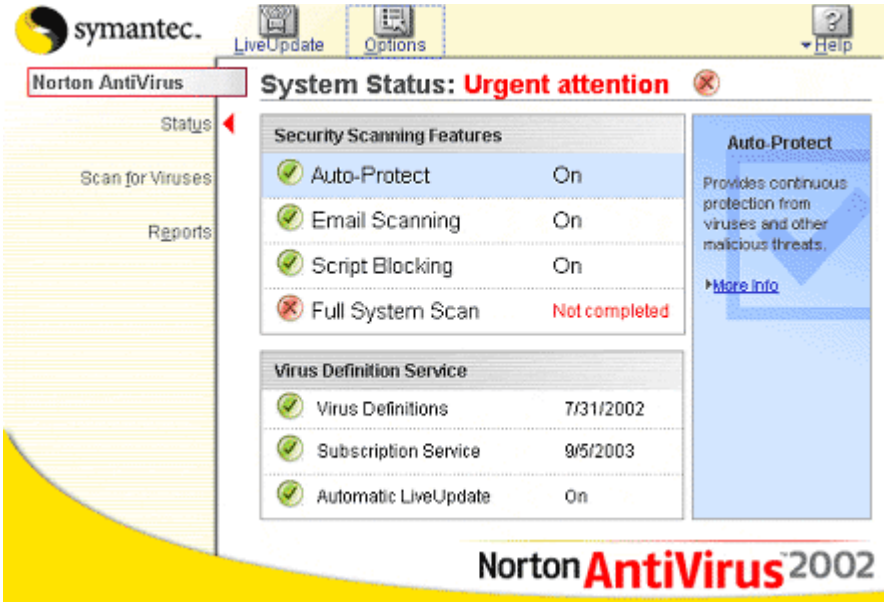
In most cases, the first item listed is the Start menu. Start is part of the Windows Task Bar and is often found at the bottom of your screen display. The Start menu is usually found at the left side of the Task Bar. So, to display general Windows 2000 help, do **Start→Help**. When you do that, you ought to see a new window that looks like the first picture, **Microsoft Windows 2000 Professional**, **Start Here**.

Operating an Anti-Virus Program

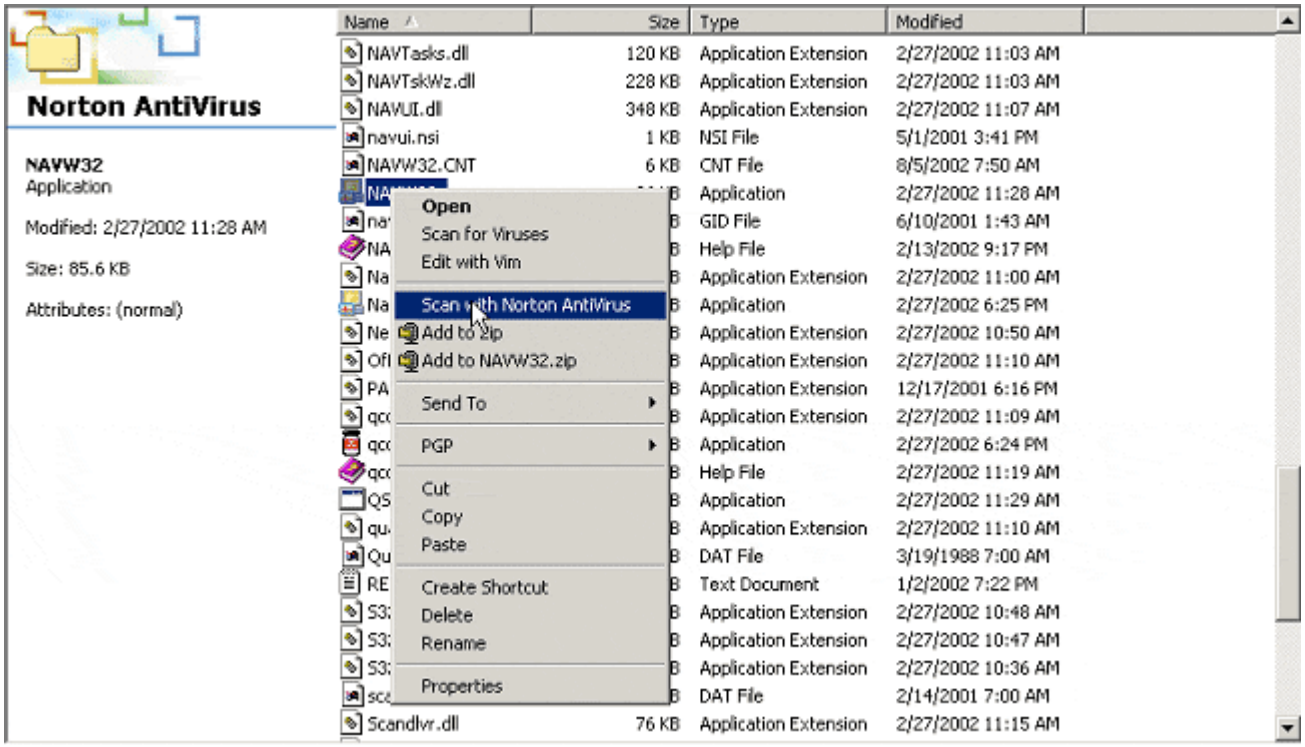
This section shows examples of some of the tasks you need to do when using an anti-virus program on your home computer. These examples use Norton AntiVirus™ 2002. We'll use the **DURCH** tests described in Task 1 - *Install and Use Anti-Virus Programs* to see how Norton's AntiVirus 2002 satisfies each of these tests.

The first window in this section shows the main window for Norton AntiVirus 2002. Through this window, you find the answers to the courthouse tests. You can get to this window through

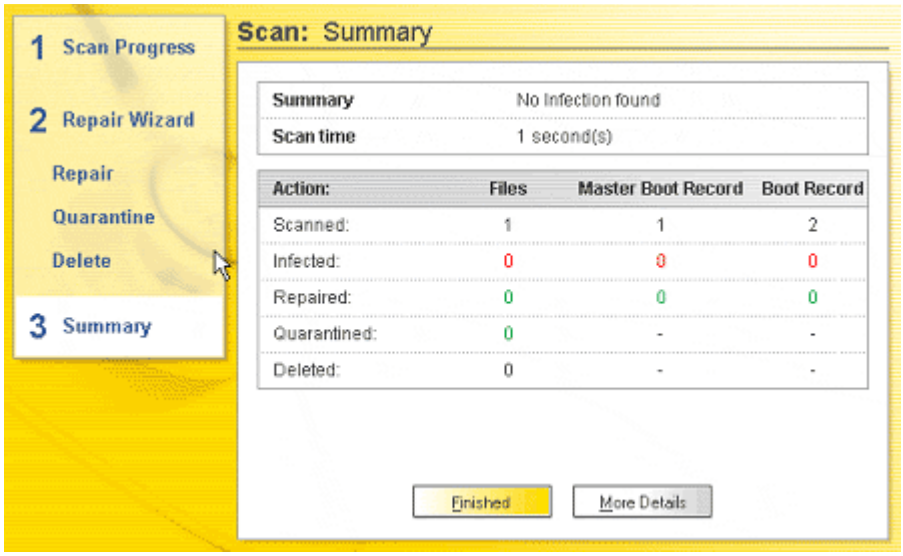
Start→Programs→Norton AntiVirus→Norton AntiVirus 2002.



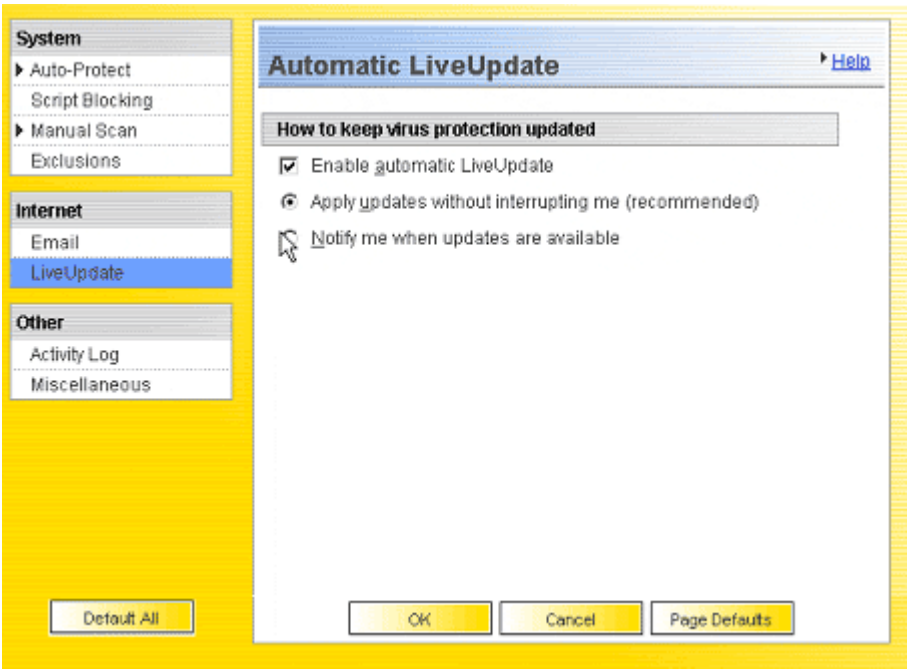
The first test is the *demand* test. Norton's product changes the menu options for Windows Explorer File Browser so that you can check a file or folder on demand. To do this checking, first go to the folder that contains the file you wish to scan. Next, select the file and then click on that file with the right mouse button. Select the **Scan with Norton AntiVirus** menu item as shown in the next window.



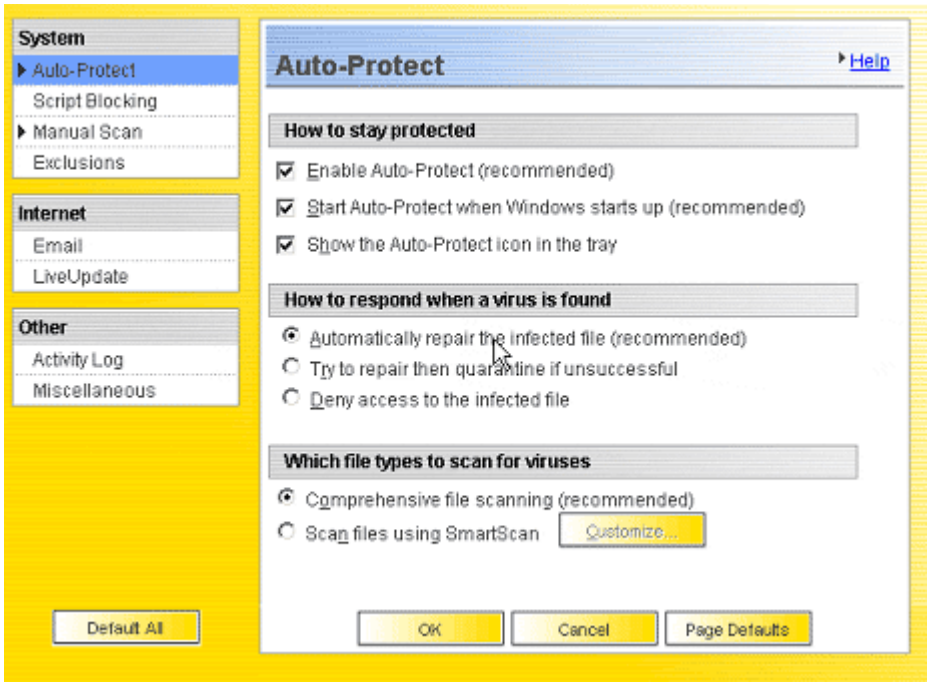
Once selected, the **Scan: Summary** window shows the results of that scan. The file selected contains no virus. This feature means that Norton AntiVirus 2002 passes the *on demand* test.



Next, virus signatures need to be updated daily. With Norton's product, you enable this feature by clicking the **Options→Live Update** buttons. You then select both **Enable automatic LiveUpdate** and **Apply updates without interrupting me (recommended)** as the picture shows. Although you cannot schedule when the update happens, the documentation, which you can view by selecting **Help**, explains that updates happen when you are connected to the Internet. With this option, Norton AntiVirus 2002 passes the *update* test.

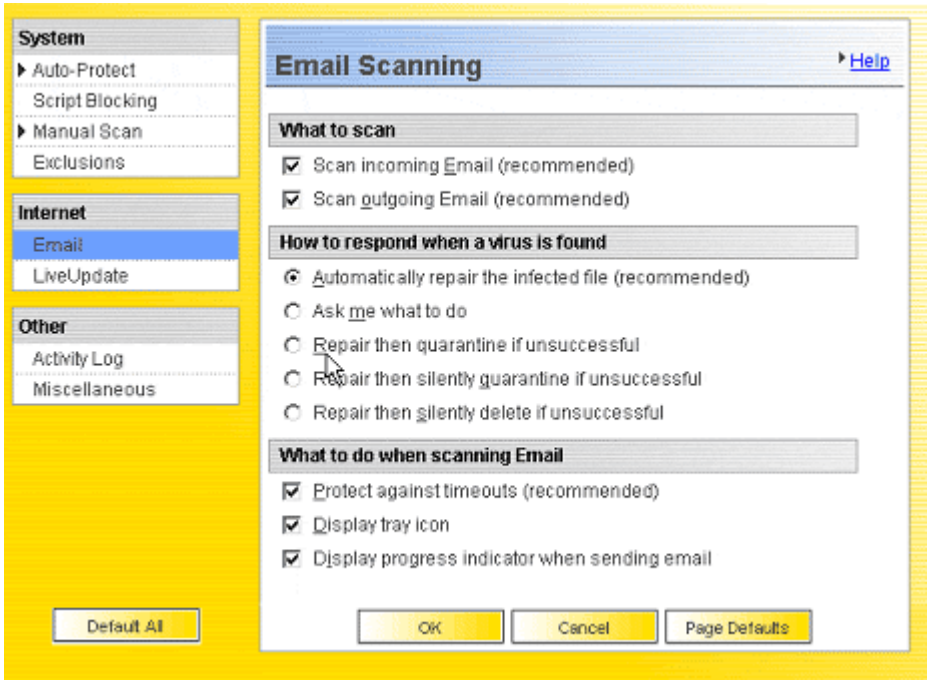


What happens if a virus is detected? This is the *respond* test. With the Norton product, you can decide what happens when a virus is detected through the **Options** menu item. When selected, the **Auto-Protect** window (shown) is displayed. Notice that the default action is to automatically repair the infected file and this action is the recommended one. You also have other options in the window.

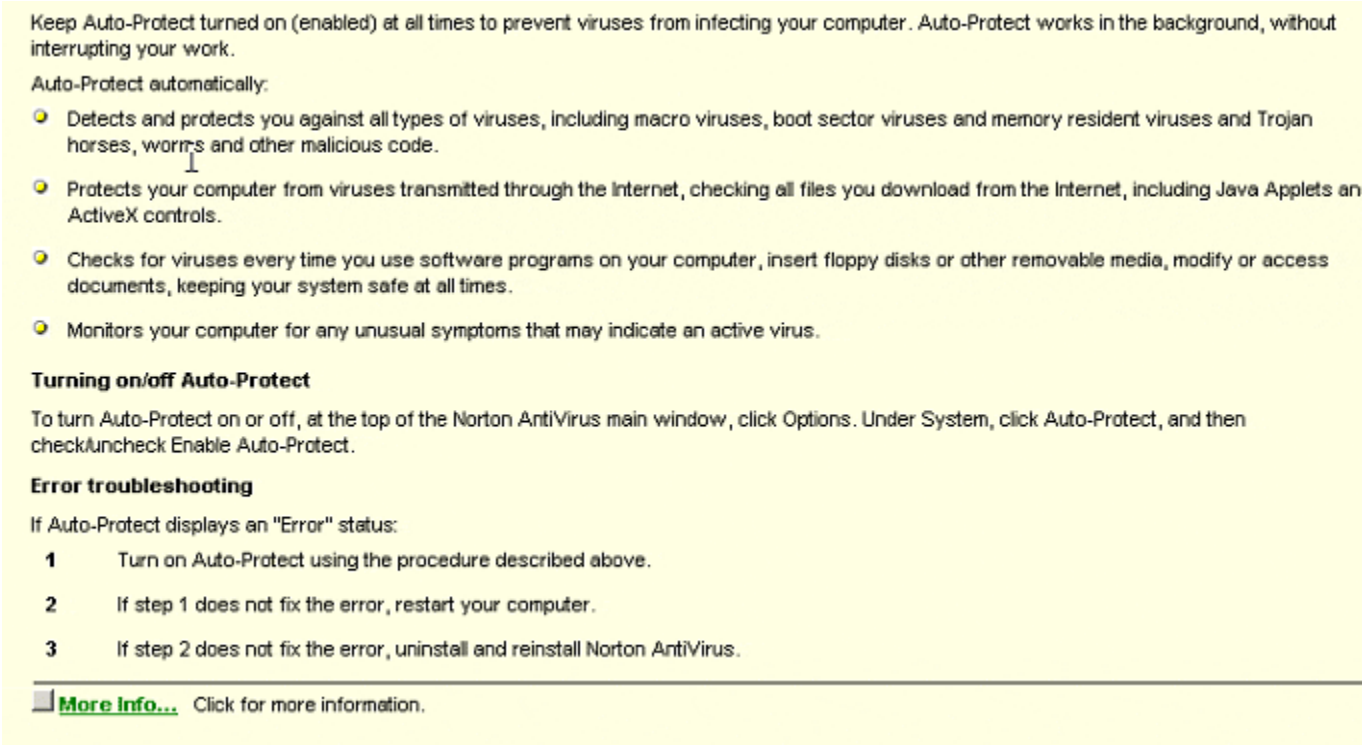


With viruses discovered in email, you have the options that are shown in the next window, **Email Scanning**. These options are available when you select **Options→Email**. Again, you should select all the recommended defaults. These give the maximum amount of scanning and repair (where possible).

With these tests enabled as shown, the Norton AntiVirus meets the *respond* test.

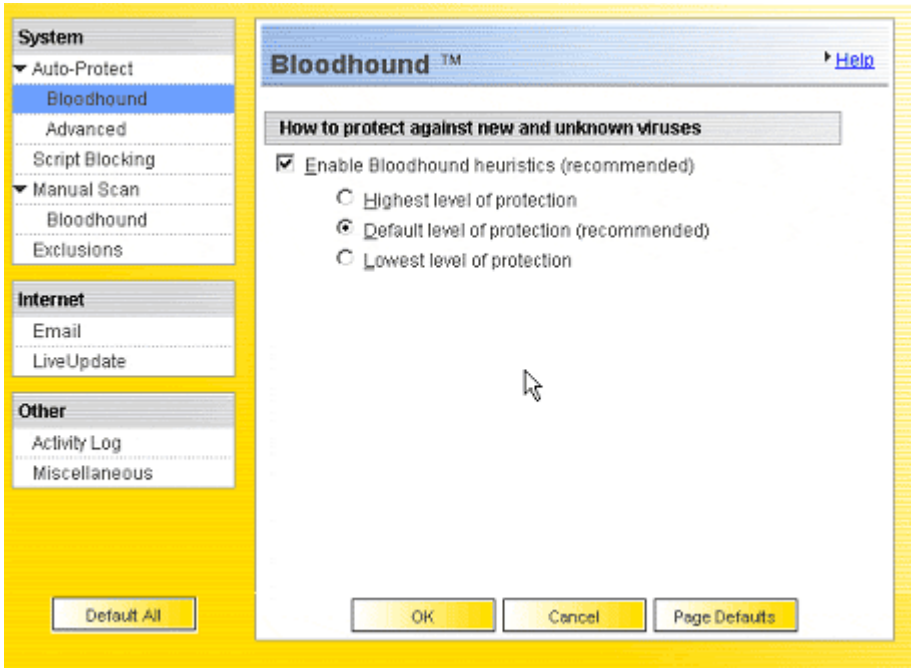


Next is the *check* test. In Norton AntiVirus 2002, this feature is called Auto-Protect. By clicking the left mouse button on the **Auto-Protect** button and then selecting **More Info**, you see a window (shown below) explaining how Auto-Protect works and how to troubleshoot errors.



Also enable the **Email Scanning** and **Script Blocking** checks. To learn more about what they do, follow the same procedure and read the information available through **More Info**. With Auto-Protect, Email Scanning, and Script Blocking checks enabled, Norton AntiVirus 2002 passes the *check* test.

The final test is the *heuristics* test. With Norton AntiVirus 2002, selecting **Options→AutoProtect→ Bloodhound** turns on heuristics tests. The **Bloodhound** window appears as shown here. The defaults in our example screen are the recommended ones. Verify that they are, in fact, what are set up and turned on for your computer.



By selecting **Help**, you'll see an explanation of what the Bloodhound tests do, as shown next.

Norton AntiVirus includes a technology called Bloodhound, which dramatically increases your virus protection against new and unknown viruses.

Bloodhound isolates and locates the various logical regions of a file and then analyzes the program logic for virus-like behavior. Bloodhound detects a high percentage of unknown viruses. In addition, Norton AntiVirus detects unknown viruses by monitoring activity on your computer for behaviors that viruses typically perform. When a suspicious activity is detected, Norton AntiVirus prevents the action from continuing.

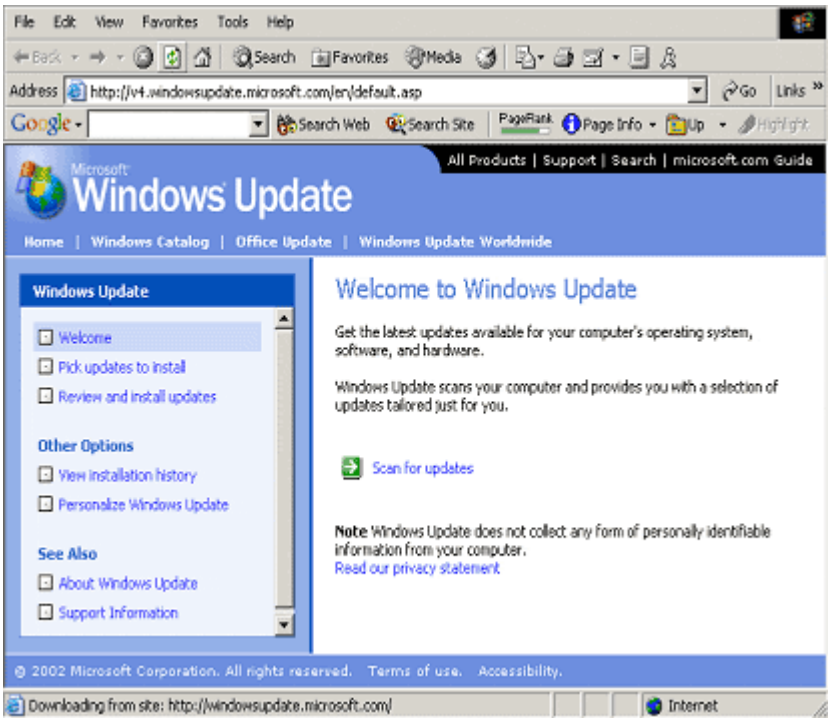
How to protect against new and unknown viruses

Enable Bloodhound heuristics (recommended): Enable or disable Bloodhound by selecting or unselecting the check box. If Bloodhound is enabled, you can also specify Bloodhound's degree of sensitivity to possible viruses. A higher level of protection increases your virus protection against difficult to detect and unknown viruses, and may cause scanning to take a bit longer.

So then, according to the **DURCH** tests, the Norton AntiVirus 2002 product passes and should be considered a viable candidate for you to use to combat intruders who attempt to gain access to your home computer using viruses and worms.

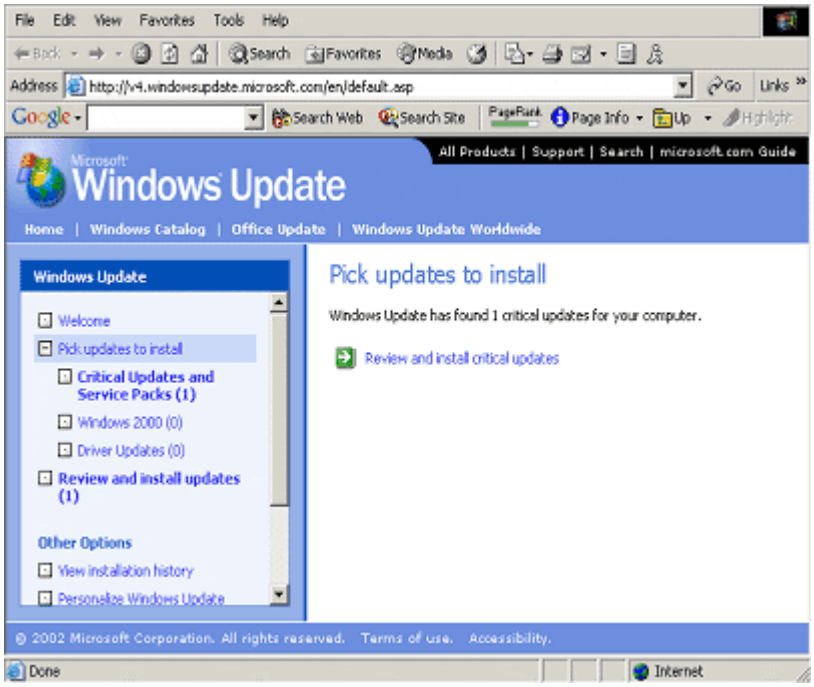
Installing Patches

Windows 2000 provides a quick way to get to patches and updates using your Internet connection. Select this "Windows Update" web site at Microsoft by selecting **Start→Windows Update**. When you do this, you see the picture to the right. By selecting the **Scan for updates** button, you check the patches installed on your computer against the latest set of patches available from Microsoft. Please read the information in the **Note** button to learn how this update scheme works and how it maintains your home computer's privacy.

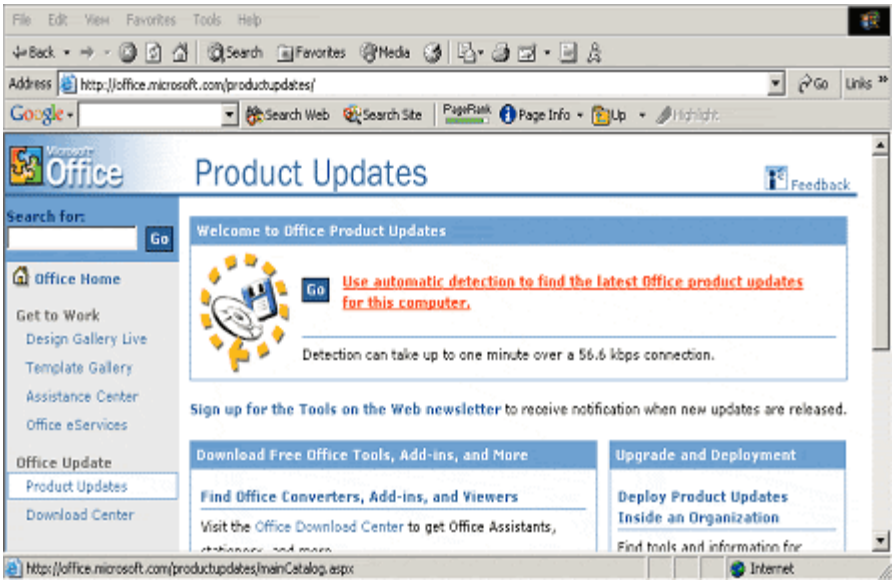


After scanning for updates, you see what patches are available for you to install. What you will see on your computer will almost certainly differ from the window shown below, but you get the idea about what's going on.

This example shows that there is one critical update and service pack available for the computer used in these examples. By clicking the left mouse button on the **Critical Updates and Service Packs (1)** button, you see what the patch does, how big it is, how to install it, and if it can be uninstalled. This is much of the information you need to fill in worksheet for Task 2. From this screen, you select the **Review and install critical updates** button to start the process of installing this patch on your computer.



Similarly, by selecting the **Office Update** button near the top of the Windows Update screen, you see something similar to the next window shown below. Again, the update process scans your computer for any updates that are appropriate to the Office products you've installed. Simply select **Use automatic detection to find the latest Office product updates for this computer** to scan your computer. The results of the scan show the relevant patches for your computer. You select what you want or need, and then install them as you did with the operating system patches we discussed previously.



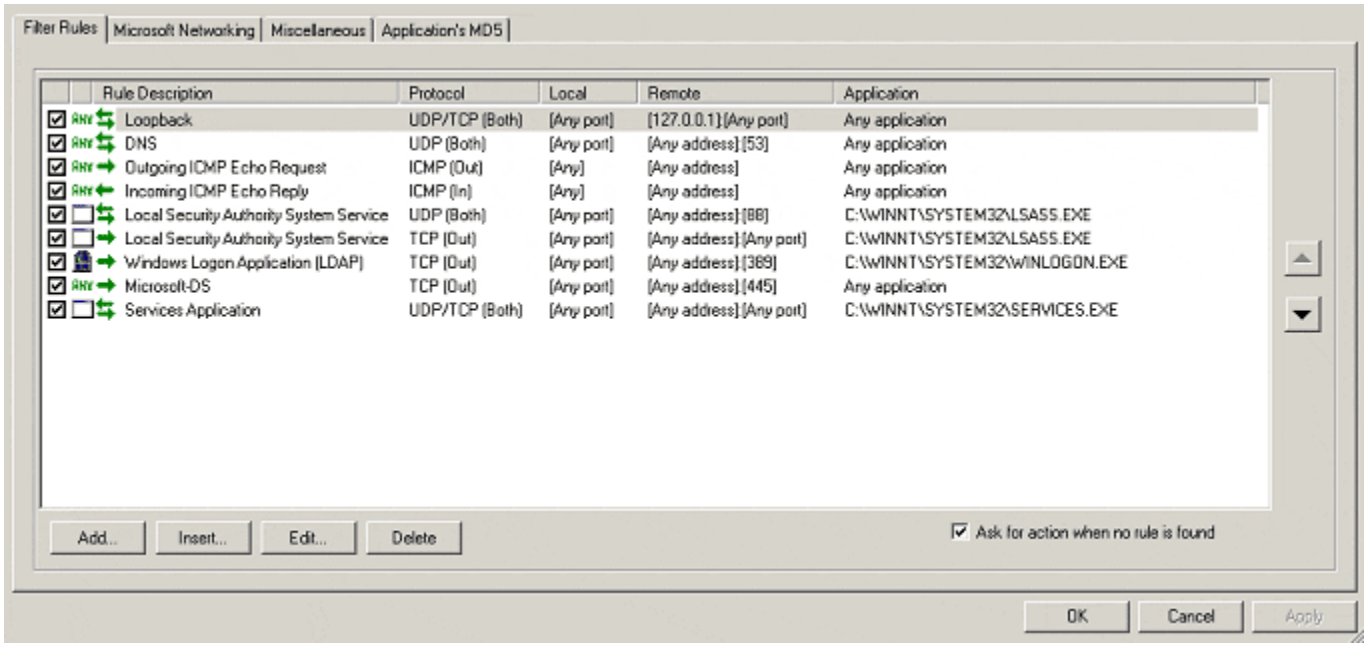
Both of these web pages also let you see which patches you've installed, when you installed them, and where the patch came from. This is a helpful way to see what you've done so far.

Operating a Firewall Program

The product shown in the examples here is the Tiny Personal Firewall (TPF) product from Tiny Software, Inc. Presently, Version 2 is free for home use, but there are newer versions that have more features, such as content filtering. At a minimum, you should install Version 2 if you plan to use it the way the license allows. These examples use version 2.0.15A.

The first task to do with TPF is to make a backup copy of its rules. To do that, you need to copy the `C:\Program Files\Tiny Personal Firewall\persfw.conf` to wherever your backup files are located. It is best to do this when TPF is not running so that the current rule set file is not being changed during your copying operation.

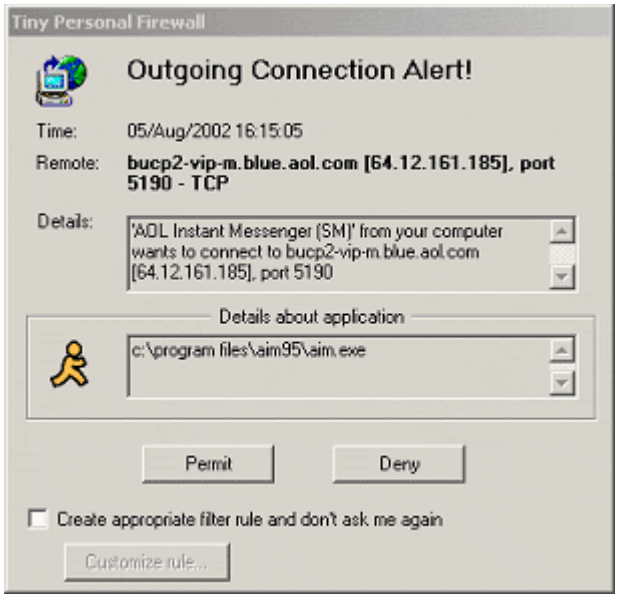
The first window in this section shows the default rules that TPF uses to control access to and from the Internet. You get to this window with **Start→Tiny Personal Firewall→Personal Firewall Administration→Advanced**.



Notice that the **Ask for action when no rule** box is checked. This means that any time traffic is sent to or received from another computer and it is not already referenced by one of these rules, a window appears that asks what to do with that traffic. This TPF feature helps you to screen all traffic to decide what to do with it. You can slowly fill in the rows and columns of the checklist to answer the template tests described in Task 4 - *Install and Use a Firewall Program*.

Let's try to fill in one of those rows in that checklist. To do that, we'll run an application to learn what connections it makes. Based on what we learn, we'll gradually configure TPF so that it allows the connections we want and need, and nothing more. The application chosen for this example is AOL's Instant Messenger (AIM). We'll assume that AIM and TPF are already installed. We'll also assume that TPF is running with the default rules as noted in the window above.

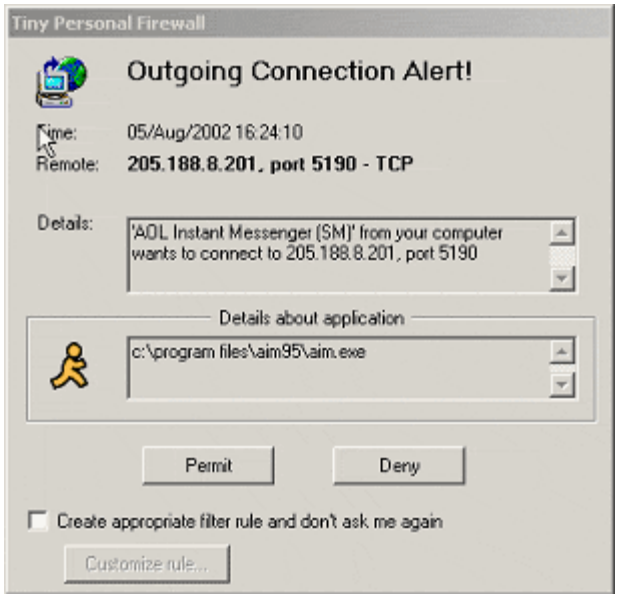
Once we start AIM, we begin to get new windows similar to the one shown here, **Outgoing Connection Alert!** From this window, we know the name of application making the connection (`c:\program files\aim95\aim.exe`) and the remote location to which it wants to connect (both its address – 64.12.161.185 – and port – 5190). We then need to decide if we should allow or deny the connection and if we should make it permanent.



According to the suggestions in Task 4 of this booklet, we don't know the answer to either of these yet, so we'll be conservative and deny the connection. We won't update the rules just yet because we don't know if we want to make that decision permanent. We'll do both of these by selecting the Deny button. For now, we'll just wait and see what AIM does with our decision.

Immediately, the exact same window pops up again, so we'll deny it a few more times to see if it eventually goes away. After a few more tries, we've learned that it won't go away, so now we need to allow the connection. We'll only click on the **Permit** button to temporarily allow that connection. We've not quite ready to take the plunge and updated any of the rules just yet.

Once we permit that connection, another window like that to the right appears. We'll follow our strategy and deny that window for a bit to see what happens. Eventually learn as we did before and permit the connections.



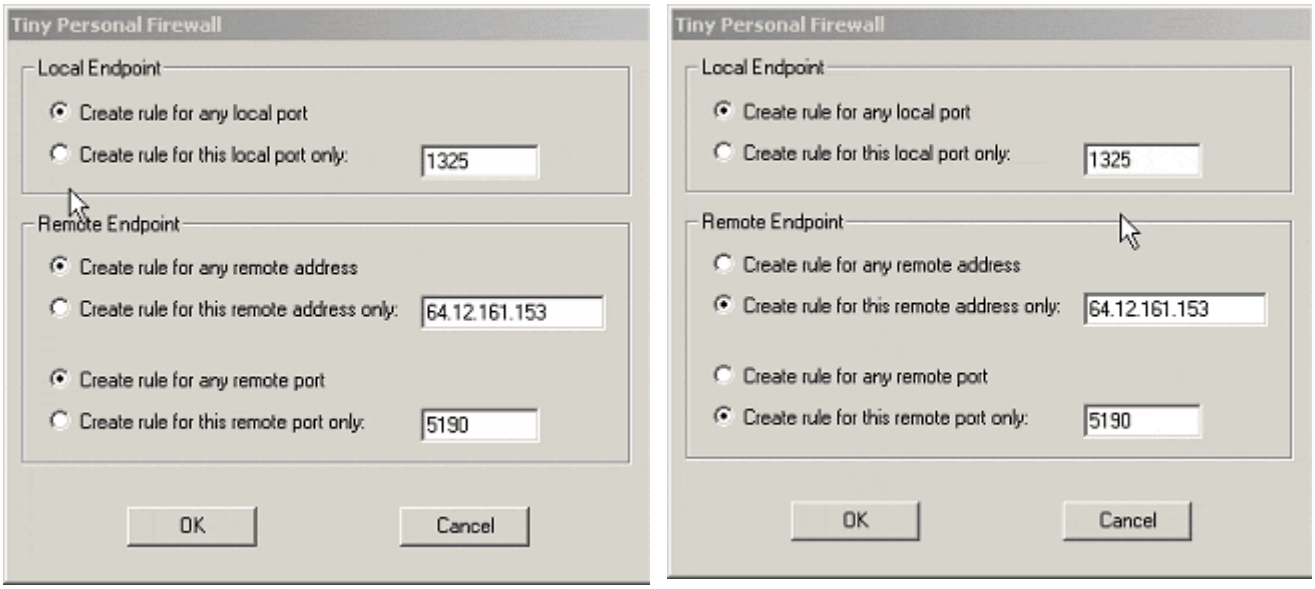
So far, we've learned that AIM has connected to two computers – 64.12.161.185 and 205.188.8.201 – both on port 5190. A reasonable conclusion at this point is that AIM needs to connect to at least these hosts on these specific ports as part of doing its job. Let's continue our investigation.

We'll stop and restart AIM to observe its behavior. We're trying to learn if it makes any other connections or if those we've observe so far are the only connections AIM uses. What we'll find is that it wants to connect to more computers – this time on 64.12.161.153 – again on port 5190. We'll save some time and immediately allow those connections.

At this point, we've learned that AIM wants to connect to a series of locations in the **aol.com** name space. Each time, the port number of the location is 5190, so we'll assume that that is AIM's preferred port. Based on what we've learned, we're willing to accept the fact that AIM should be allowed to connect to any host within the **aol.com** name space but only on port 5190. Now we can begin to add rules that allow these connections without prompting us for our approval. We will designate these connections allowed and permanent.

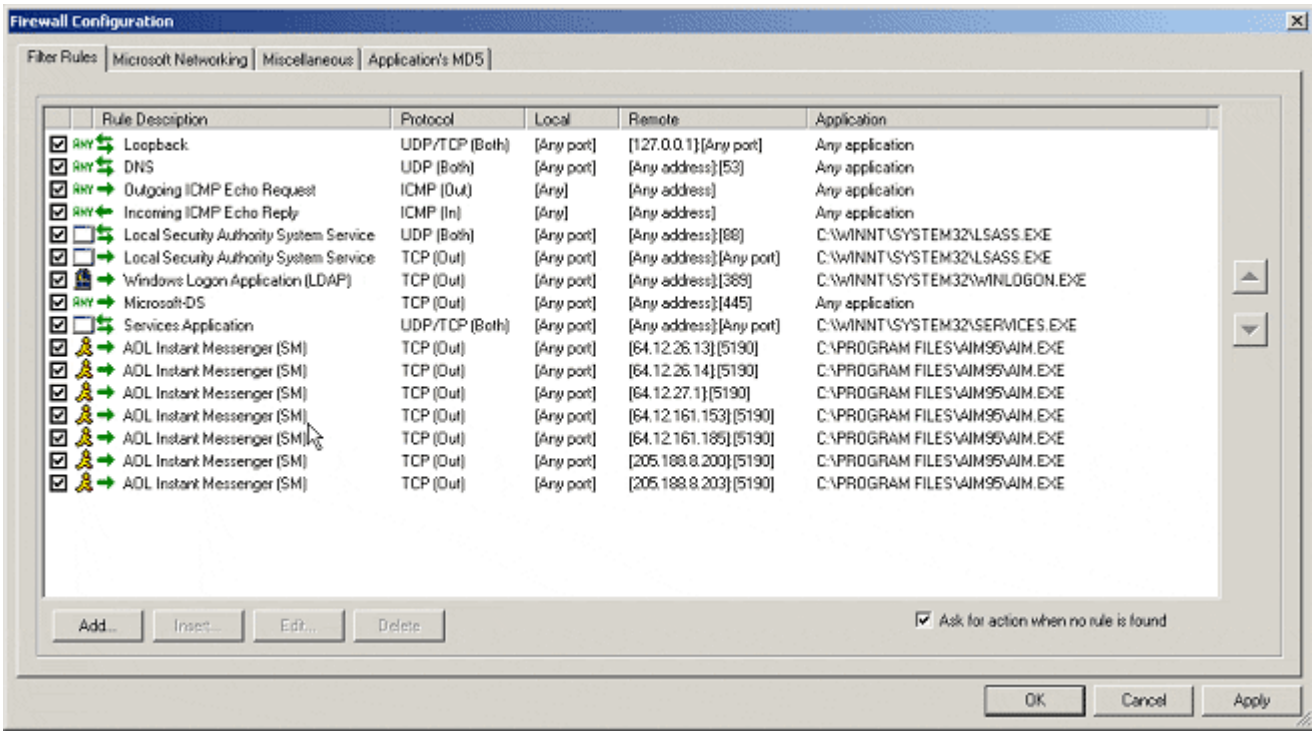
To do this, we'll stop and restart AIM one more time. Instead of temporarily permitting individual connections to **aol.com** computers, we'll select the **Create appropriate filter rules and don't ask me again** button to make them permanent. Selecting this button turns on the **Customize rule** button, and we'll click on it. We get the first of the pair of windows shown, and we'll change it to match

the second window of the pair. We are allowing AIM to connect to a specific computer at a specific port and nothing else. This is the *permanent* test.



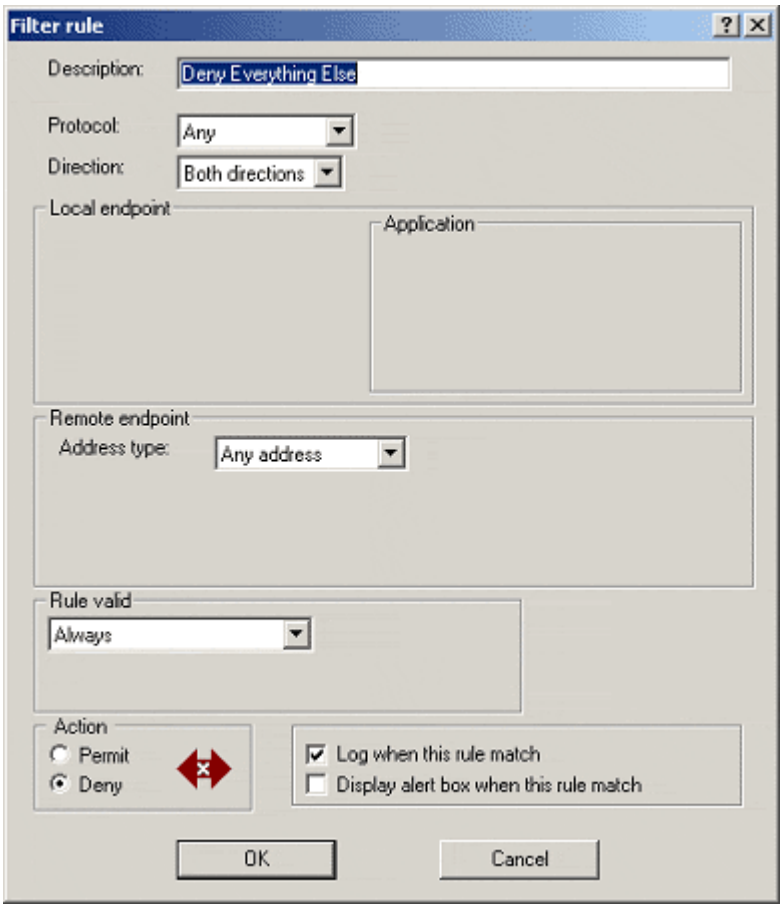
Once we've selected the **OK** button, we'll get back to the original popped up window, where we'll select the **Permit** button. This is the *allowed* test from the template tests.

What we're doing here is to only allow AIM to connect to port 5190 of very specific computers on the Internet, and nothing else. When we restart AIM a few times to let it connect to all the available AIM servers, we'd end up with something like the **Firewall Configuration** window shown below. What you see on your home computer should be similar.



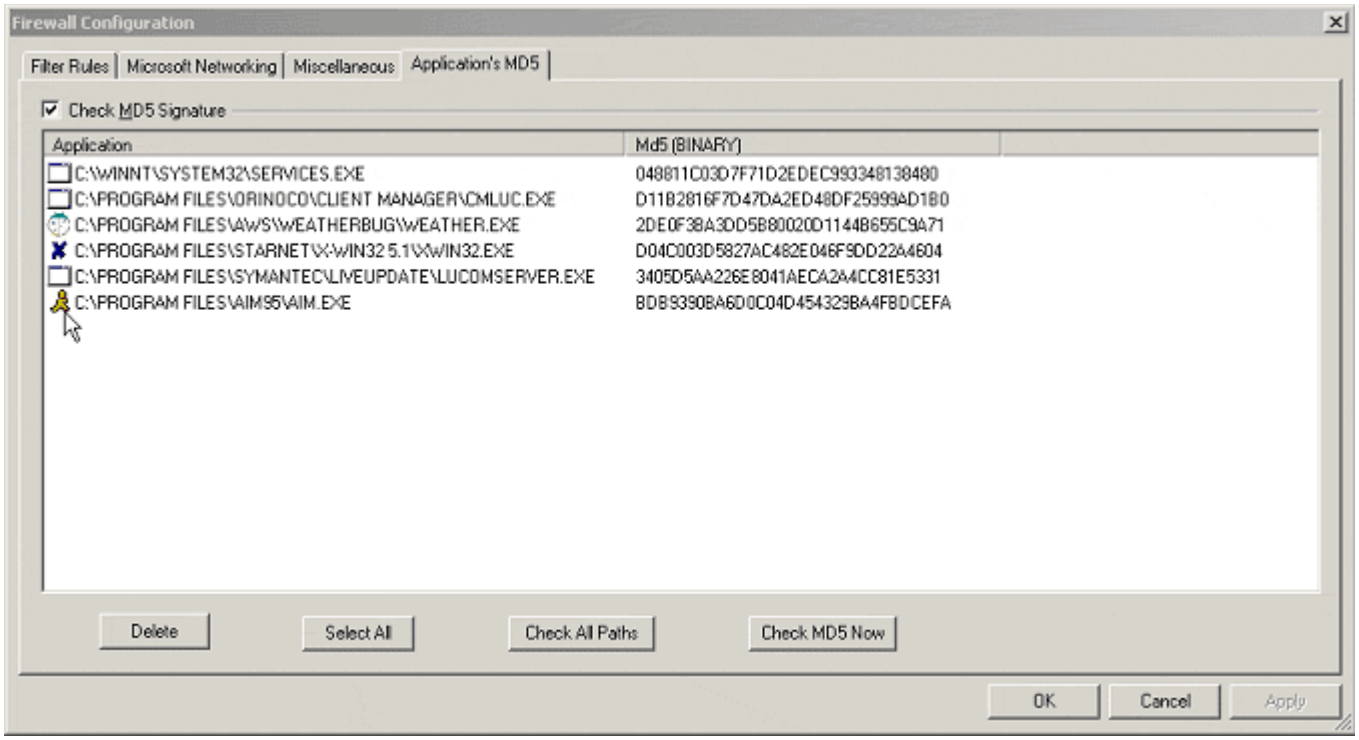
We now have the rules that let AIM connect to the computers it needs to do its job. We've filled in a few rows in Worksheet for Task 4. On your home computer, you'd keep doing this for each application you use. For now, you need to keep the **Ask for action when no rule is found** box checked. This keeps you in a learning mode without granting any extra privileges in the meantime.

Eventually, just like the security guard, you'll create a new rule that denies everything else. The **Filter rule** window shows how to set this up. To get to this window, go to **Start→Tiny Personal Firewall→Personal Firewall Administration →Advanced→Filter Rules →Add**. Click the **OK** button to create the rule, and use the up and down arrows to make sure that this rule is the last rule. You may also want to check the **Display alert box when this rule matches** button for a while so that you can be sure that you are denying what you want to deny.



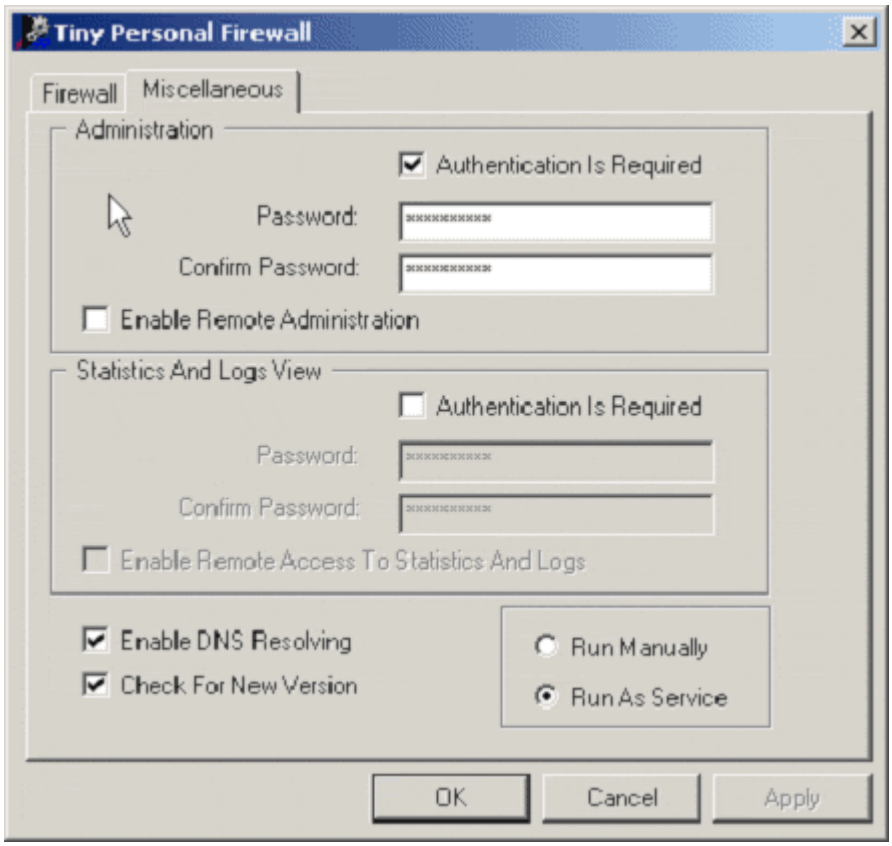
Notice that in the **Filter Rules** tab, each rule lists the application and the constraints place upon it by that rule. If the constraints on the application were based solely upon the application's name, it would be all too easy for an intruder to replace that application with another that does its designed task and perhaps a little more. For example, imagine the AIM application also connects to some other computers on the Internet for the purpose of also relaying the confidential information you have on your hard disk.

To reduce the likelihood of this problem, TPF maintains integrity information about each application referenced by a rule. The **Application's MD5** tab shown below lists this information. To turn on this feature, check the **Check MD5 Signature** box.

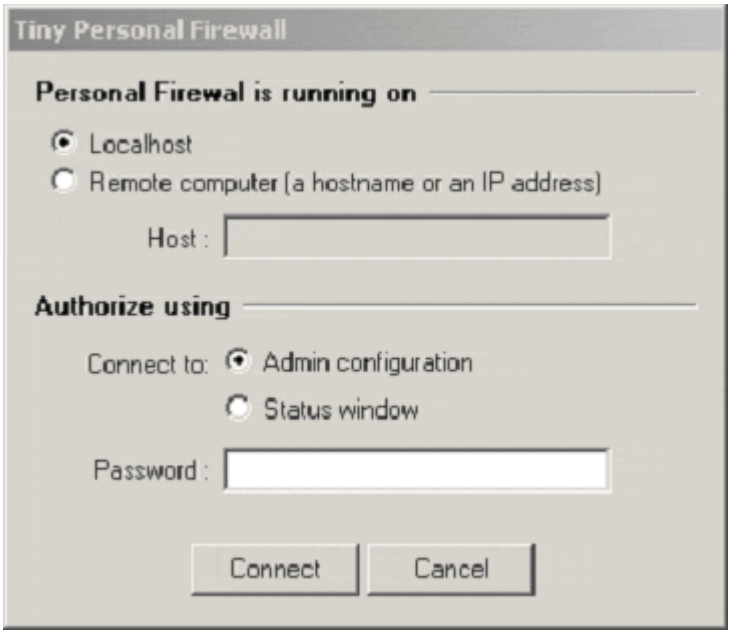


If you or someone else installs a new version of an application, TPF will notice that the MD5 signature has changed and will alert you. You can decide if the change was expected and TPF should update its signature, or if something has gone wrong.

The last feature to demonstrate is putting password protection on changes to the rules. By selecting the **Miscellaneous** tab, TPF displays the window shown here. This window lets you setup TPF so that it requires a password before doing administrative tasks. Notice that remote administration is disabled. In the home computer environment, this restricts those who can change the rules on your firewall. Leave this turned off so that only someone sitting at your home computer can change the firewall's operation.



The more important of the two passwords that can be set is the firewall administration password. You should add an administrative password to guard against unexpected changes being made to your rules. You may choose to add a password to the statistics and logs if you wish to restrict access to them. Remember to use the guidelines given in Task 6 - *Use Strong Passwords* when selecting a password.



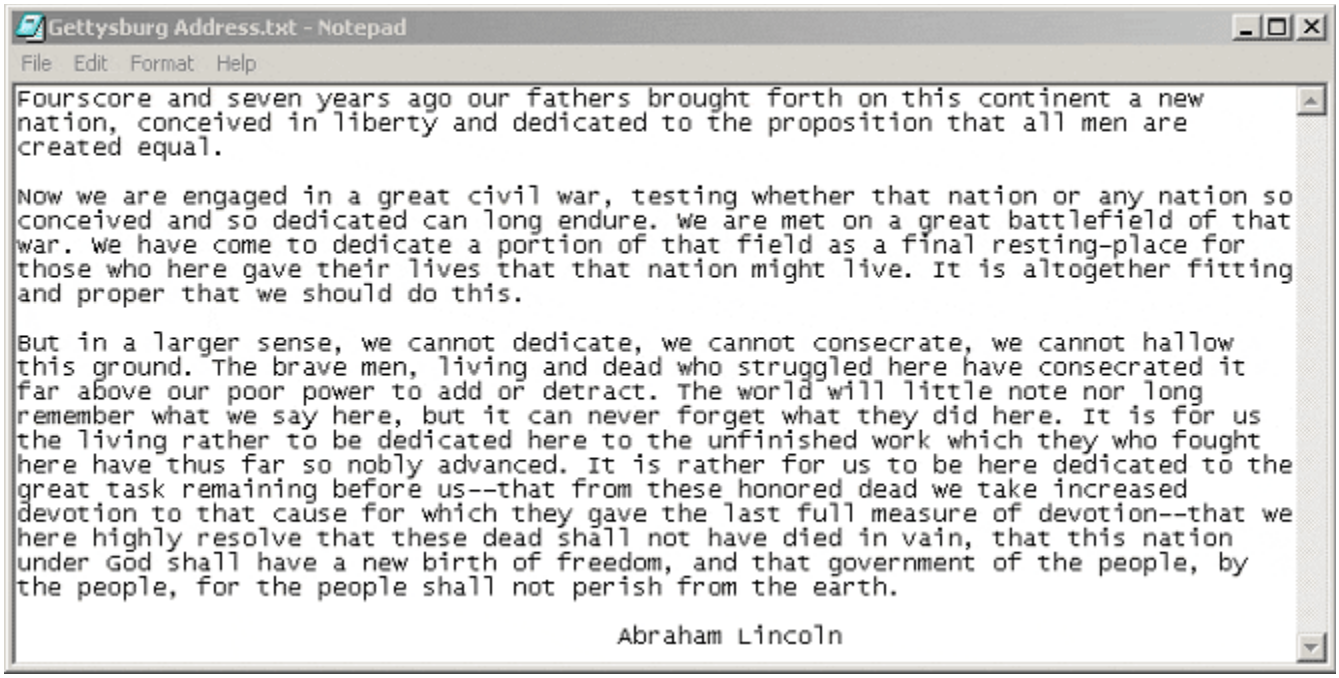
With an administrative password, attempts to access most of TPF's features are first greeted by a window similar to that shown here (beginning with **Personal Firewall is running on**). For your firewall on your home computer, you will connect to the computer identified as **Localhost**. Once you've entered the correct password, TPF operates just as it did before.

Tiny Personal Firewall from Tiny Software, Inc. is a firewall application that gives you control over the connections that your home computer makes. It has a learning mode that lets you review each connection as it happens. You can learn what your home computer is doing and allow only those connections that you want and need. Through integrity checking, even small changes to applications are recognized and can be used to disallow future connections. TPF administration can be guarded by a password.

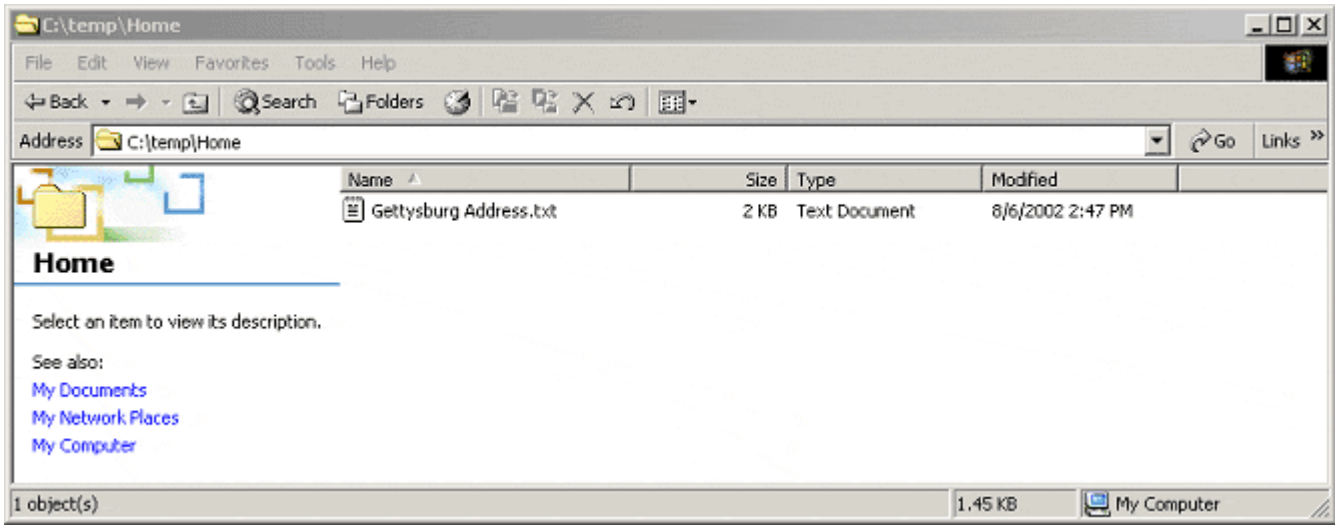
Encrypting and Decrypting Files

File encryption is one way to guard against losing information confidentiality if a file be stolen or in some other way captured. This section shows an example of a file encryption tool. There are many file encryption tools on the market. The tool selected for demonstration here is HandyBits EasyCrypto Deluxe. Version 5.5 is free of charge for personal use. It runs under many versions of Windows, and the examples shown here are run under Windows 2000.

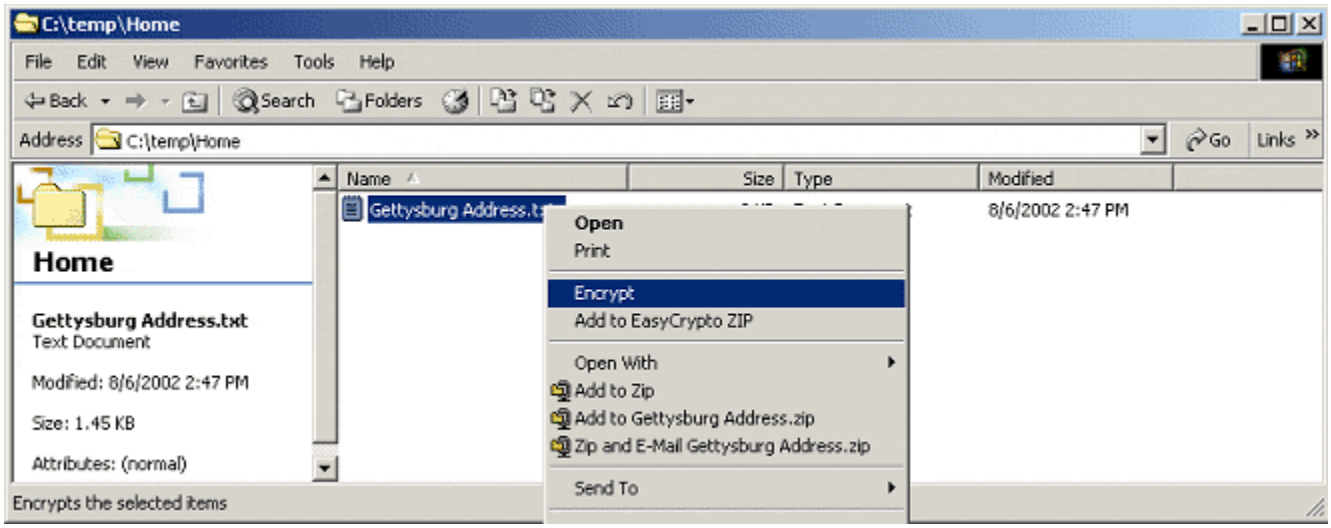
EasyCrypto Deluxe is integrated into Windows Explorer so that you can easily encrypt a set of files and folders by selecting them and then right clicking to bring up the encryption menu. To demonstrate this, let's first create a simple file using the Notepad application (**Start→Programs→Accessories→Notepad**). The window below shows Lincoln's Gettysburg Address saved in a file named `Gettysburg Address.txt`.



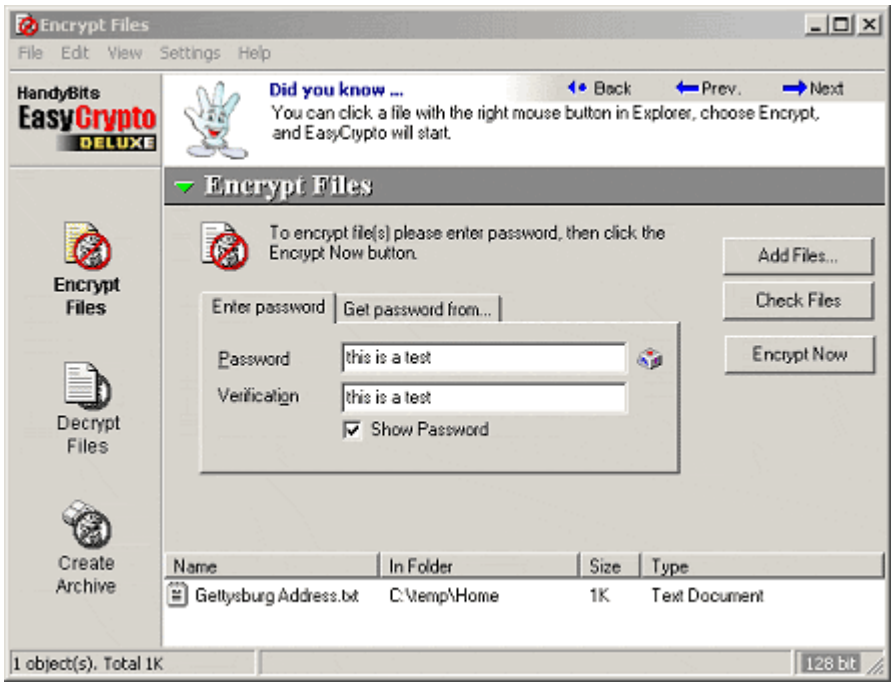
The next window shows it stored on disk. This is the Windows Explorer view.



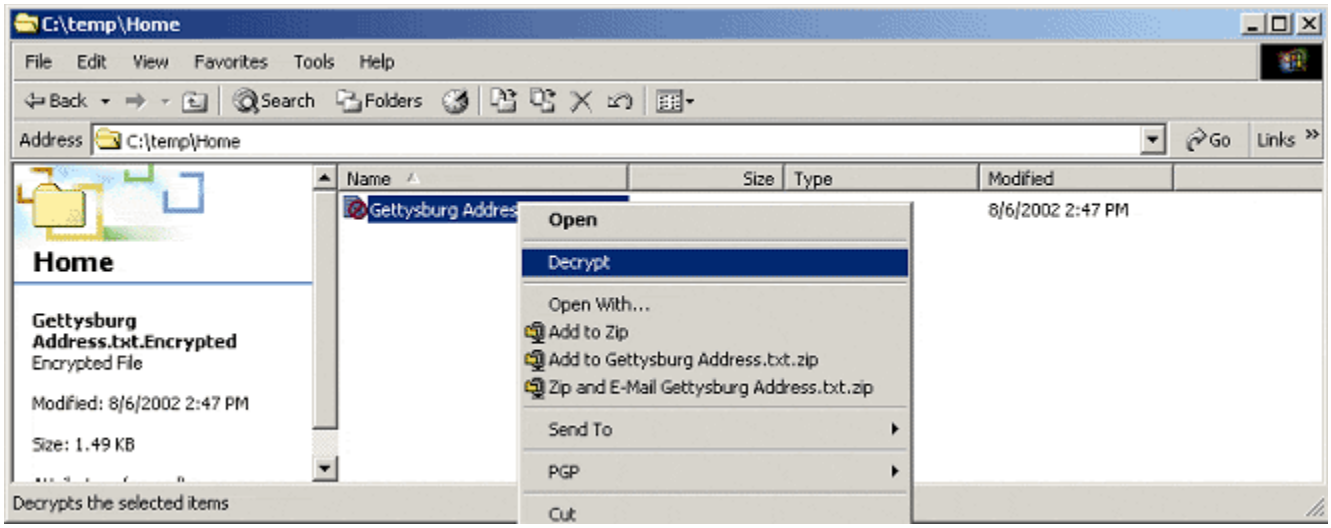
To encrypt this file, select it by clicking once with the right mouse button on the file's name, and a menu will appear. Because of the integration into Windows Explorer, that menu will contain an item appropriate for the type of entry. That is, since this file is not encrypted, the menu will contain an **Encrypt** item, as the window below shows.



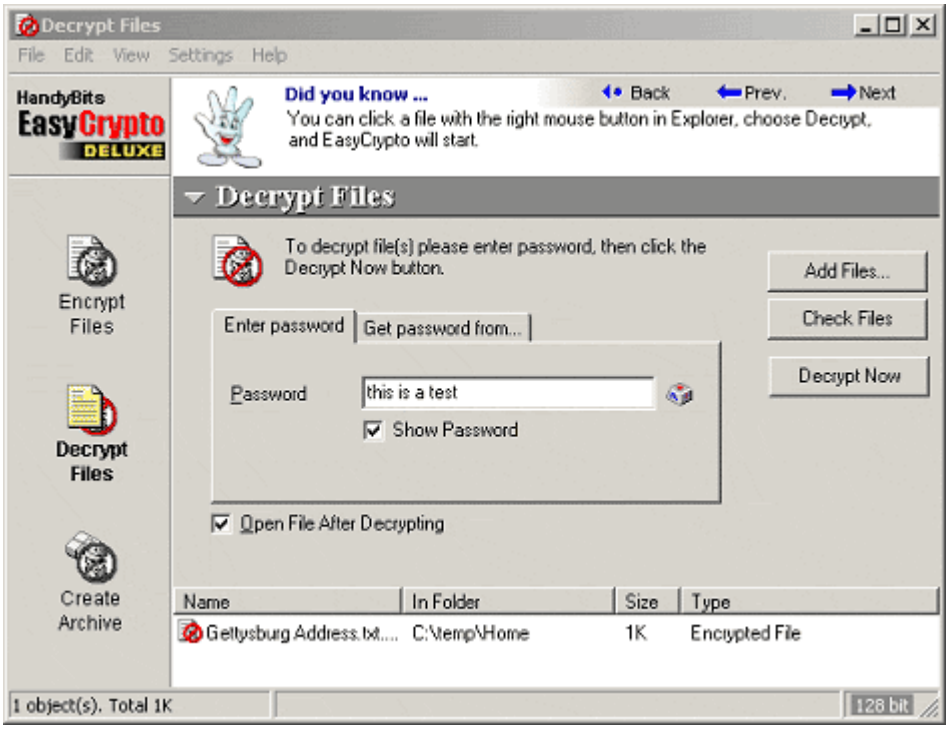
When you select **Encrypt**, the next window (**Encrypt Files**) appears. This window shows the name of the file to be encrypted. The **Show Password** box is checked so that you can see the password used to encrypt this file. This is not the default, and in general you shouldn't check this box. Showing a password in the clear makes it easier for someone to look over your shoulder and see the password. Clicking the **Encrypt Now** button encrypts the selected files. EasyCrypto removes the clear text version once it has been encrypted. This helps keep your confidential information private since the readable copies are destroyed after encryption.



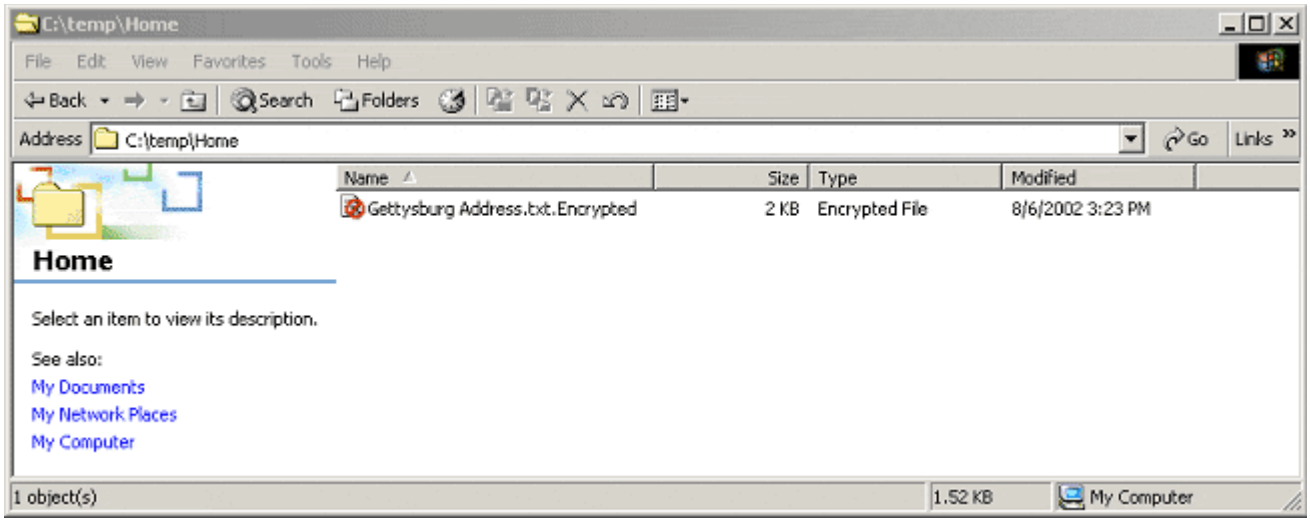
Now, to decrypt the same file, use Windows Explorer again in the same way. Notice this time, the menu item has been changed to **Decrypt** because the selected file is encrypted.



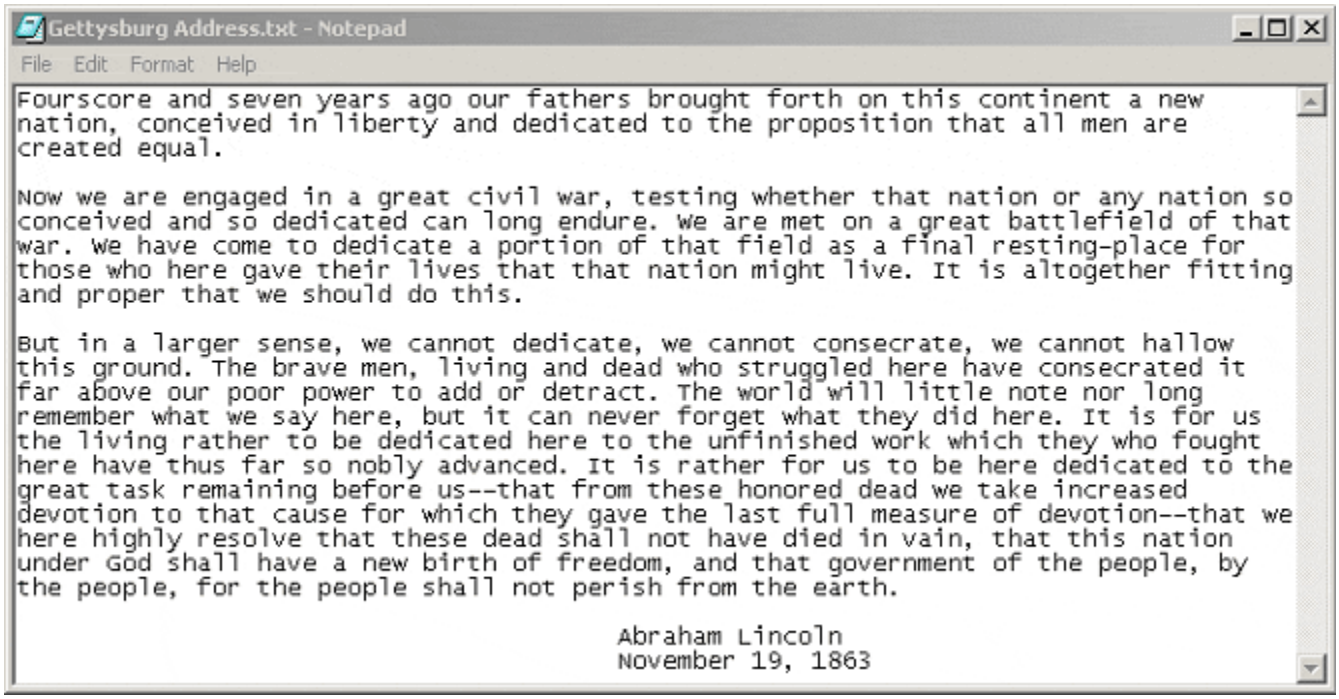
The window that pops up has also changed since the action to be taken – decryption – is also different. Again, notice that the **Show Password** box is checked, as is the **Open File After Decrypting**. This is especially useful if you are going to work on an encrypted file by decrypting it first and then encrypt again it with the changes you've made. Once you click on **Decrypt Now**, it will be decrypted and the appropriate application started to open the file.



In this case, the date when the Gettysburg Address was delivered – November 19, 1863 – is added below Lincoln's name, and the file is then saved. To encrypt again, select **Edit→Undo**. The window below shows the encrypted version as it appears in Windows Explorer.



The next window shows the decrypted file, along with date change just added.

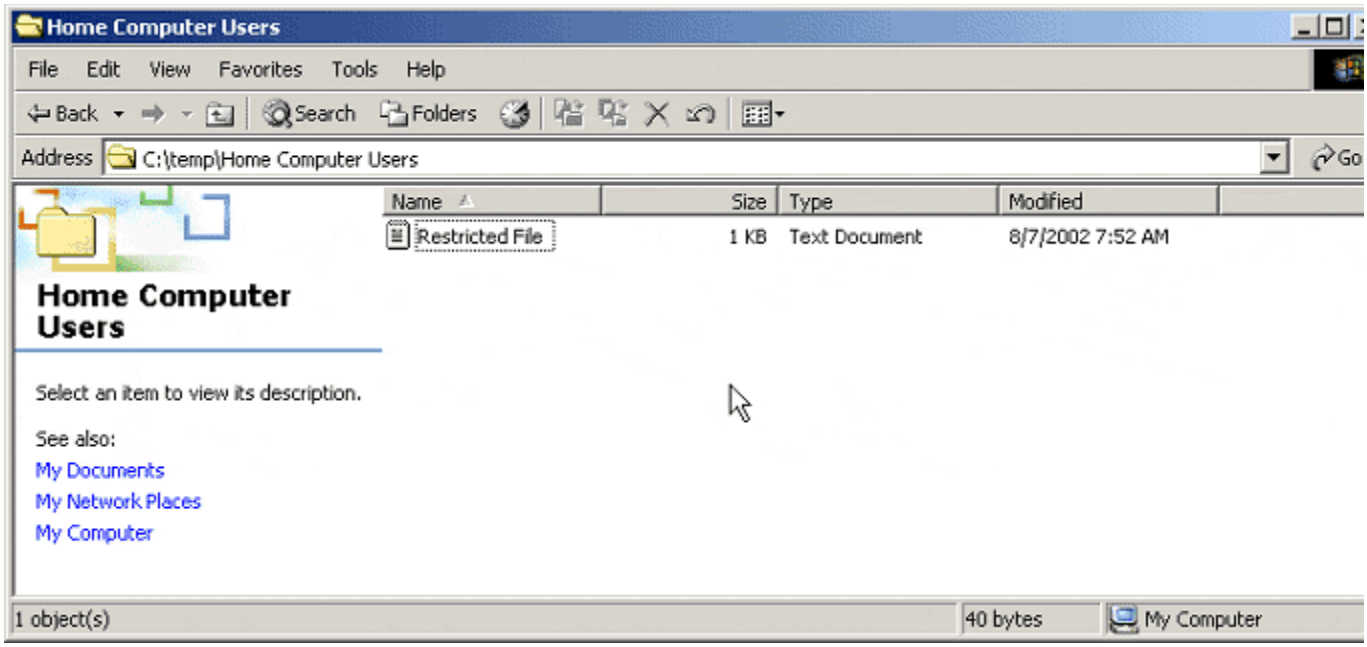


Encrypting files is an extra way to guard against losing the confidentiality of information if the files are stolen or in some other way captured. Remember from Task 9 - *Install and Use a File Encryption Program and Access Controls* that the encryption method should be strong enough to safeguard the information during its useful lifetime. The product that has been shown here – HandyBits EasyCrypto Deluxe – uses strong encryption to achieve that goal.

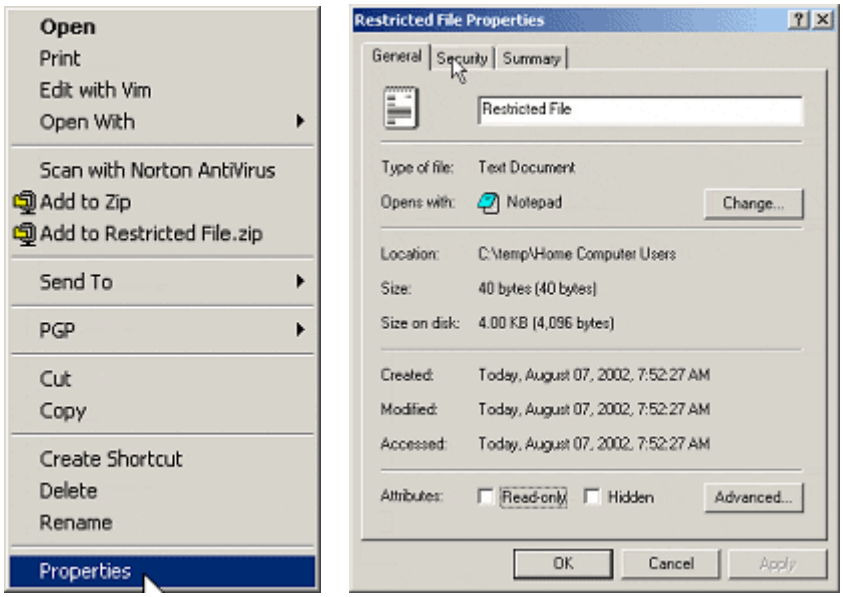
Adjusting Access Control Lists

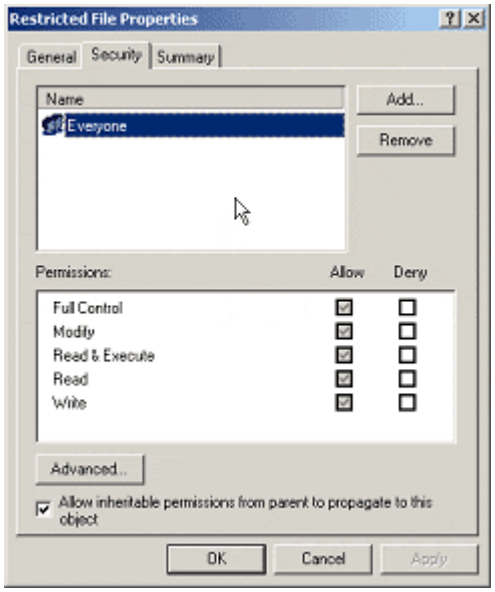
The reason for adjusting access control lists (ACLs) on files and folders is to grant only those permissions needed for your home computer's users to do what they need to do. Just like important papers stored in a locked file cabinet, ACLs lock access to the files and folders they guard. The examples of setting ACLs use Microsoft Windows 2000. Please note that only Windows NT, Windows 2000, and Windows XP have ACLs. If you do not use one of these systems, you can skip this section.

Where do you find the ACLs for a file or a folder? Before answering that question, let's first create a folder and put a file in that folder. We'll work with this test folder and file to show how ACLs work and how to adjust them to restrict access. The folder we'll create is `C:\temp\Home Computer Users`. We'll use Windows Explorer to create it. We'll then add a file named "Restricted File" to that folder. We'll use the Notepad application (**Start→Programs→Accessories→Notepad**) to create it. The window below shows the contents of this folder after we've created this file. If your computer does not have a `C:\temp directory`, you need to create it first.



Click with the right mouse button on this file and you'll see a menu similar to the next one shown. Next, select **Properties** from this menu and the **Restricted File Properties** window will appear as shown. Finally, select the **Security** tab and you'll see a window similar to that shown with the **Security** tab on top. This window shows the access control list for `Restricted File`.



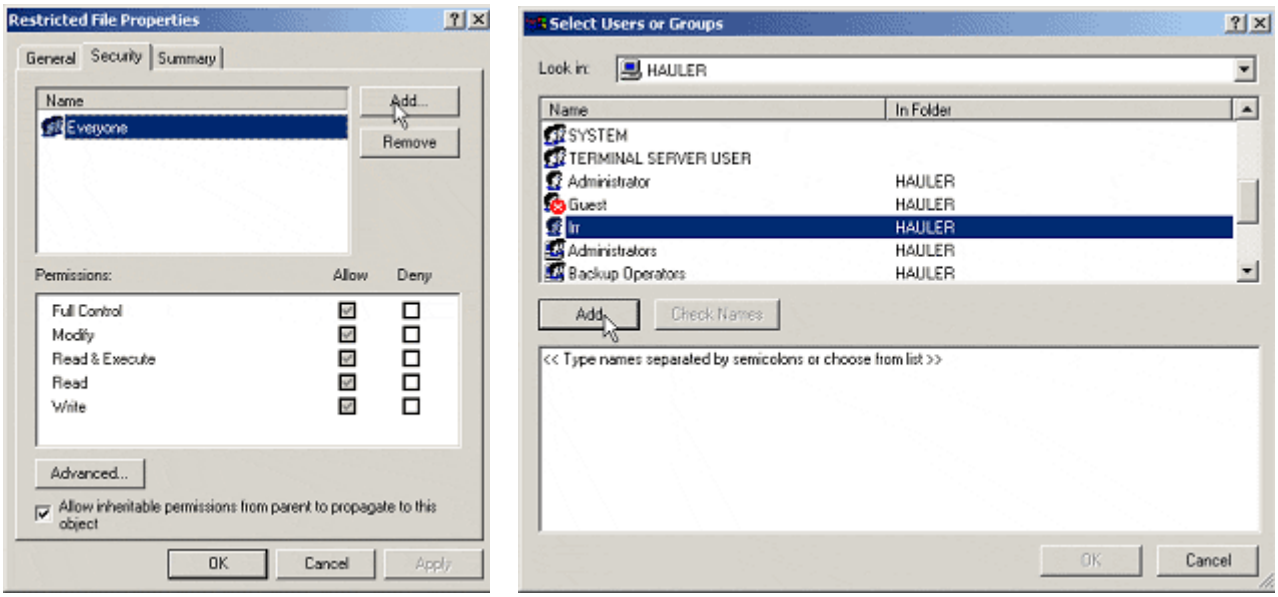


From the **Security** window, we see that an entity named **Everyone** has **Full Control** over `Restricted File`. This means that everyone who can access this file can modify it, read it, and write in it. This access control list is too lenient and needs to be adjusted.

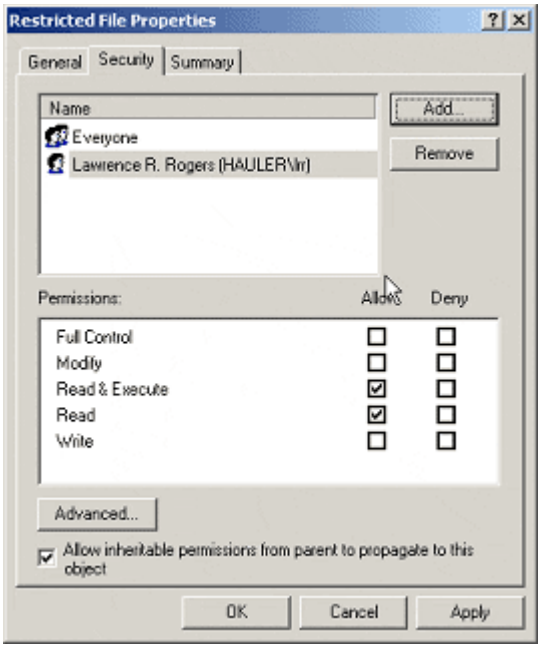
To restrict access, we need to add the users who need access and remove those who don't. In addition, those who need access also need the right type of access. These are the watchful tests from Task 9 - *Install and Use a File Encryption Program and Access Controls*.

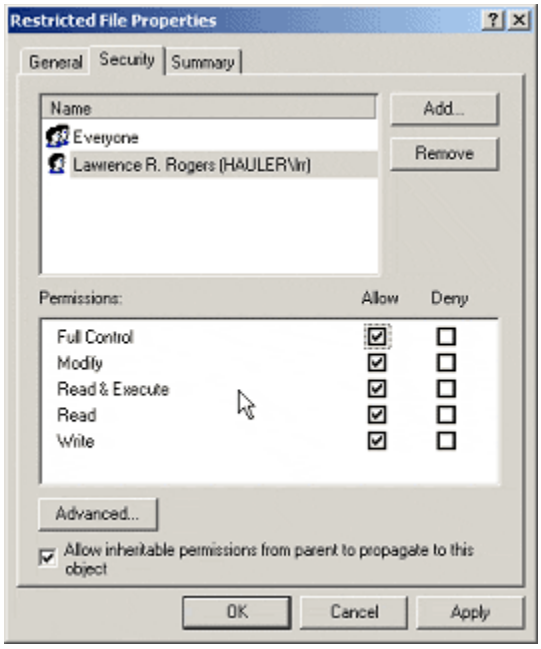
The user who needs access to this file is **lrr**, the author of this document, and the access that he needs is **Full Control**. The **Everyone** entity should have no access. Now that we know who needs access and the type of access, we can proceed.

First, let's add **lrr** to the access list. We begin by clicking **Add** on the window on the left. When we do, we get the window on the right. We scroll down to the user we want to add – **lrr**– and then click **Add** and then **OK**.

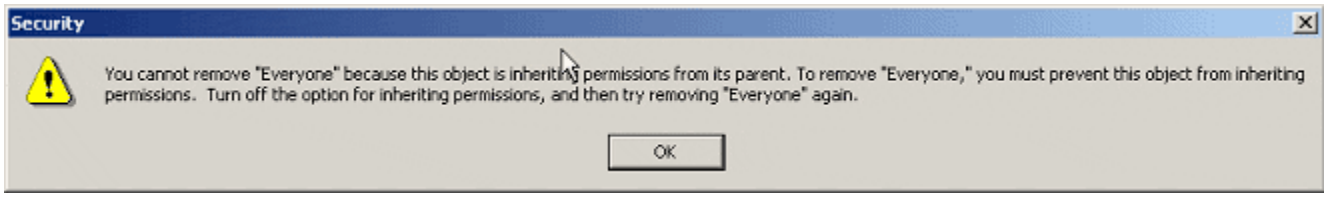


This gives us the next window, which we then change to the window that follows it by giving **Full Control** to **lrr**.

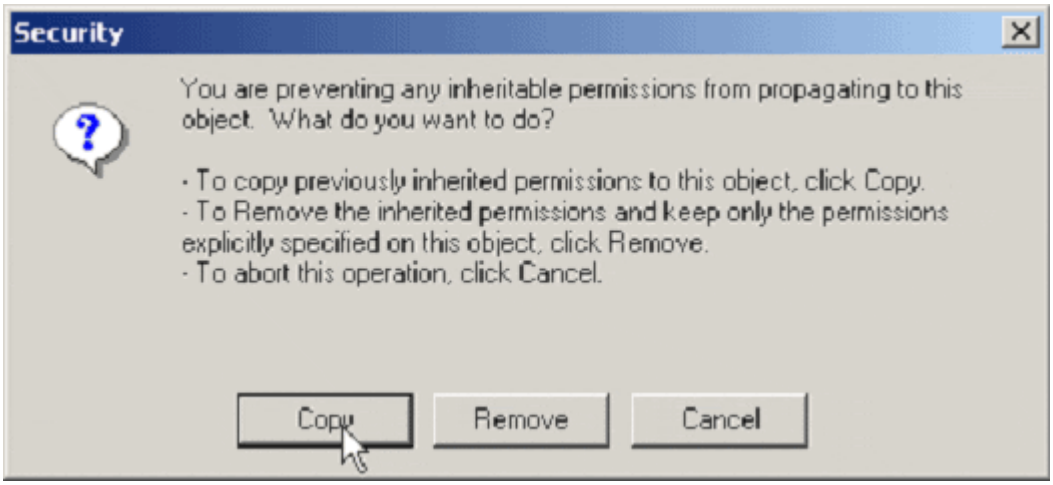




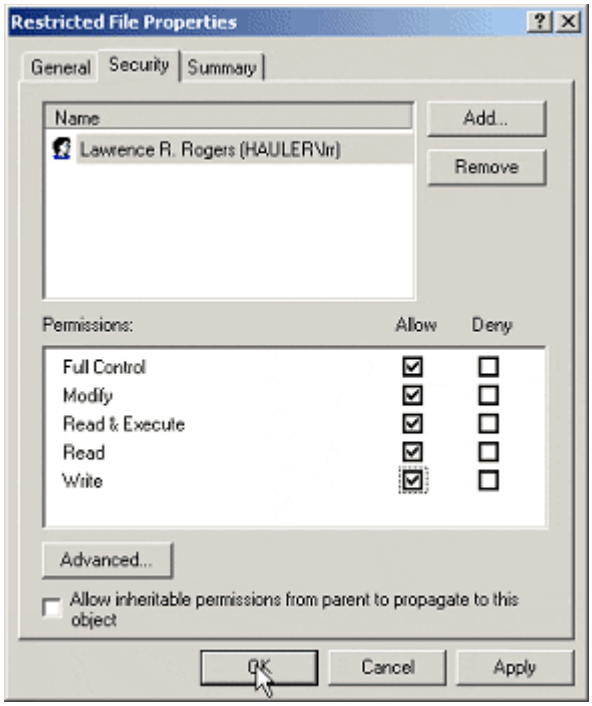
Next, we're going to remove **Everyone** from the access list. We left click on **Everyone** and then click **Remove**. When we do, we get a warning (shown) that we can't remove **Everyone**.



This means that we need to uncheck the **Allow inheritable permissions from parent to propagate to this object** box. When we click **OK**, we get a set of choices, as shown in the next picture.



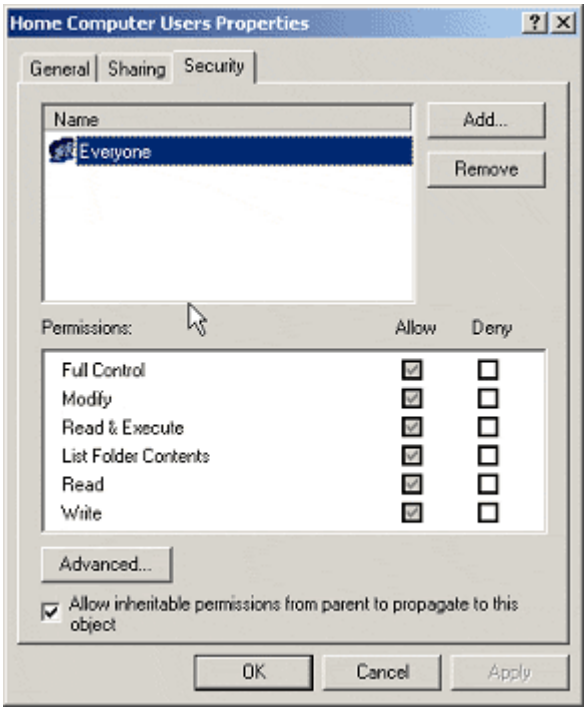
We'll click **Copy**, and then the **Restricted File Properties** window reappears. We'll select **Everyone** again and then **Remove**. When we're all done, we'll see something like the **Security** window here. We'll then click **OK**. The `Restricted File` now has the permissions we want: **lrr** has full control over the file, and all other users have no access at all.



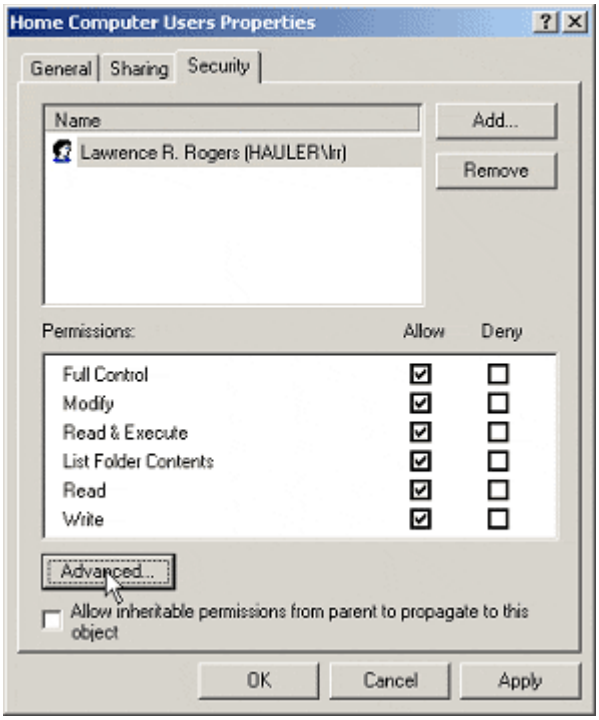
If we want all files in this folder to have the same permissions, we need to adjust its ACLs as we did above. After a while, the process may become unwieldy. Perhaps we'd even forget to adjust ACLs for some files. The confidentiality of these files might be compromised because some of the files may not be appropriately secured.

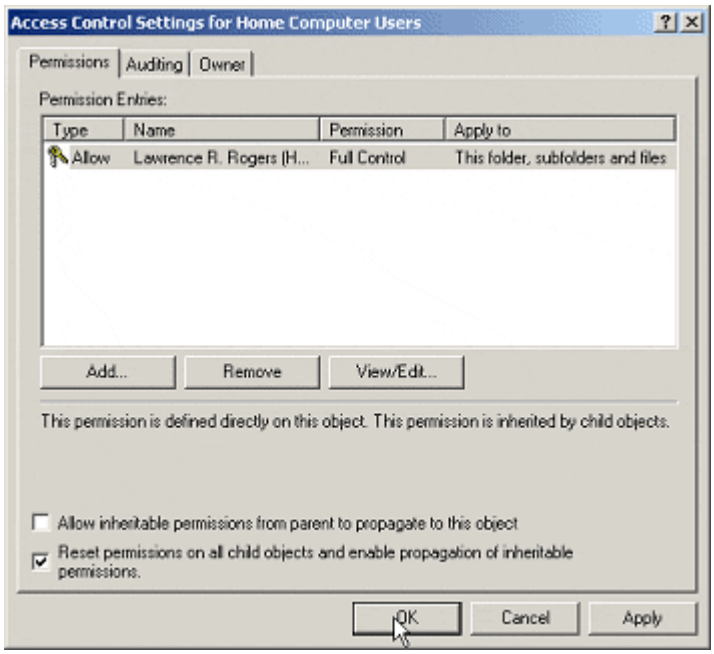
Fortunately, there is a better way to adjust all files and subfolders in a folder, including those yet to be created, so that they inherit the permissions from a parent folder. We'll set this up next.

We first need to move to the parent directory, `C:\temp`, so that we can work on the `Home Computer Users` folder. Once there, we'll right click on that folder, select **Properties**, and then the **Security** tab. Initially, it looks like the window shown here, with **Everyone** listed in the Security window. We'll repeat what we did before, except that we'll do that to a folder instead of a file. Those tasks are: add **lrr** with **Full Control**, turn off the **propagate permissions** check box, and remove the permissions for the **Everyone** entity.

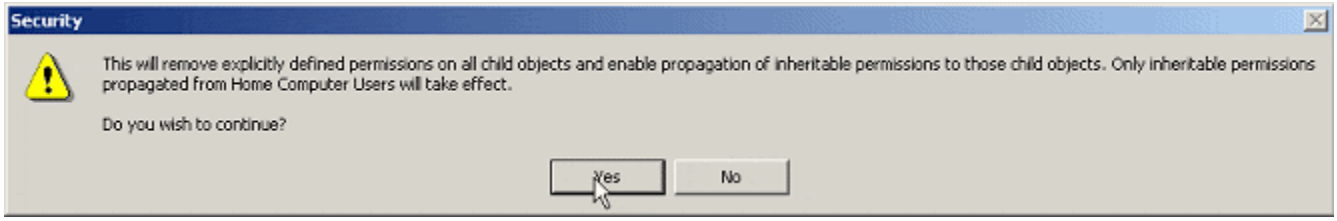


When we're all done, the window looks like the next window, with **lrr** listed. However, before we click **OK**, we need to do one more thing. We need to click on the **Advanced** button to bring up another window. This new window lets us propagate the permissions we've just set to all files and subfolders in that `Home Computer Users` folder. This window looks like the one shown with the **Permissions** tab on top and **Permissions entries** listed.





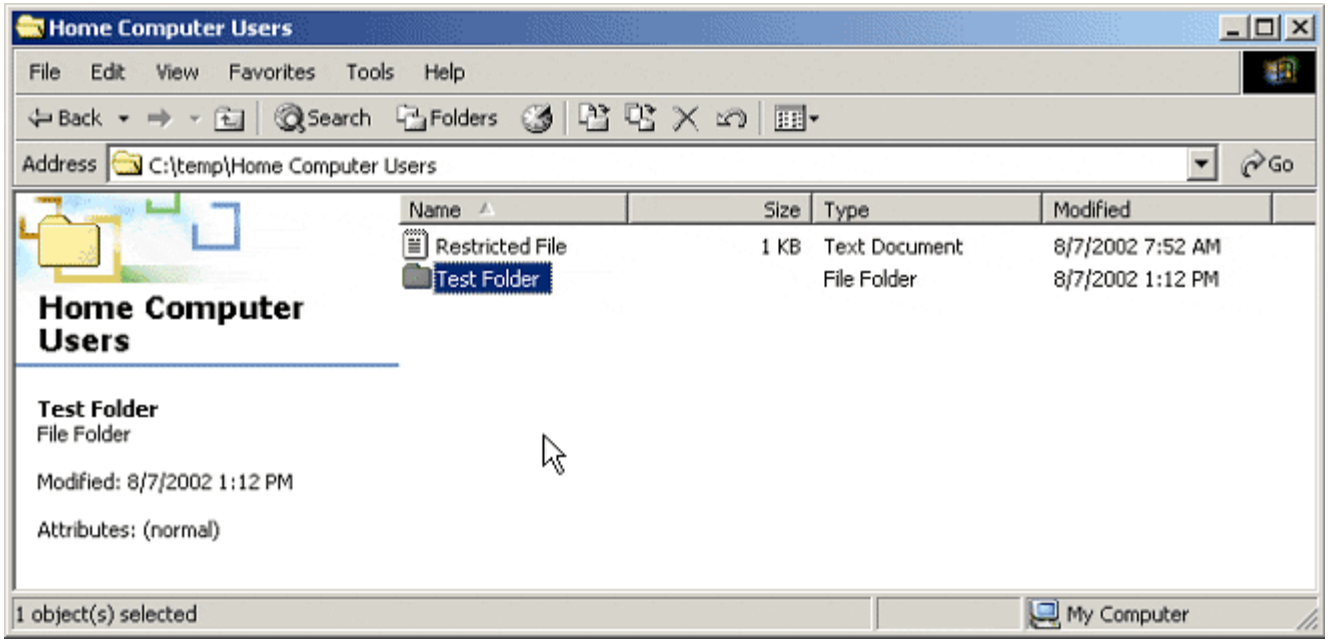
Notice that we've checked the **Reset permissions in all child objects and enable propagation of inheritable permissions** box. We'll then click **OK** and we'll be greeted with another new window. We'll click **Yes** here too and then we'll be done.



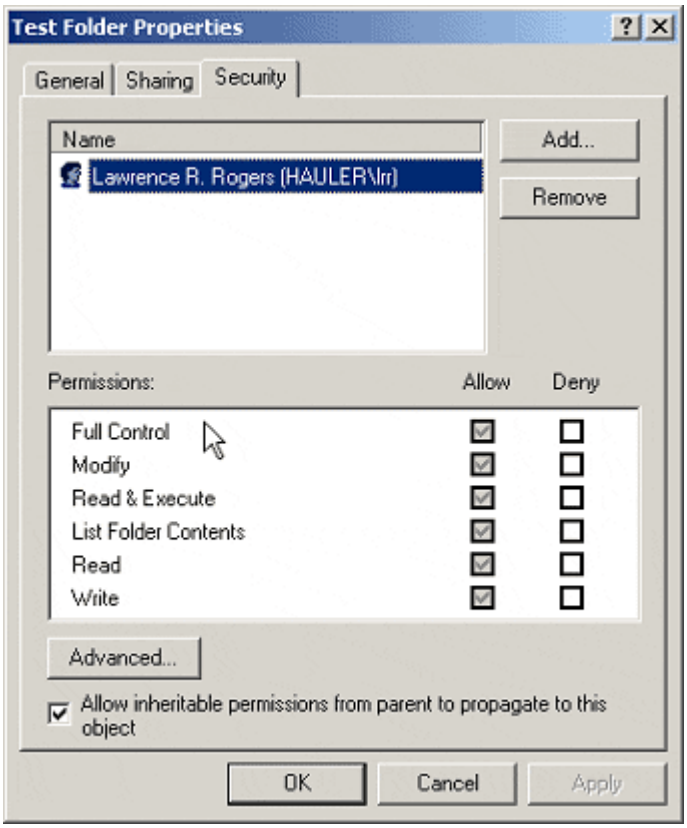
The `Home Computer Users` folder is now set up so that **lrr** has **Full Control** and no one else has any permission. Further, all files and folders that will be created later in that folder will have the same

permissions. We'll test this next.

To verify that we've done what we think we've done, let's create a new folder in `Home Computer Users` using Windows Explorer. We'll name it `Test Folder`. Once created, we'll check its permissions by right clicking it, selecting **Properties**, and then the **Security** tab.



When we do all that, we get the **Test Folder Properties** window shown here. This window verifies that we've set up the folder permissions as we wanted them and that they are, in fact, propagated to folders and files created in that folder.



If your home computer supports ACLs, Windows NT, Windows 2000, or Windows XP for example, then you can guard files and folders by adjusting those ACLs to satisfy the needs of the users who need access to them. Use the watchful tests described in Task 9 - *Install and Use a File Encryption Program and Access Controls* to set those ACLs as needed.

[top]

Services Agency (GSA), or any agency of the U.S. Government. Inclusion of a product name does not imply that the produ
is the best or only product suitable for the specified purpose.