Windows 2000 / IIS 5.0 Hardening Guide

Overview

This document is applicable ONLY to Windows 2000 running IIS 5.0. If any other application is running on the server to support its function (e.g., Cold Fusion), then that application must also be secured. The steps in this guide should be performed on new installations only to avoid unpredictable results. This hardening procedure should NOT be used on general-purpose NT servers on an internal LAN (e.g., file servers), as it removes several of the services that NT uses for default functionality.

NOTE: You should do all of this with your PC unplugged from the network. Create a CD with the needed files.

Instructions

Follow these steps chronologically. You may print this procedure and check off each of the steps as they are completed. Unless otherwise noted, all steps are a requirement for running on the DMZ. These steps are not a guide but the requirements for DMZ deployment. Any deviation from this process should be approved by your InfoSec Department.

Initial Configuration

Step 1 – Boot up Windows 2000 CD-ROM to begin installation and configuration.

1.1 The Welcome to Setup screen appears. Press Enter to continue.

1.2 Click F8 to accept End User License Agreement (EULA).

Note: Install only one instance of the operating system. If you need to get on to a server using another instance, install on need, and delete afterwards. If there are any previous versions of operating systems, remove by deleting partitions then repartition.

Step 2 – Partitioning the OS

2.1 – Choose your OS partition for installation then choose NTFS for format. Reserve a separate minimum 6.5 GB partition for the OS (more is better).

Step 3 – Choose your regional settings as appropriate

3.1 Type in name and organization.

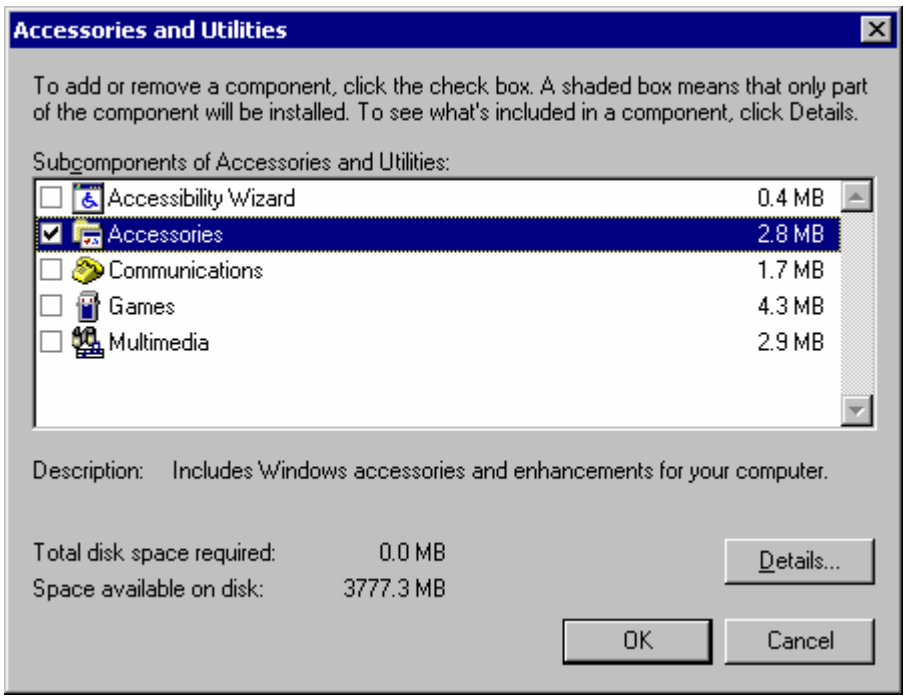
3.2 Choose Per Seat License.

Step 4 – Choose a name for the server and set a strong administrator password

4.1 – You should follow your corporate naming standards and select a strong password per the company guidelines.

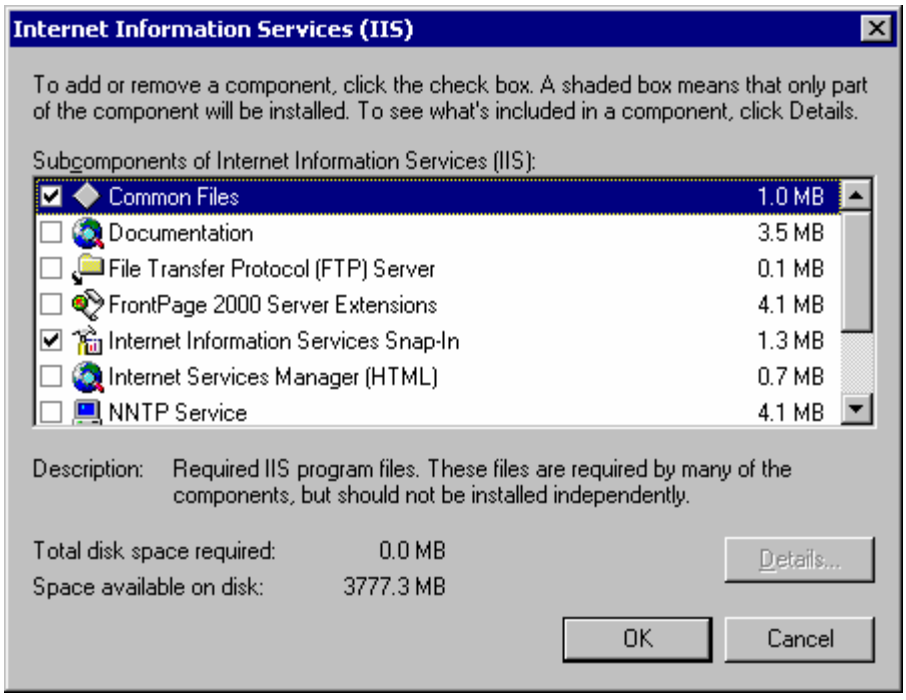
Step 5 – Choose Components

5.1 – Go into **Details** on **Accessories**; uncheck **Accessibility Wizard**, uncheck **Communications**, uncheck **Games** and uncheck **Multimedia** (uncheck all and leave Accessories checked). Then Click **OK**



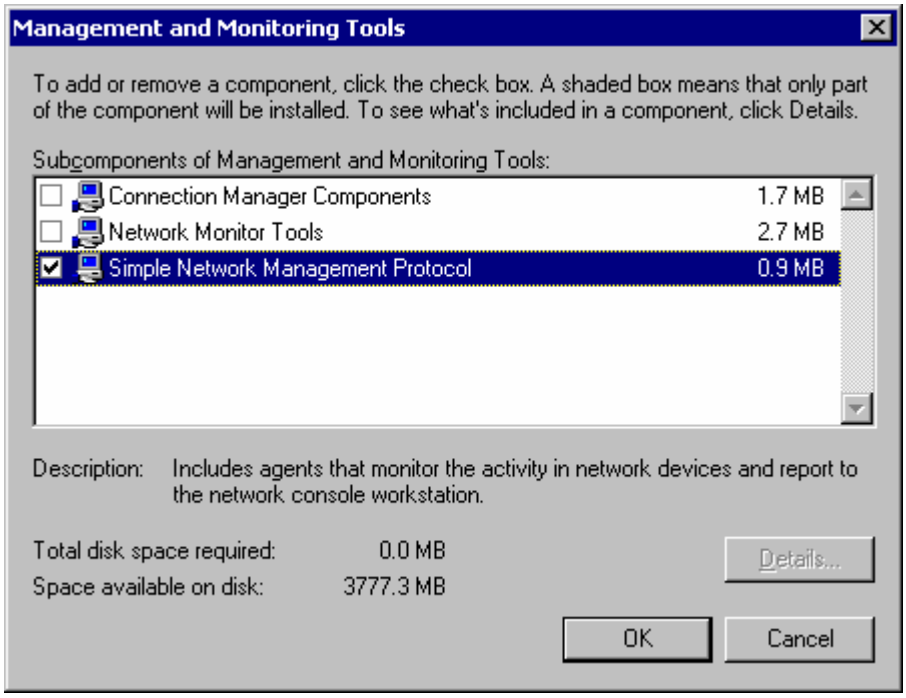
5.2 – Back at the Components menu, uncheck **Indexing services**.

5.3 – Go to **Details** on **Internet Information Services (IIS)**, uncheck all then check only **Common Files**, **Internet Information Services Snap-In** and **World Wide Web Server** then click **OK**.

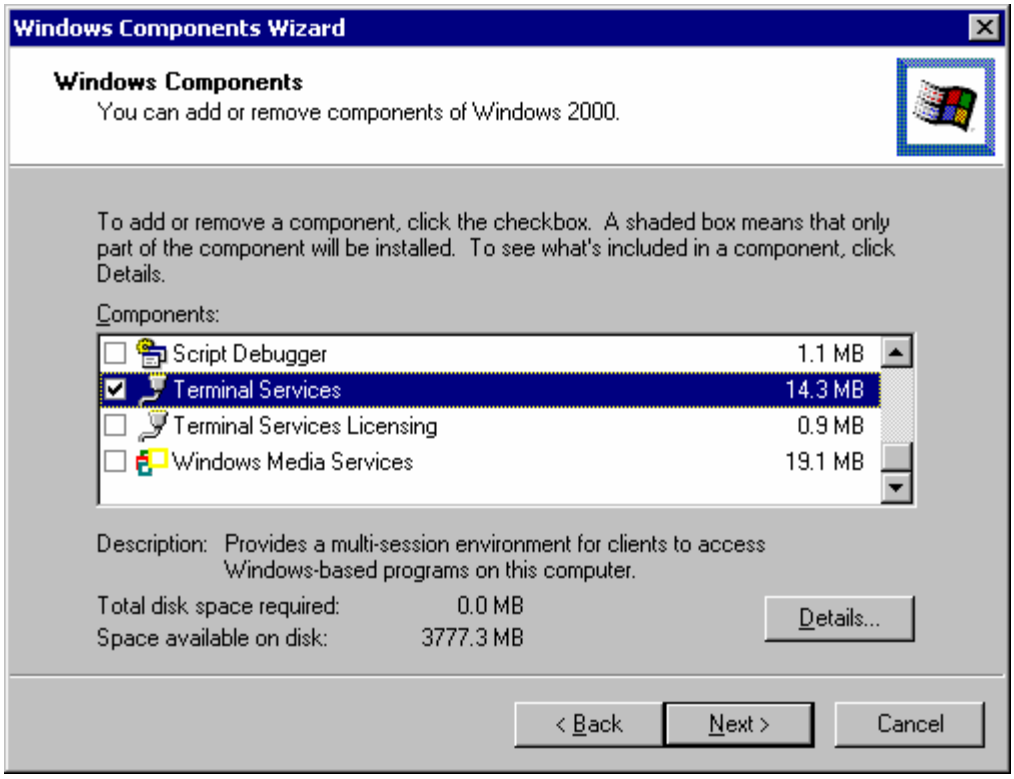


5.4 – Uncheck **Script Debugger**.

5.5 – Go to **Details** on **Management and Monitoring Tools**, check **Simple Network Management Protocol (SNMP)** if SNMP is to be used.



5.6 – Check **Terminal Services**.



5.7 – After your finished you will have only **Accessories and Utilities**, **Internet Information Services (IIS)** and **Terminal Services** checked.

5.8 – Click Next.

Step 6 – Set Date, Time and Time Zone then click Next

Step 7 – Setting up Terminal Services

7.1 – Select **Remote Administration Mode** for terminal services then click **Next**

7.2 – Choose **Typical Network Settings**

Step 8 – Workgroup or Computer Domain setup:

8.1 – Choose "**No, This Computer Is Not On a Network, or Is On a Network Without a Domain**."

8.2 – Type in a random workgroup name (Alt-255 for a blank workgroup).

Note: The file copy starts (This may take some time). Log back in after reboot.

Step 9 – When the Windows Configure Your Server screen appears:

9.1 – Choose **I Will Configure This Server Later**.

9.2 – Click **Next**, then uncheck **Show This Screen at Startup**. Close window

Step 10 – Install the latest Service Packs and Patches

As of 10/15/2004: (You should consider downloading all of these files and burning them to a CD-ROM.)

10.1 – Install SP4 for Windows 2000

10.2 – Install Internet Explorer 6.0 SP1

10.3 – Install the latest critical patches

MS04-038 (834707)	October 12, 2004 - Cumulative Security Update for Internet Explorer
MS04-037 (841356)	October 12, 2004 - Vulnerability in Windows Shell Could Allow Remote Code Execution
MS04-032 (840987)	October 12, 2004 - Security Update for Microsoft Windows
MS04-024 (839645)	August 10, 2004 – Vulnerability in Windows Shell Could Allow Remote Code Execution
MS04-023 (840315)	July 13, 2004 – Vulnerability in HTML Help Could Allow Code Execution
MS04-022 (841873)	July 19, 2004 – Vulnerability in Task Scheduler Could Allow Code Execution
MS04-020 (841872)	August 10, 2004 - Vulnerability in POSIX Could Allow Code Execution

MS04-019 (842526)	July 13, 2004 - Vulnerability in Utility Manager Could Allow Code Execution
MS04-004 (832894)	April 12, 2004 – Cumulative Security Update for Internet Explorer.
MS04-014 (837001)	May11, 2004 – Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution.
MS04-012 (828741)	April 21, 2004 – Cumulative Update for Microsoft RPC/DCOM.
MS04-011 (835732)	May 4, 2004 – Security Update for Microsoft Windows.
MS04-003 (832483)	April 1, 2004 – Buffer Overrun in MDAC Function Could Allow Code Execution
MS03-043 (828035)	December 2, 2003 – Buffer Overrun in Messenger Service Could Allow Code Execution
MS03-044 (825119)	October 22, 2003 – Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise
MS03-042 (826232)	October 29, 2003 – Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution
MS03-034 (824105)	April 13, 2004 – Flaw in NetBIOS Could Lead to Information Disclosure
MS03-041 (823182)	November 17, 2003 – Vulnerability in Authenticode Verification Could Allow Remote Code Execution
MS03-023 (823559)	May 13, 2004 – Buffer Overrun In HTML Converter Could Allow Code Execution
MS02-050 (Q329115)	November 11, 2003 - Certificate Validation Flaw Could Enable Identity Spoofing

You may now plug the server into the network.

Step 11 – Installing SSH Server for Remote Management

For remote access we will use SSH as the only transport.

11.1 – Install the SSH Server and Client Software

We use and recommend the Tectia SSH Server and Client from http://www.ssh.com. The screenshots below illustrate the installation of these components.

11.2 – After installing the server application, open the SSH Secure Shell Server Configuration window:

Go to **Start** > **Programs** > **SSH Secure Shell Server** > **Configuration**

This will bring up a window that looks like the following:

Under the **General** Tab**:**

Increase the "**Maximum Number of Connections**" value to **2**

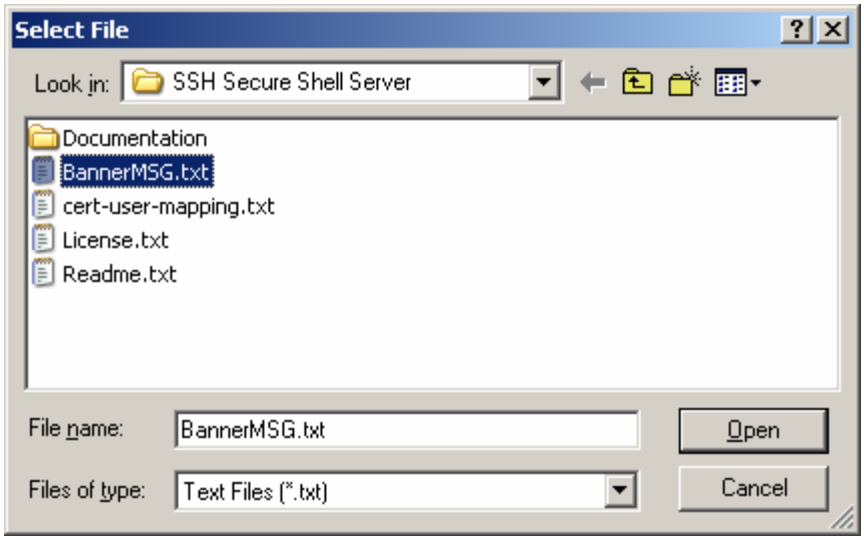
11.3 – Create a new text file called **BannerMSG.txt** and place it in:

C:\Program Files\SSH Communications Security\SSH Secure Shell Server directory

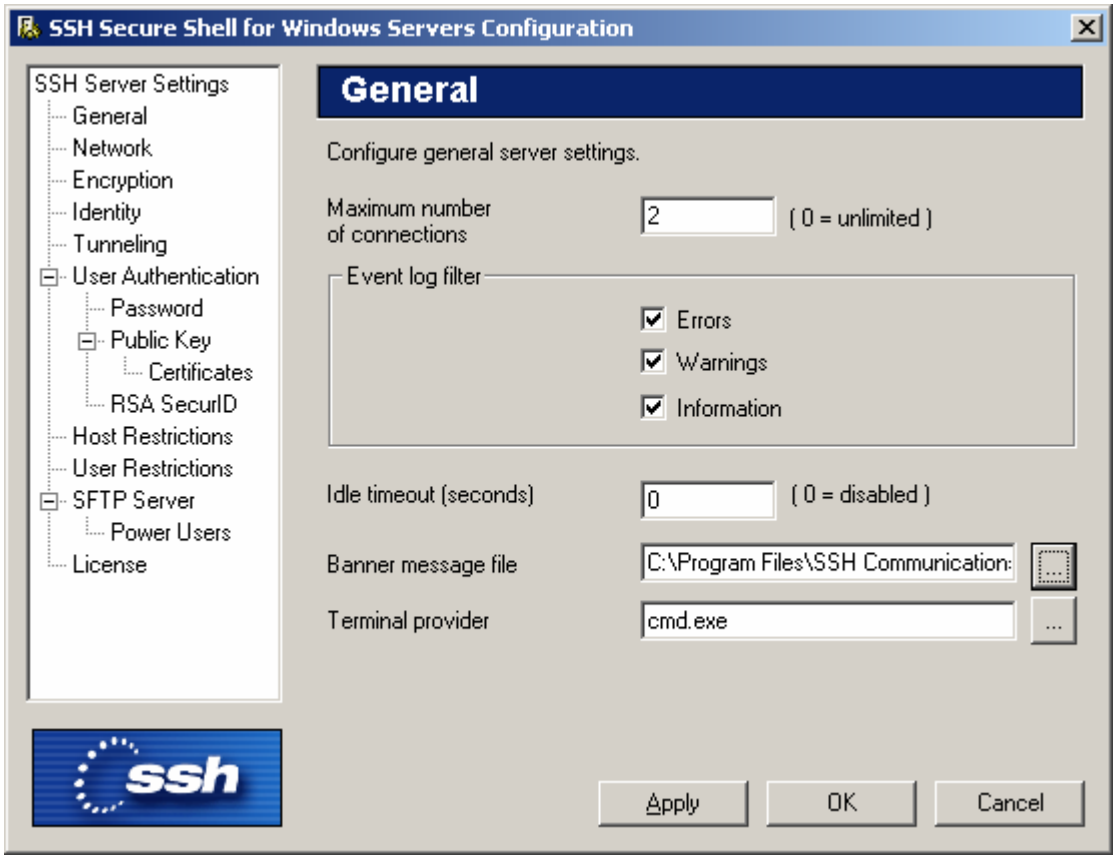
The file should contain the following verbiage:

```
WARNING!!!
READ THIS BEFORE ATTEMPTING TO LOGON
This System is for the use of authorized users only. Individuals using this computer
without authority, or in excess of their authority, are subject to having all of their
activities on this system monitored and recorded by system personnel. In the course of
monitoring individuals improperly using this system, or in the course of system
maintenance, the activities of authorized users may also be monitored. Anyone using this
system expressly consents to such monitoring and is advised that if such monitoring
reveals possible criminal activity, system personnel may provide the evidence of such
monitoring to law enforcement officials.
```

11.4 – Link the **BannerMSG.txt** file that you just created in the "**Banner message file**" box by clicking on the box with the three dots on the right of the white space and finding the file in the above named directory.



The resulting screen should look like this:



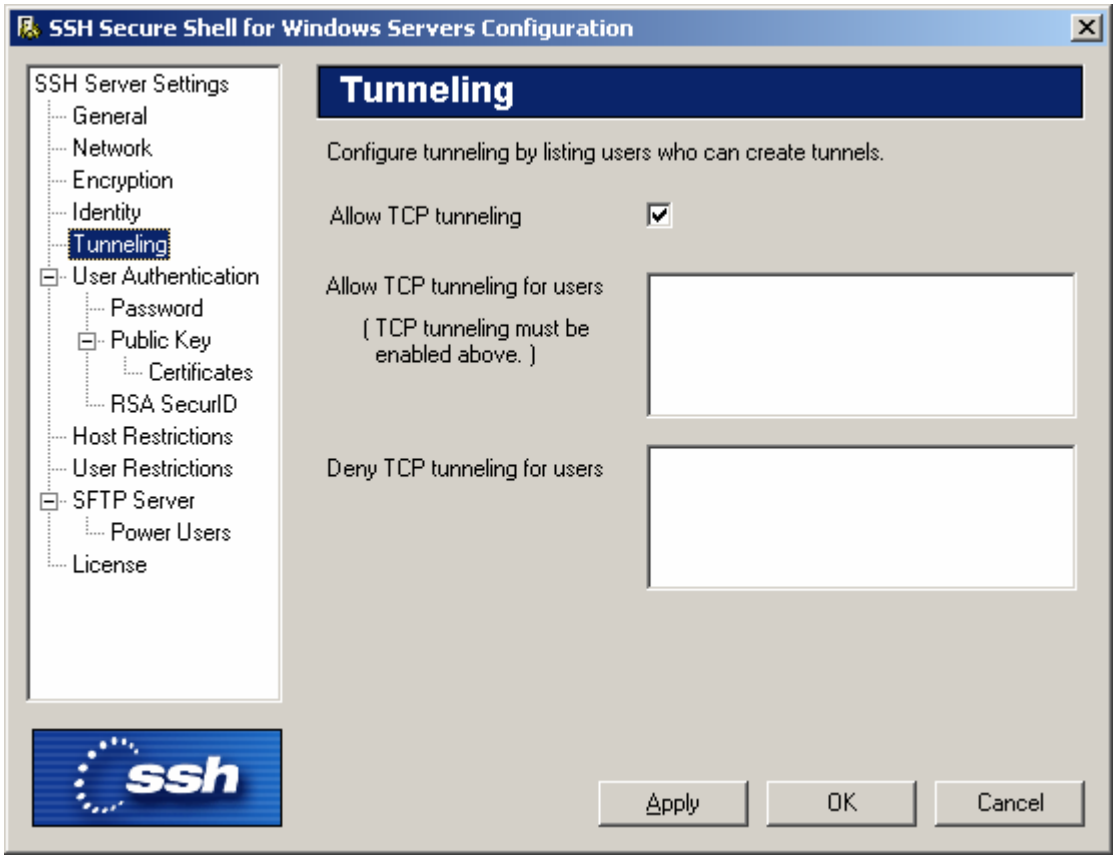
11.5 - Under the **Encryption** Tab**:**

Ensure that the following settings are selected:

Ciphers: AnyStdCipher
MACs: AnyStdMac

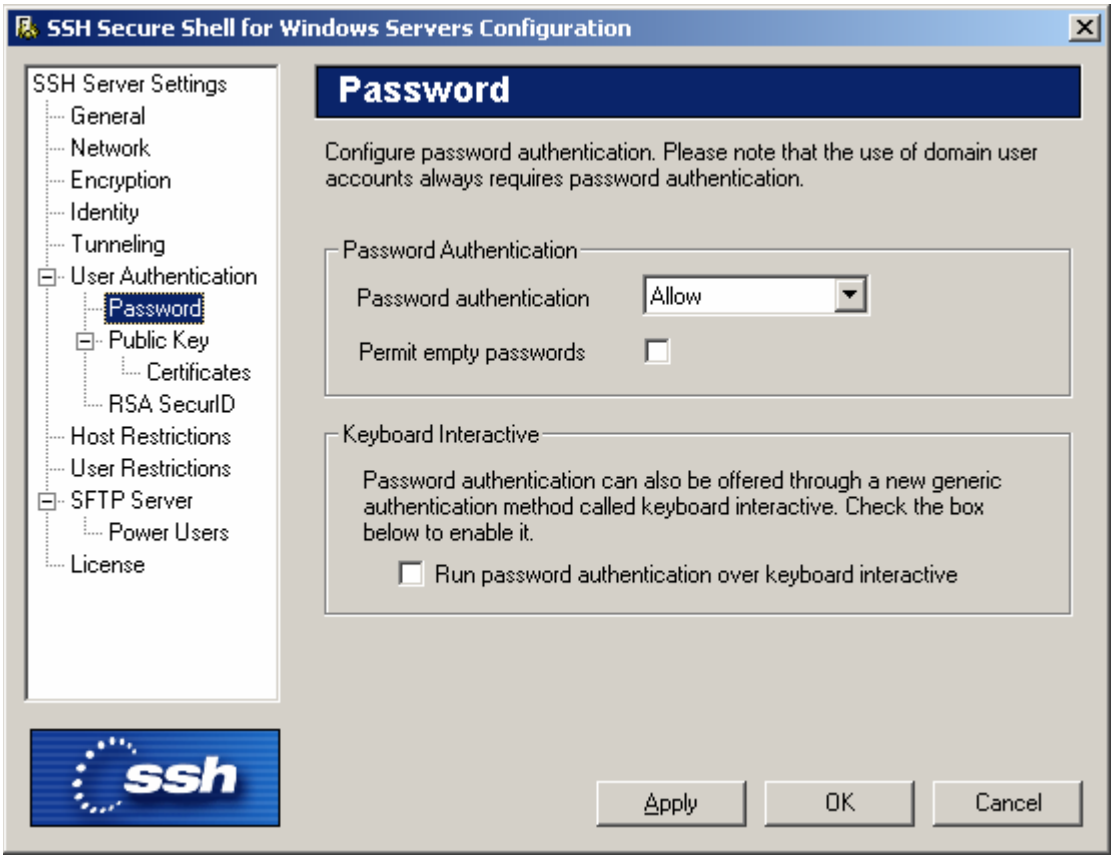
11.6 - Under the **Tunneling** Tab**:**

Place a check mark in the box next to **Allow TCP Tunneling**.



11.7 – Under the User Authentication > Password **Tab**

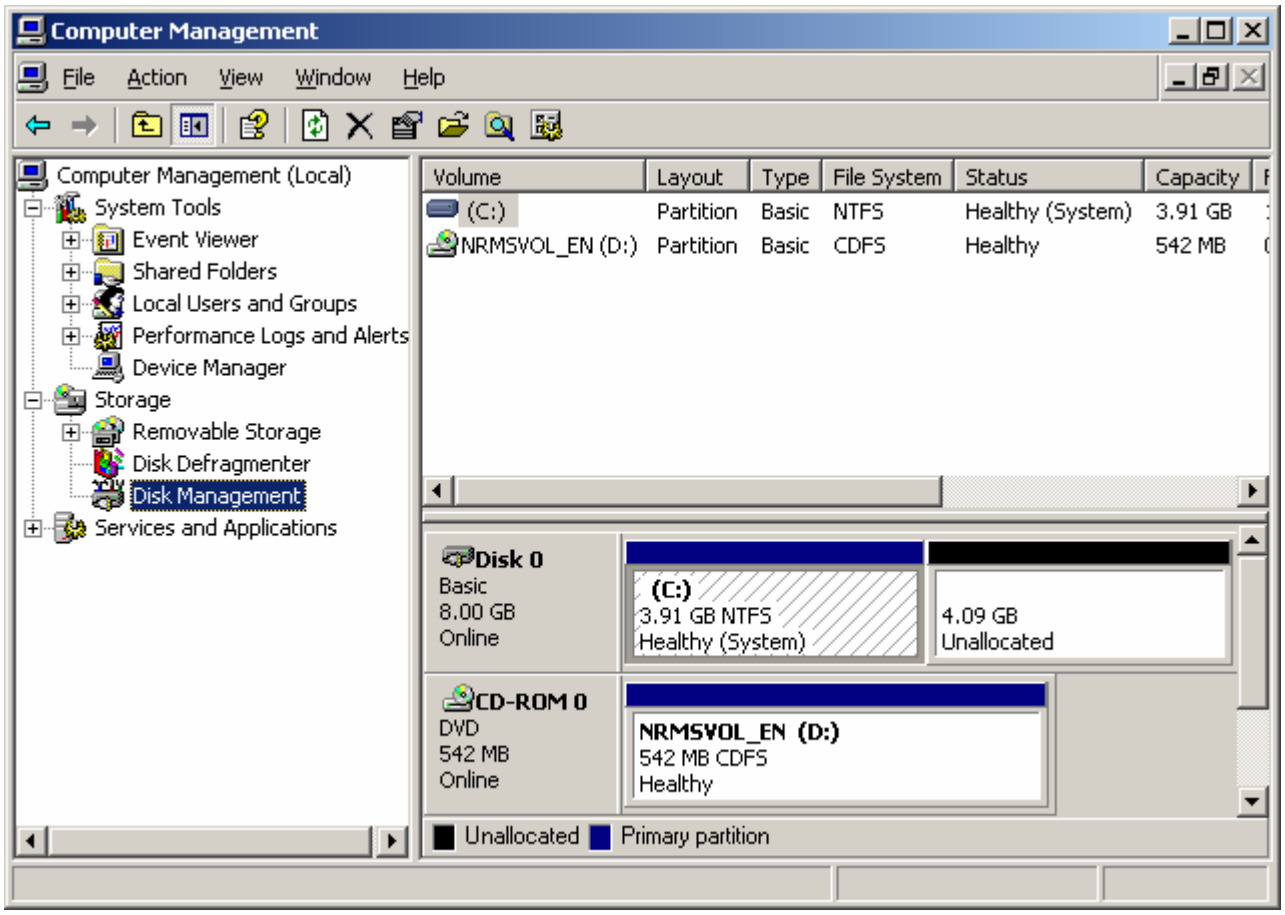
Ensure that the "**Permit empty Passwords**" box is **NOT** checked.



Click **Apply** to make the changes permanent. Click **OK** to exit.

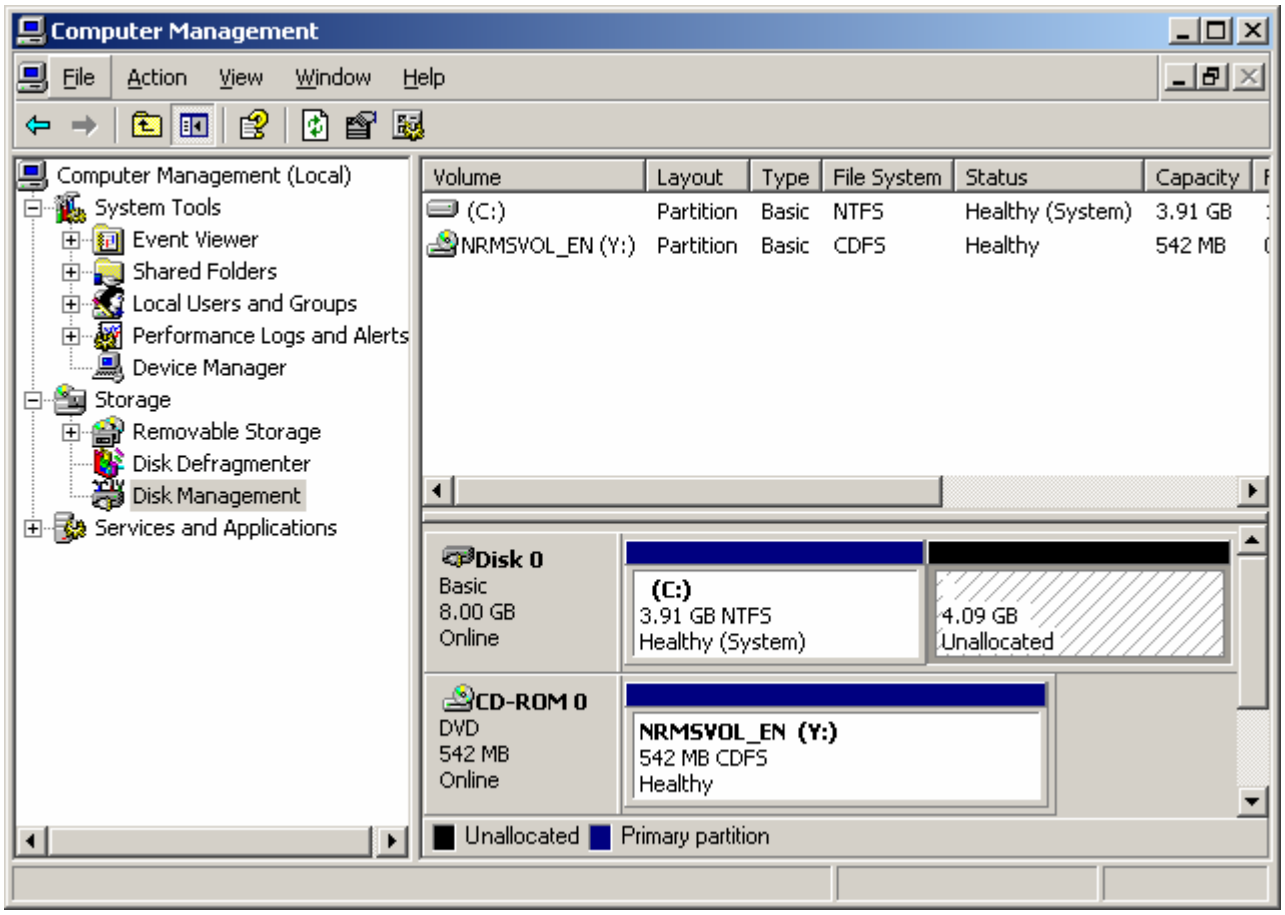
Step 12 – Media Configuration

12.1 – Go to **Start > Programs > Administrative Tools > Computer Management > Disk Management**

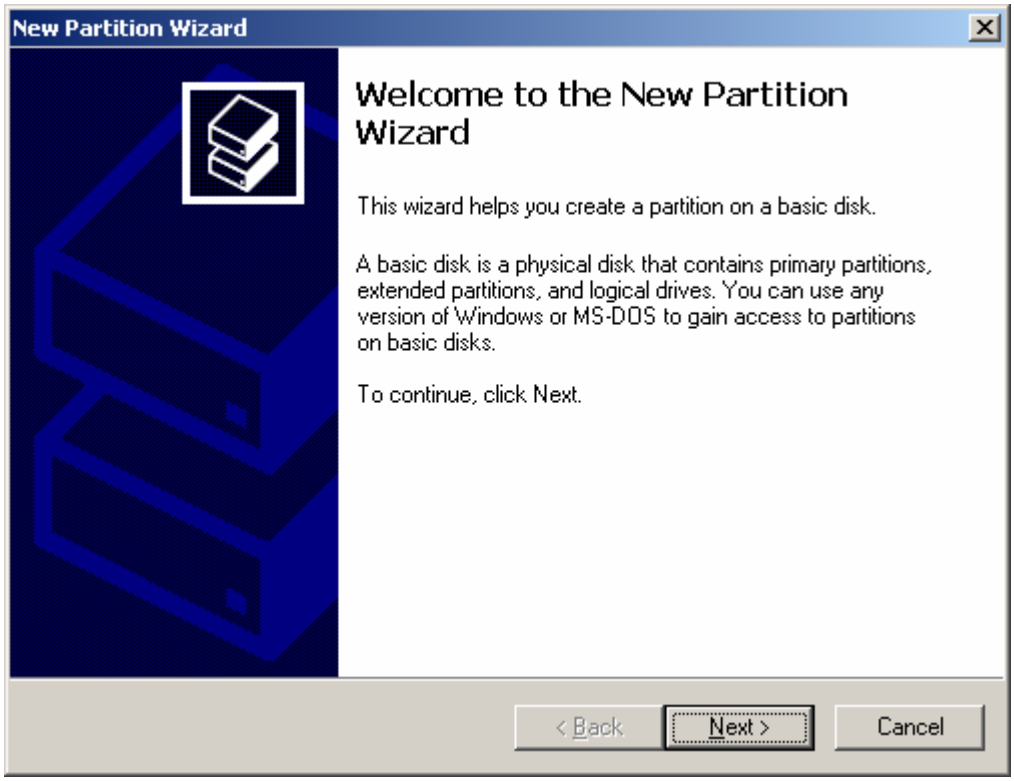


12.2 – Format unallocated disk space.

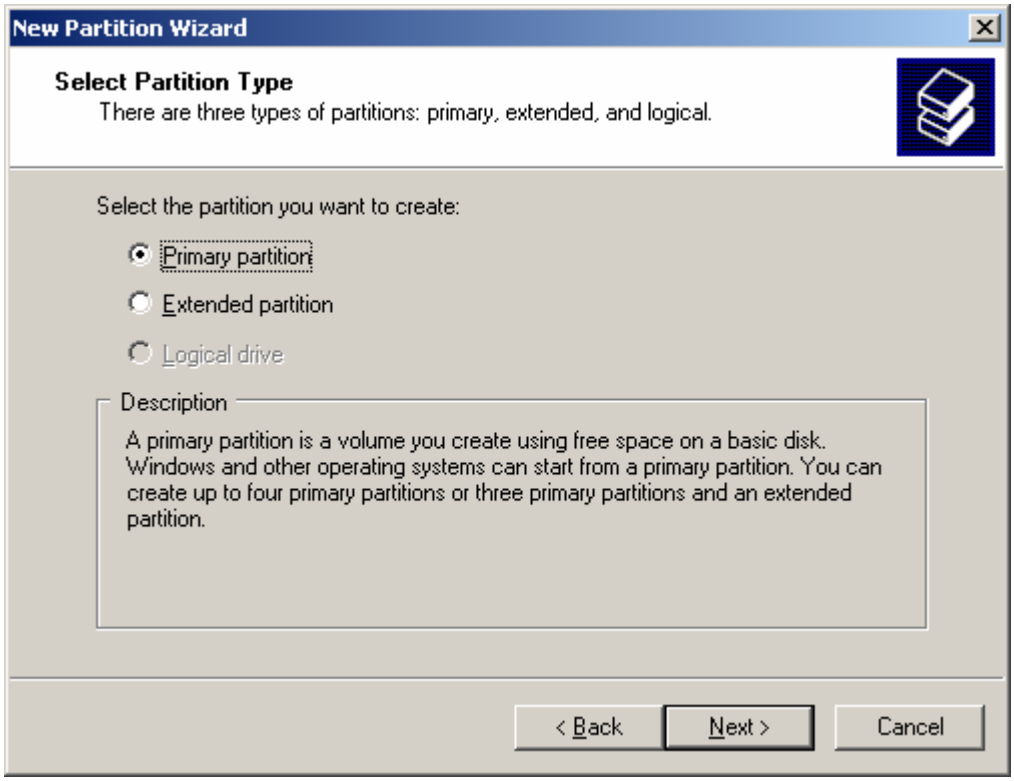
In the bottom right panel, Right Click on the section labeled **Unallocated** (shaded in the picture below) on Disk 0 and choose **New Partition**.



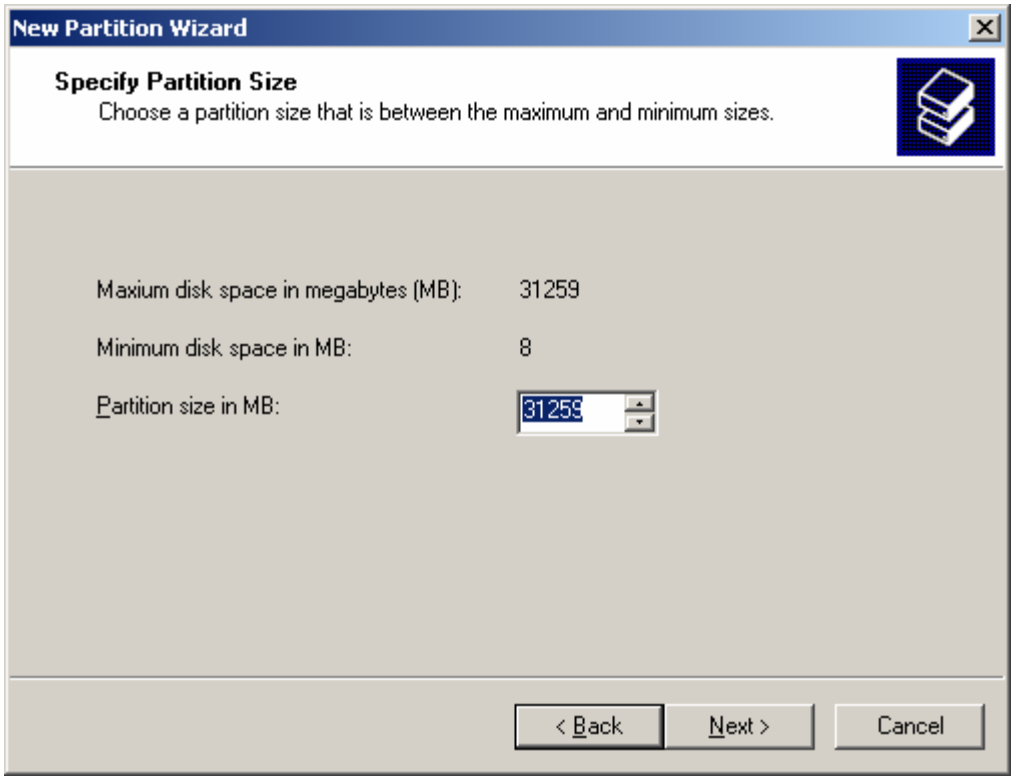
This will bring up the New Partition Wizard



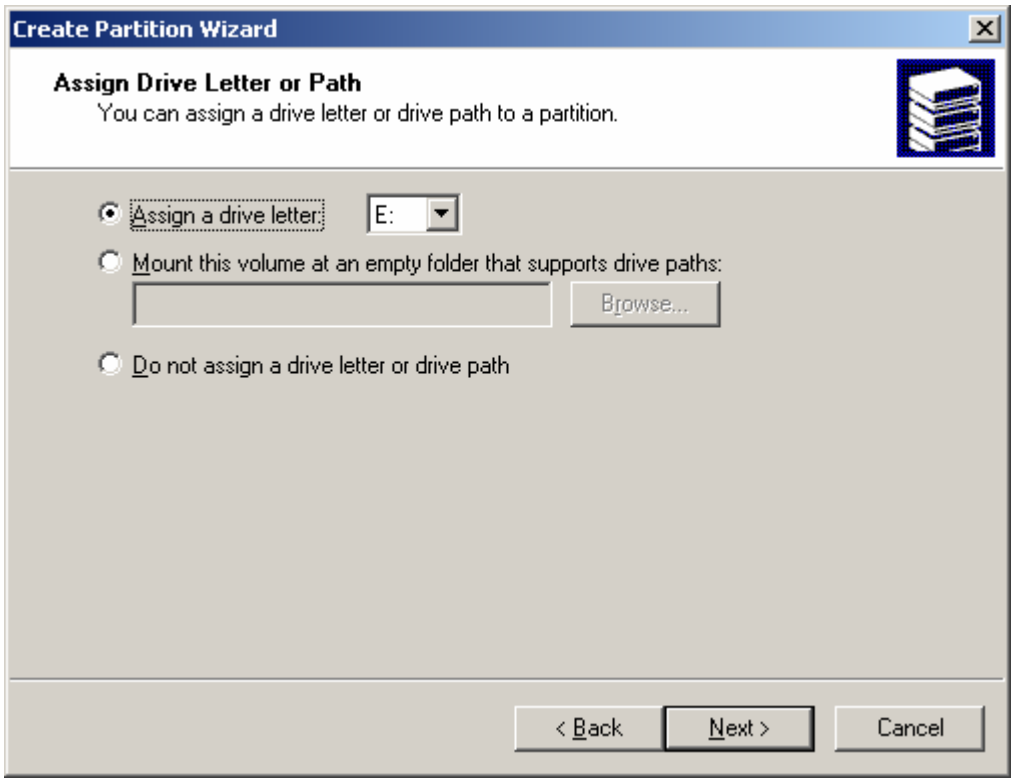
12.3 – Click **Next** to continue



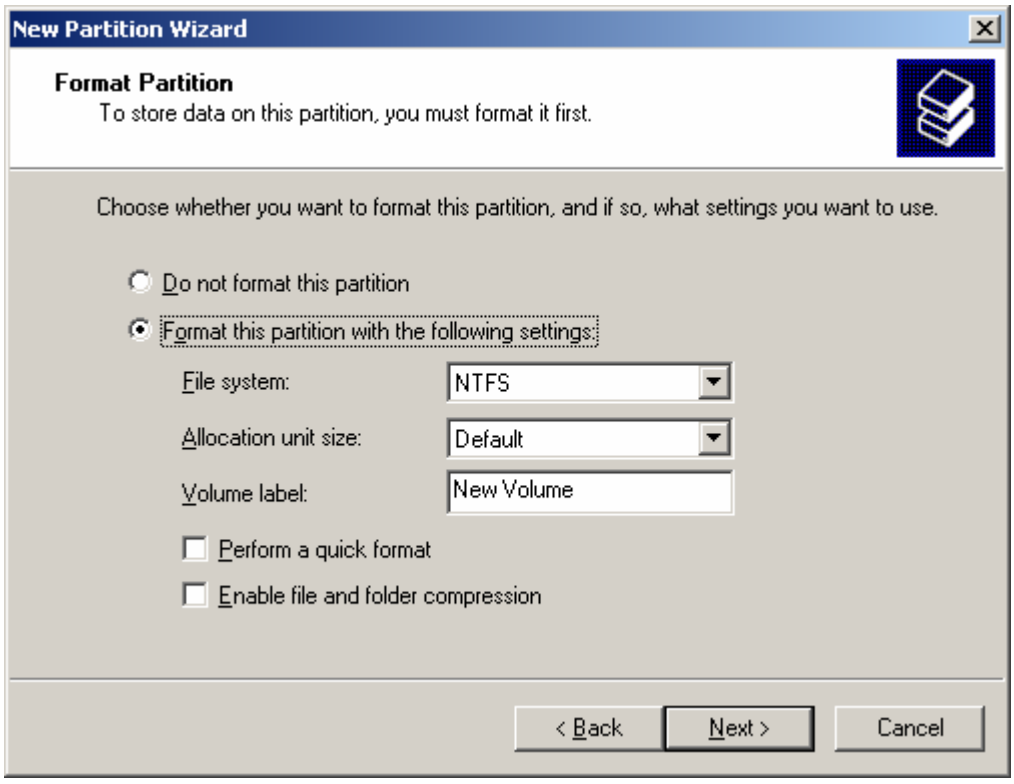
12.4 – Ensure that **Primary partition** is selected and click **Next** to continue.



12.5 – Select the size of your partition in MB and click **Next** to continue.

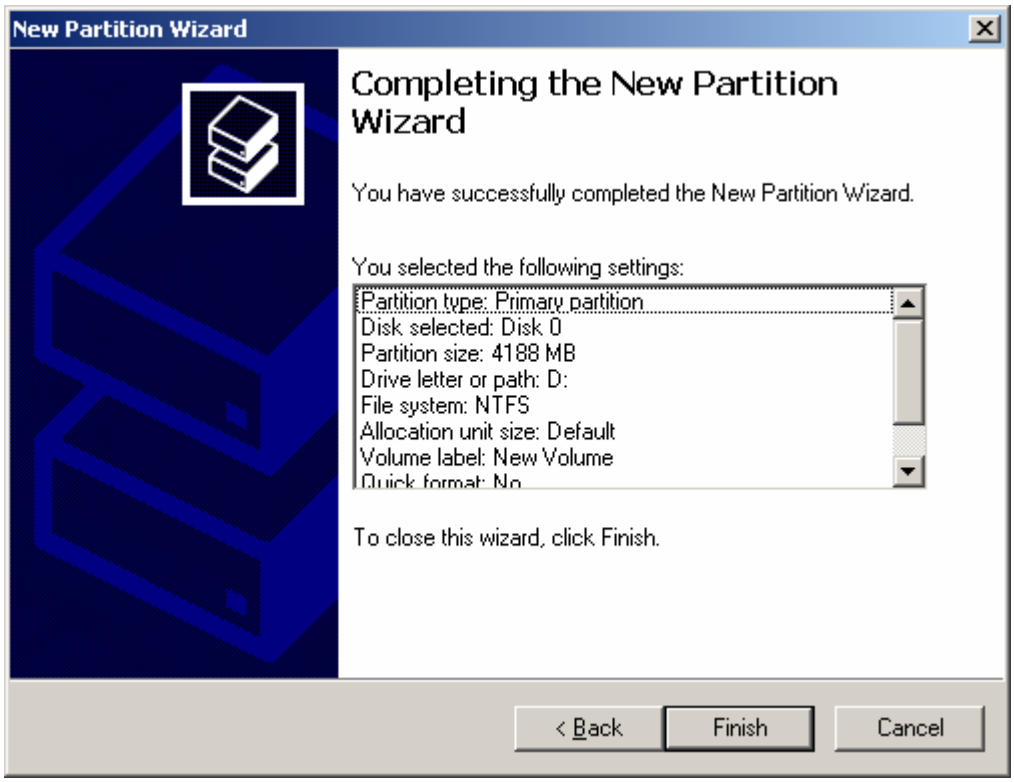


12.6 – Assign it the appropriate drive letter, **E:** and click **Next** to continue.



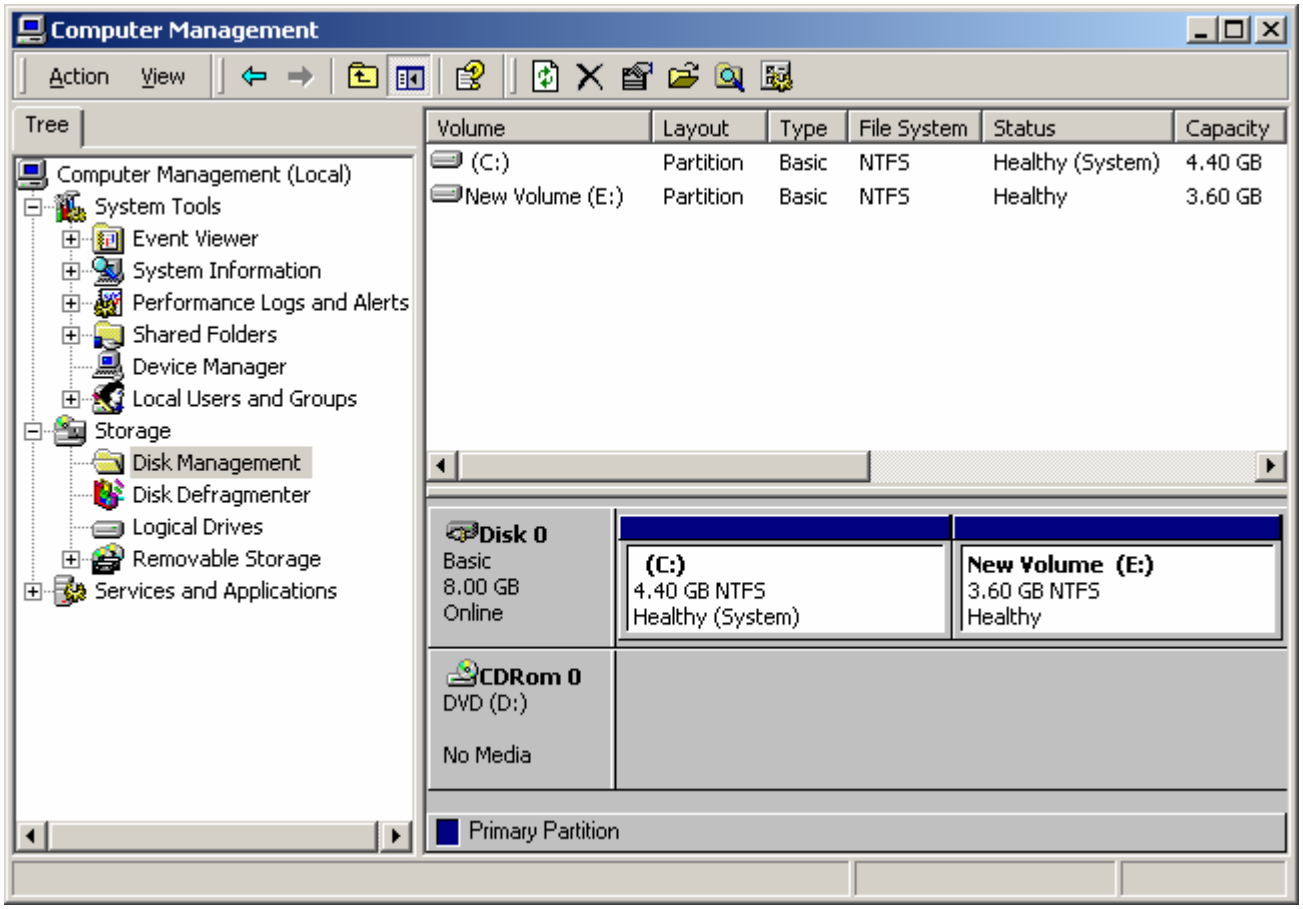
12.7 – Ensure that **Format this partition with the following settings** is selected and the values for **File System** is **NTFS** and the **Allocation unit size** is **default**. You may change the **Volume Label** if you desire.

Click **Next** to continue.



12.8 – After reviewing your selected settings, click **Finish** to begin the format.

Upon completion, your disk manager should show 2 partitions on Disk 0 as pictured below.



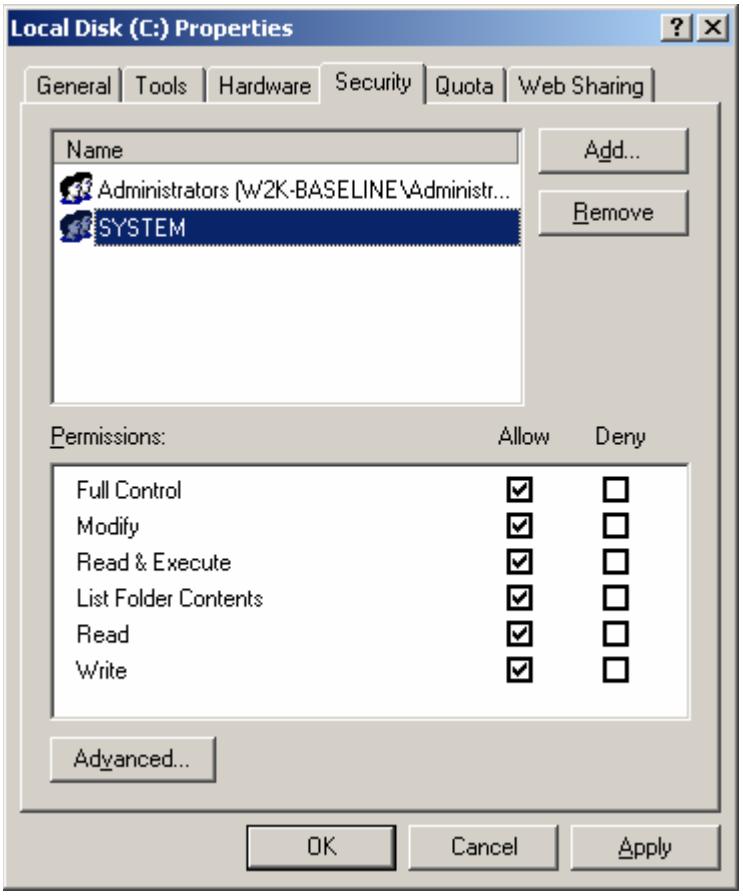
When the formatting is complete, you can close the **Computer Management** window.

12.9 – Double click on the My Computer icon, Right click on the **C:** drive and select **Properties**

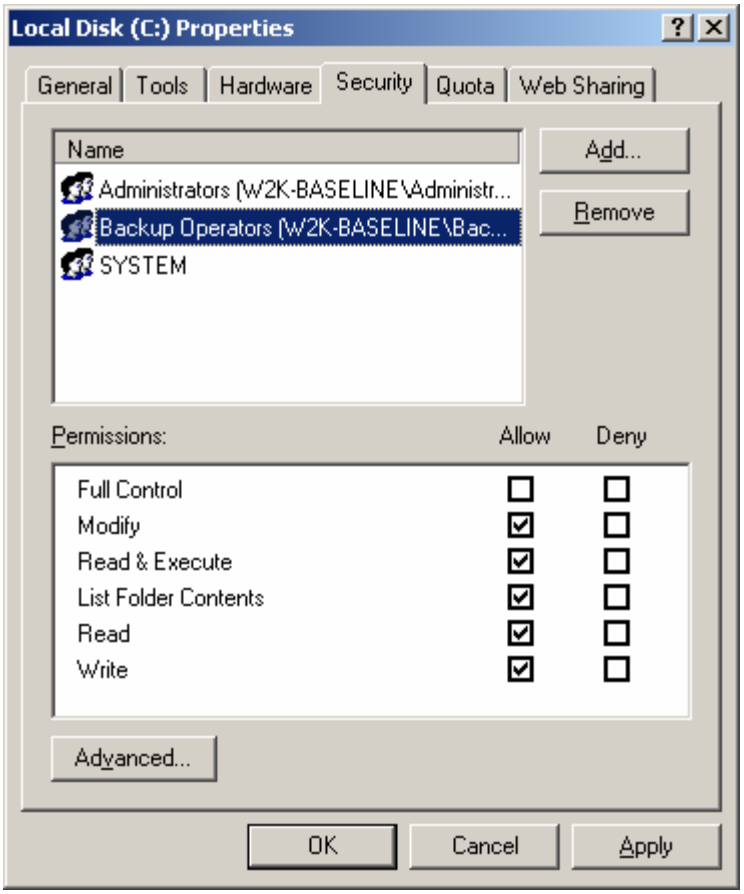
Click on the **Security** Tab

12.10 – Remove the **Everyone** Group

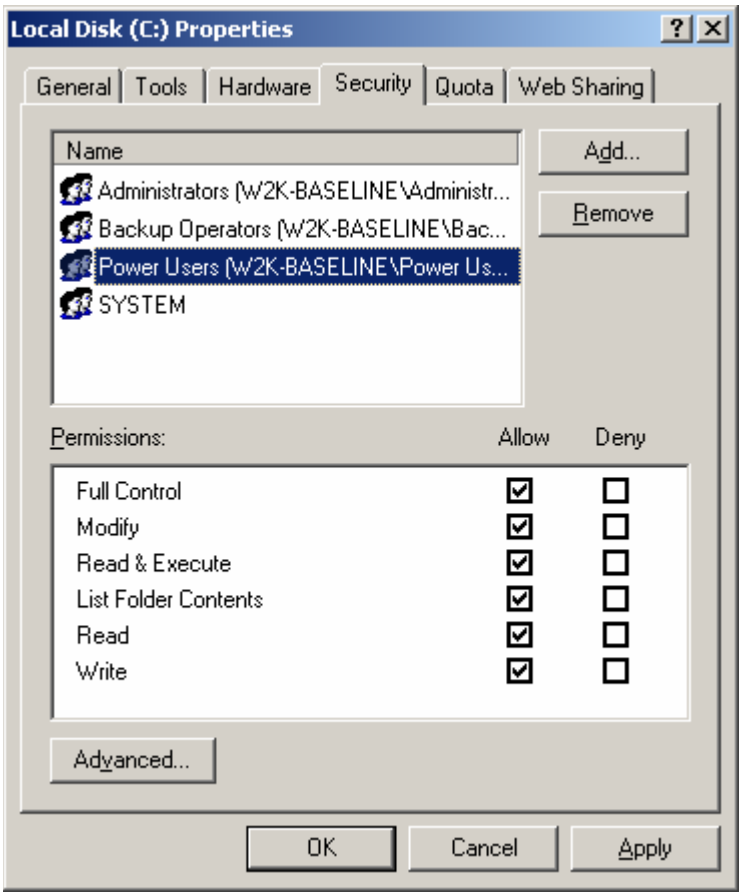
12.11 – Click on **Add** and add the **Administrators** Group and the **SYSTEM** Group giving them permissions for **Full Control**.



12.12 – Add the **Backup Operators** Group and give them permissions for **Modify**.

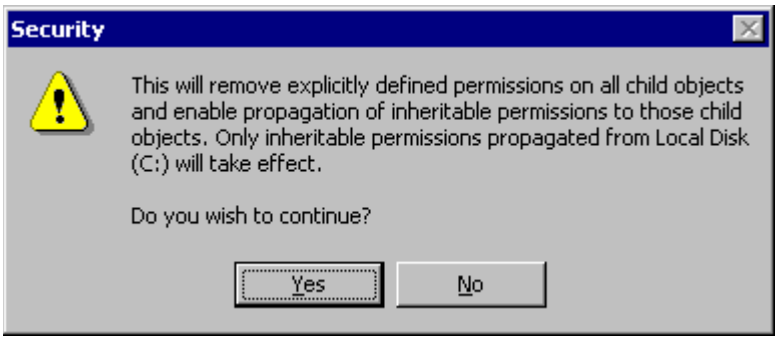


12.13 – Add the **Power Users** Group and give them permissions for **Full Control**.



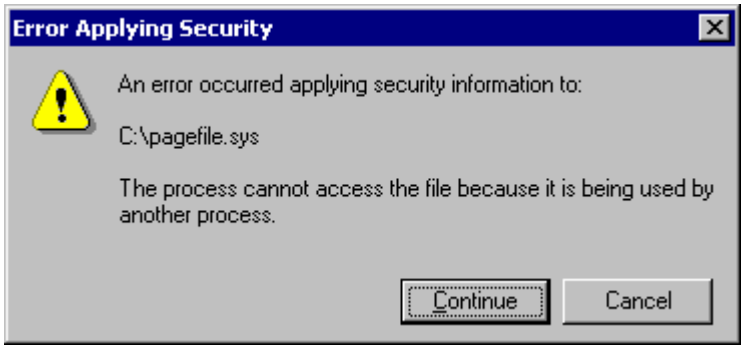
IMPORTANT!! Click **Advanced** > place a checkmark in the box labeled **Reset Permissions on all Child Objects**.

A Security screen will pop-up.



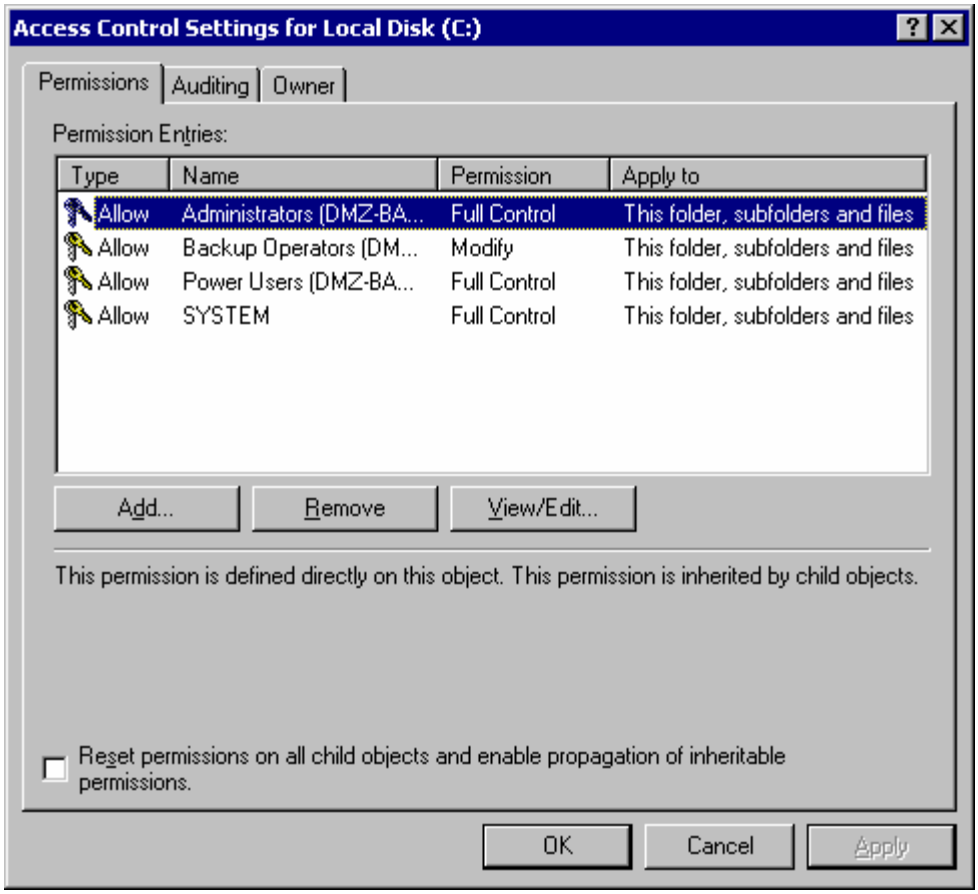
You should click **Yes** to continue.

An Error screen will pop-up.

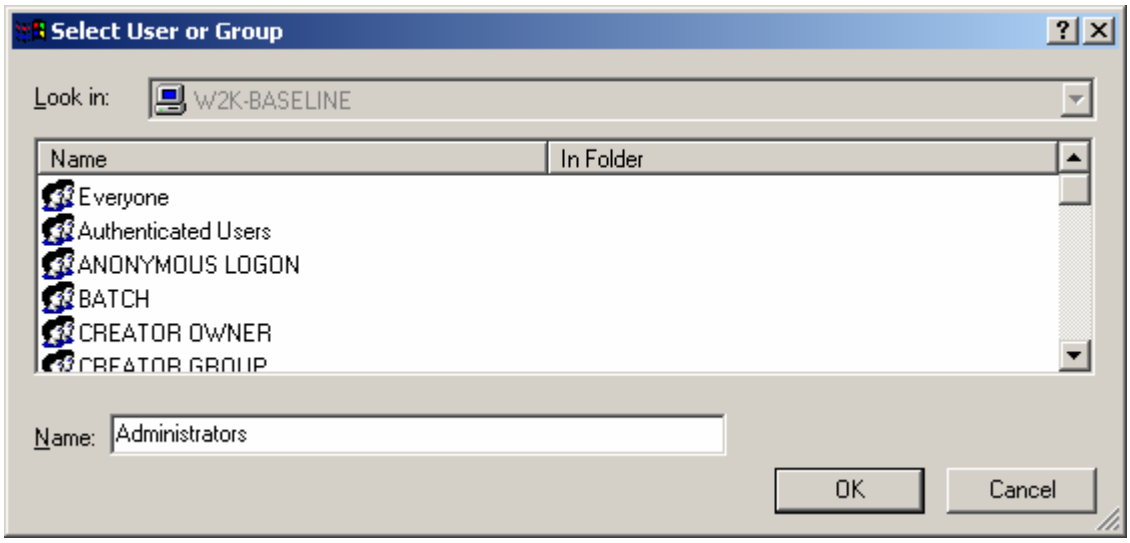


Click **Continue** (you can safely ignore the error on the Pagefile).

Your results should look like this:

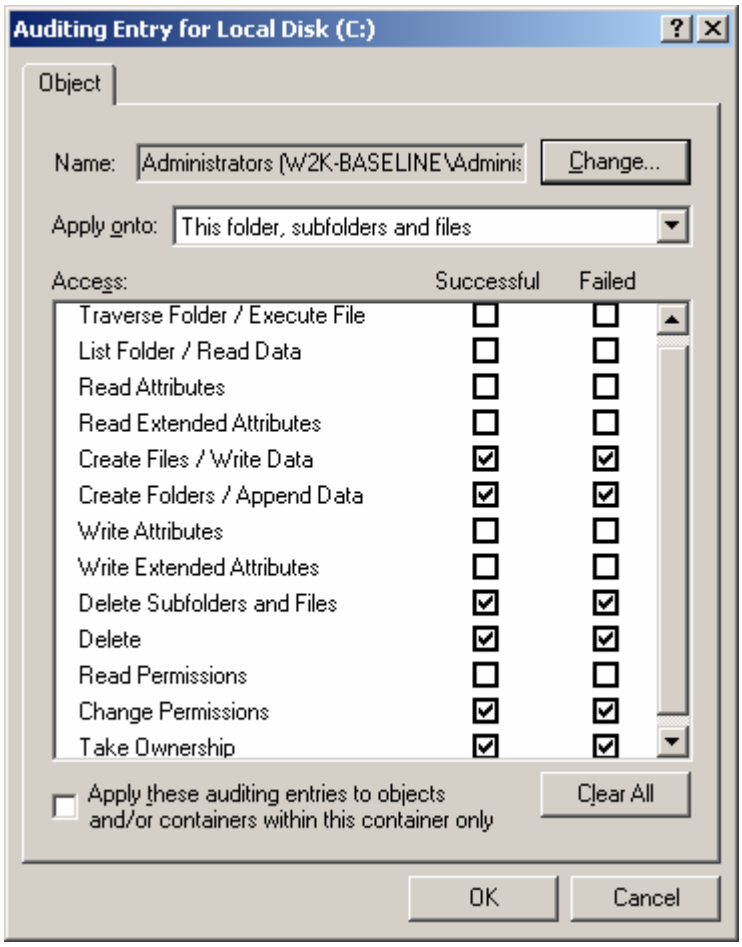


12.14 – Click the **Auditing** tab > **Add** > **Administrators** and click **OK**.

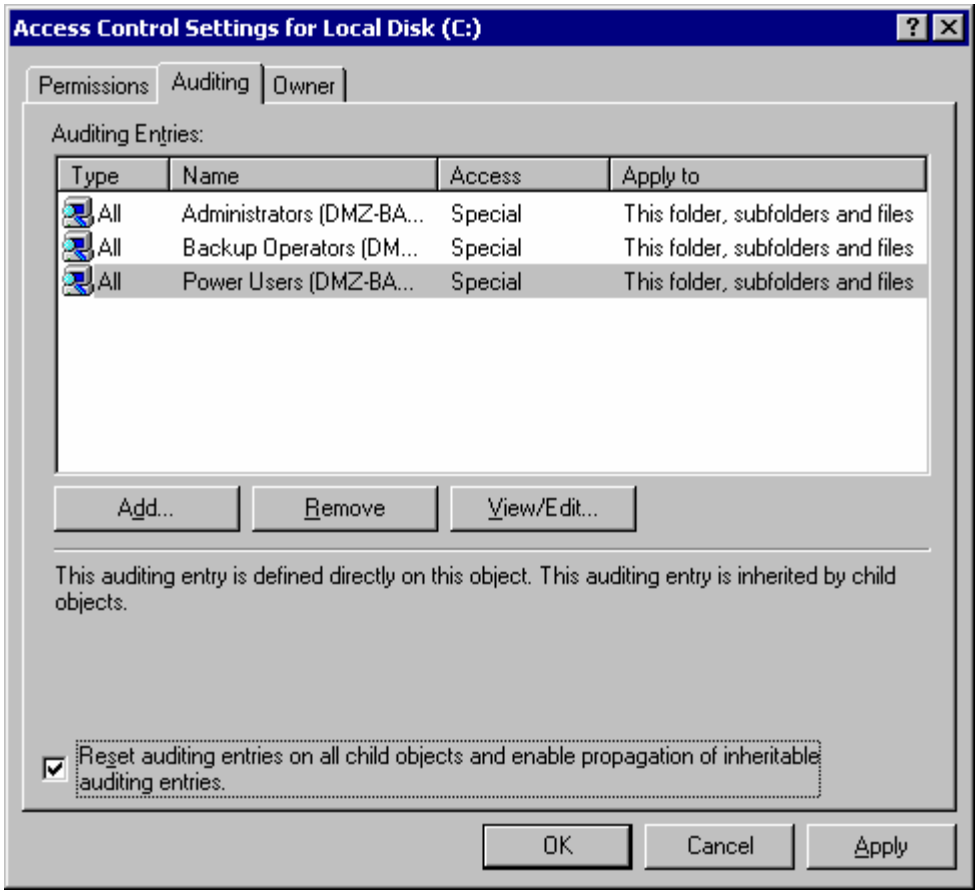


12.15 – Check the boxes for each of the following:

- Create Files/Write Data
- Create Folders/Append Data
- Delete Subfolders and files
- Delete
- Change Permissions
- Take Ownership



12.16 – Add the **Power Users** Group, the **Backup Operators** Group to be Audited with the same permissions in Step 12.15. Click Apply and then OK.

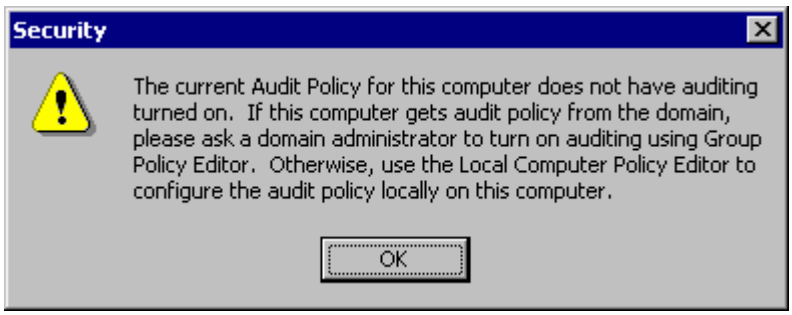


IMPORTANT!! Place a checkmark in the box labeled **Reset Auditing Entries on all child objects…**

A pop-up box like the one below will appear:

Click **Continue** (You can safely ignore the error on the Pagefile).

12.17 – You will get a message that auditing is not turned on.

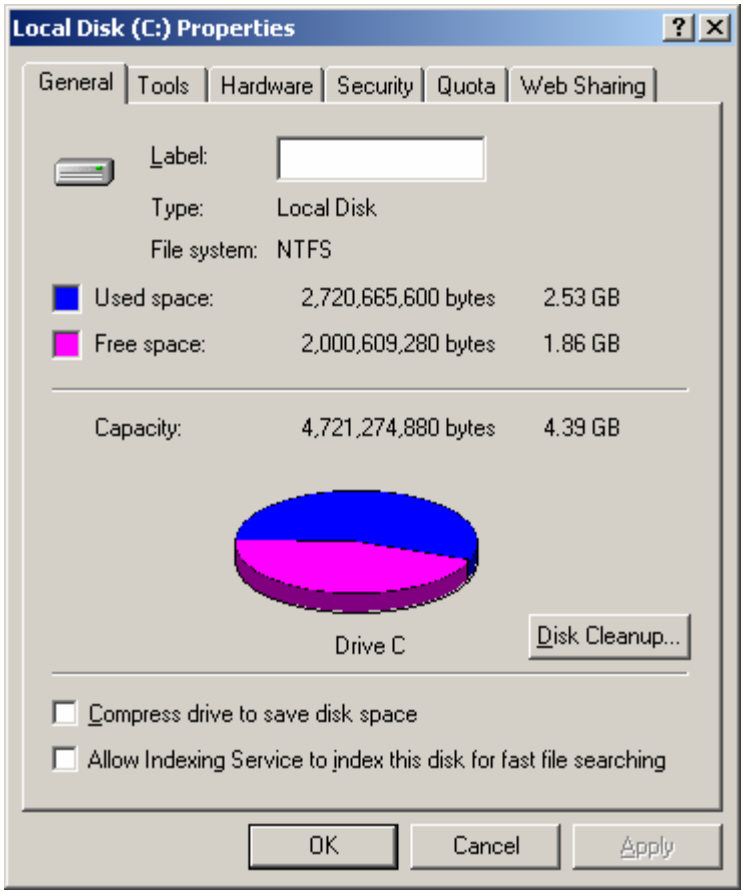


Click **OK**

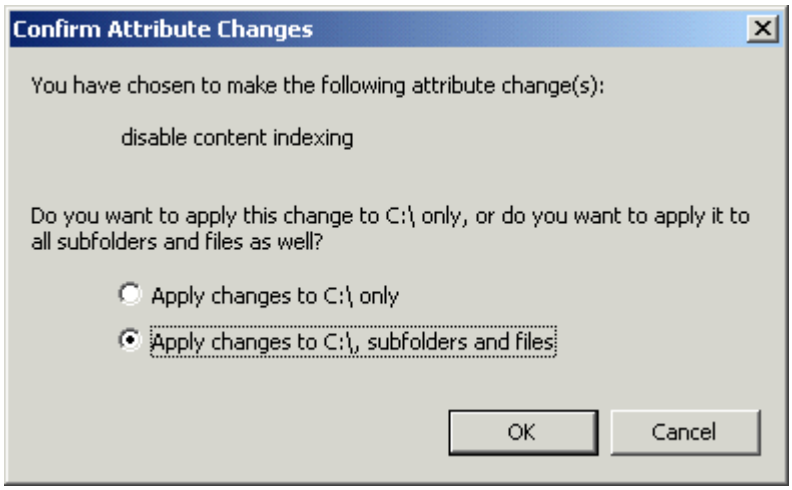
12.18 – Repeat this procedure (**Steps 12.9 – 12.17**) for all other partitions on your hard drive.

Step 13 – Turn off Indexing on all Volumes

13.1 – Under the **General** Tab, uncheck the box labeled "**Allow Indexing Service to index this disk for fast file searching**"



A box will pop up, and you should choose "**Apply changes to C:\, subfolders and files**"



Click **OK** to continue

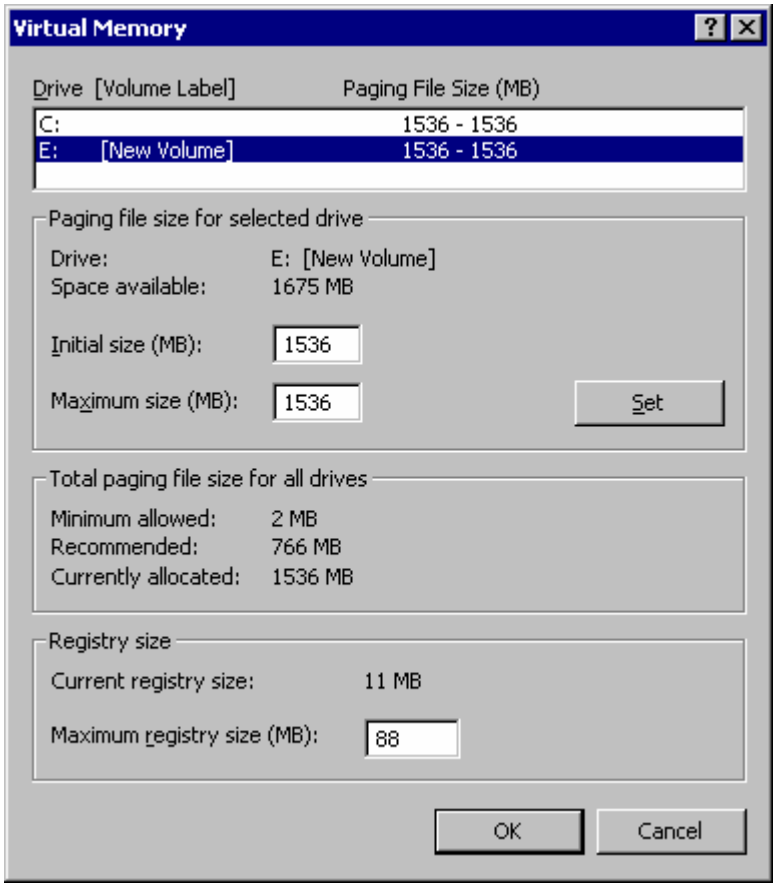
13.2 – Repeat this procedure for all other hard drive partitions.

Step 14 – Virtual Memory Settings

14.1 – Right mouse click on the **My Computer** icon and choose **Properties** and go to the **Advanced** Tab.

14.2 – Under the **Performance** subsection, choose **Performance Options** and click on the **Change** button.

14.3 – Under the **Paging file size for selected drive**, ensure that **Custom size:** is selected and set the Initial and Maximum size to be the same (**NOTE**: use the **Maximum size (MB):** figure for both values).



14.4 – Click the **Set** button.

14.5 – Repeat these same steps (**Steps 14.1** – **14.4**) for all other volumes.

14.6 – Click **OK** to get back to the System Properties window.

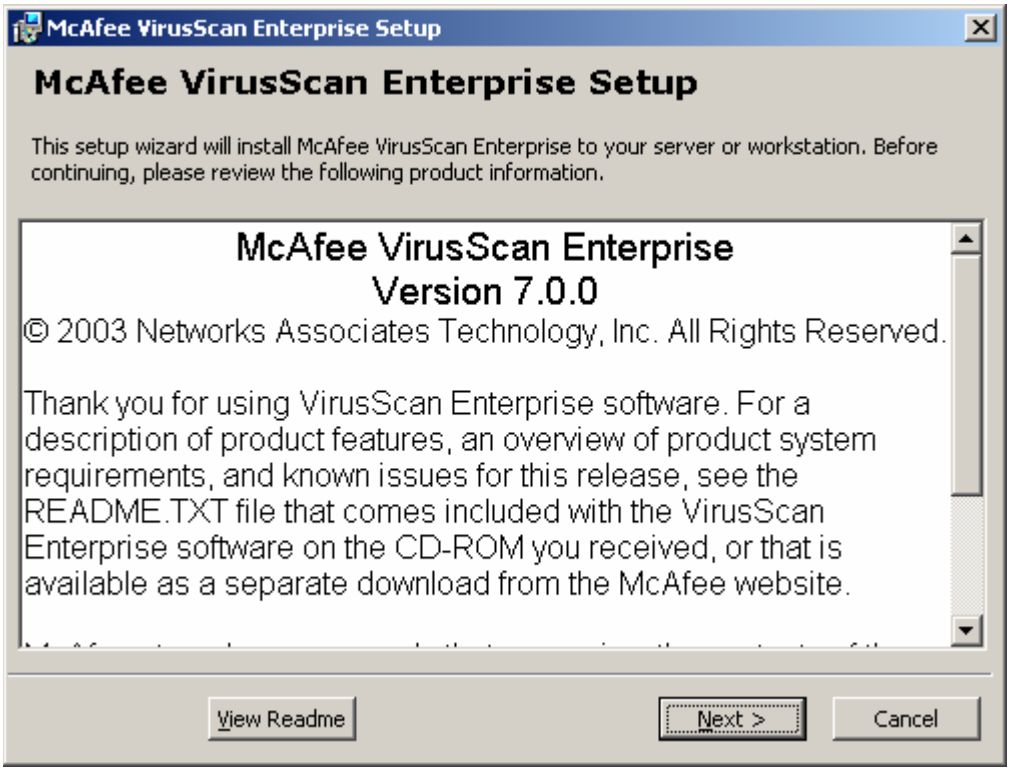
Step 15 – Installing the McAfee Anti-Virus Engine

We recommend McAfee VirusScan for Antivirus.

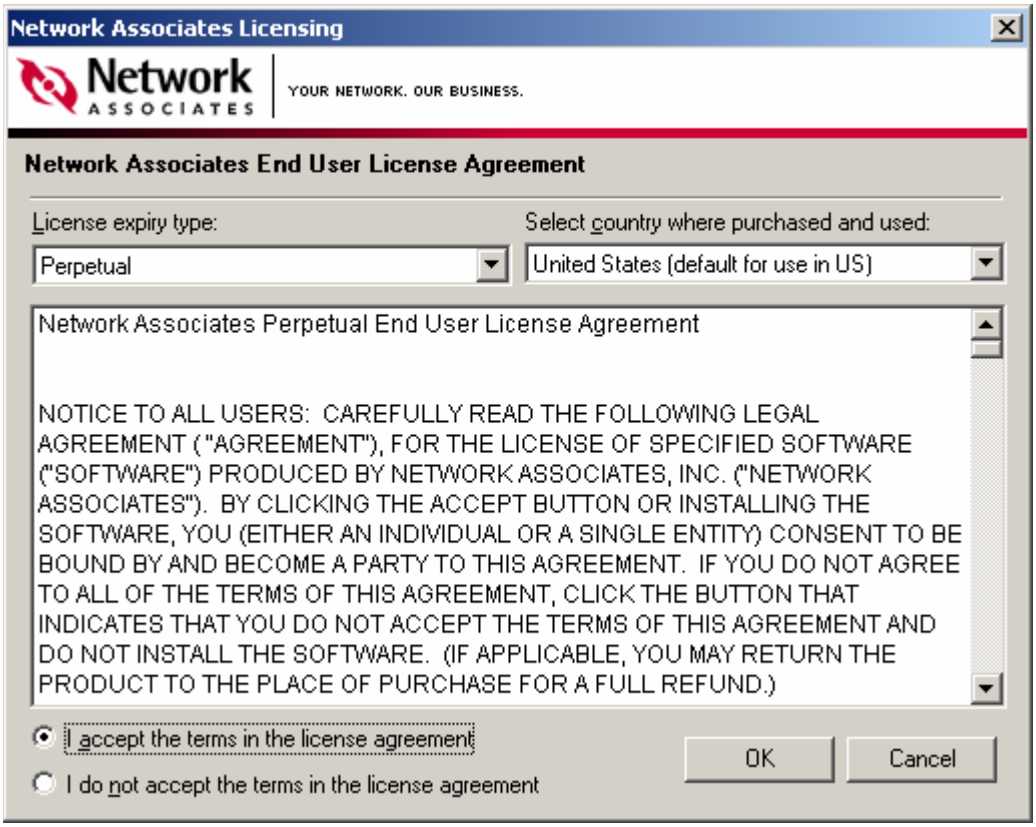
15.1 – Download the Virus Scan Engine.

15.2 – Create a folder and extract the Virus Scan Engine into it.

15.3 – Go to the folder that you extracted the file to and double click on **vse700.msi**



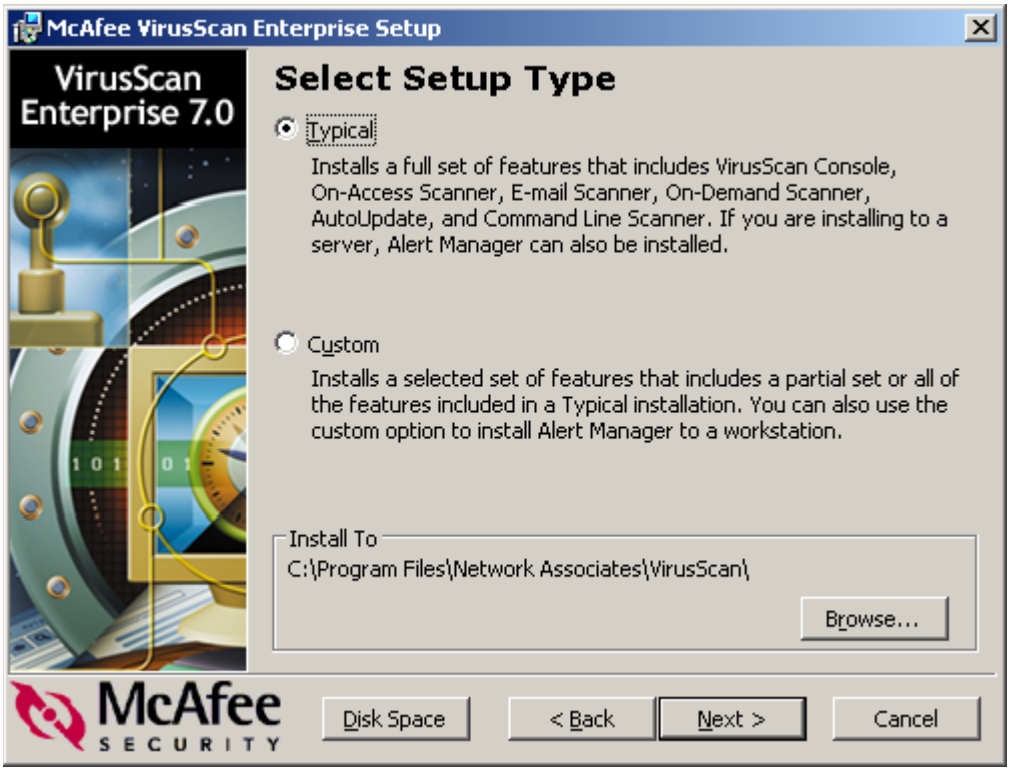
Click **Next**



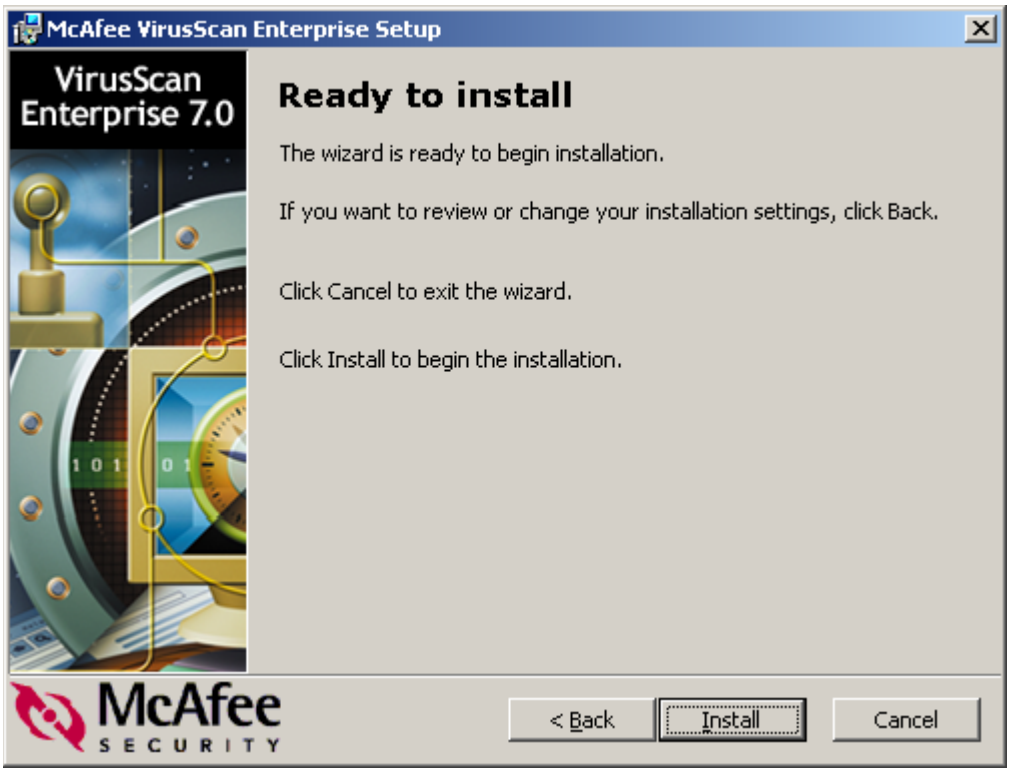
15.4 – Change the License expiry type to: **Perpetual**

15.5 – Click on **I accept the terms in the license agreement**

Click **OK**.



Click **Next**



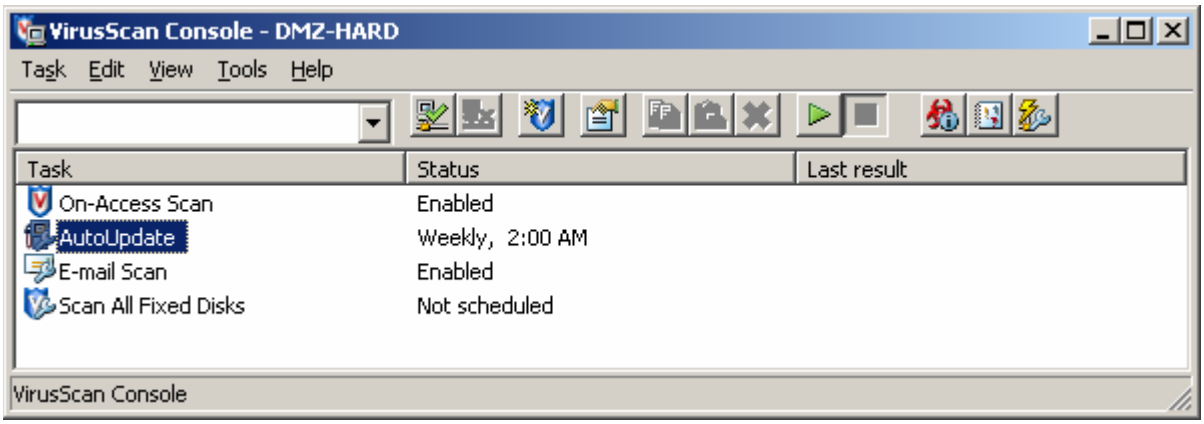
Click **Install**

McAfee will now install the necessary drivers and files.

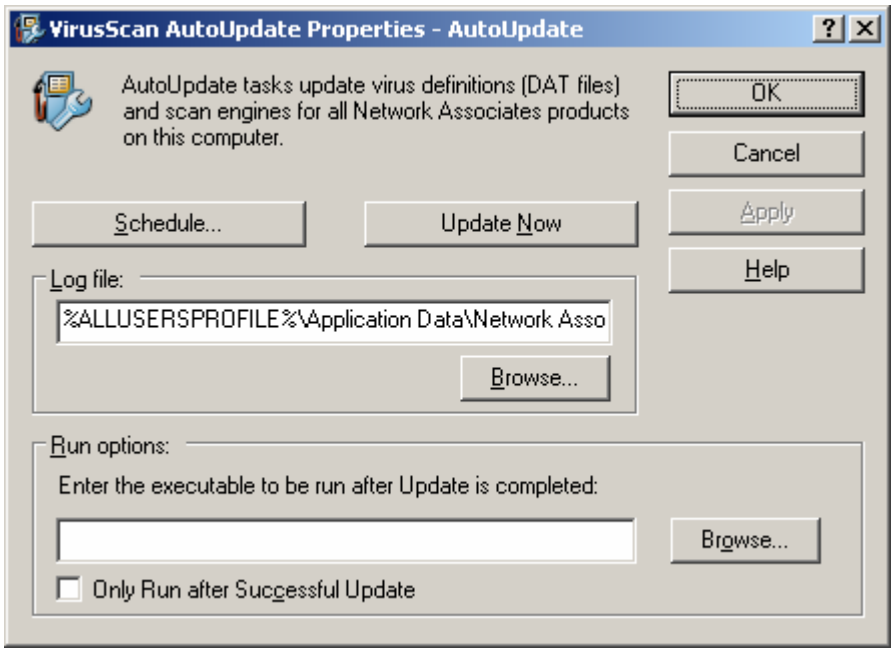
15.6 – Uncheck **Update Now** and **Run On-Demand Scan**

Click **Finish**

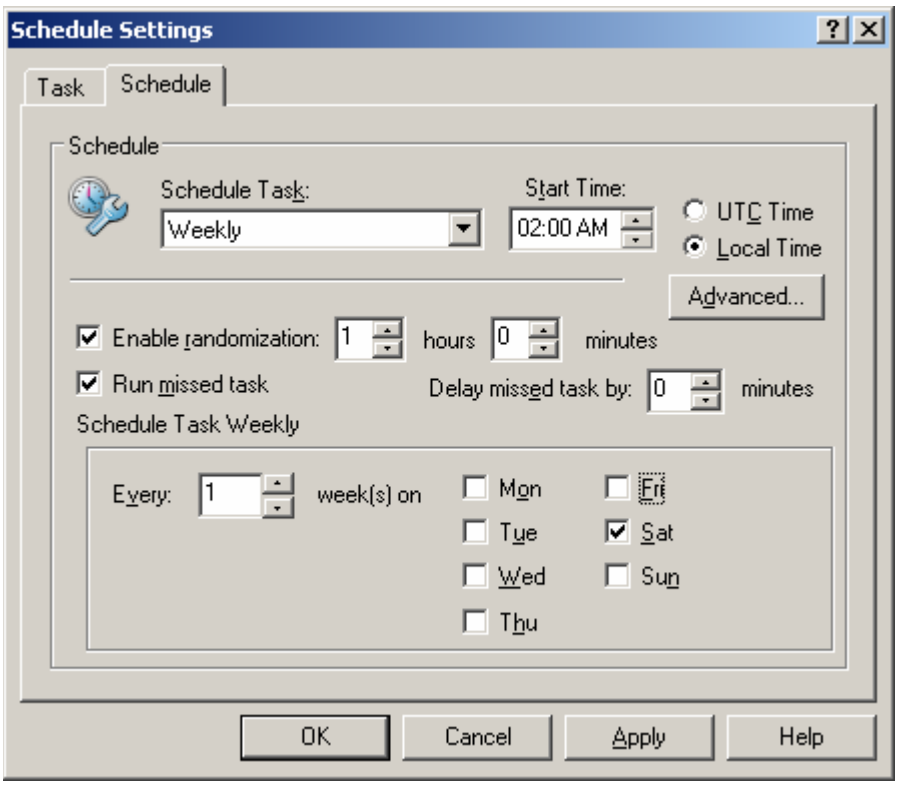
15.7 – In the task bar, Right click on the McAfee Antivirus icon and choose **VirusScan Console**



15.8 – Right click on **Auto Update** and select **Properties**

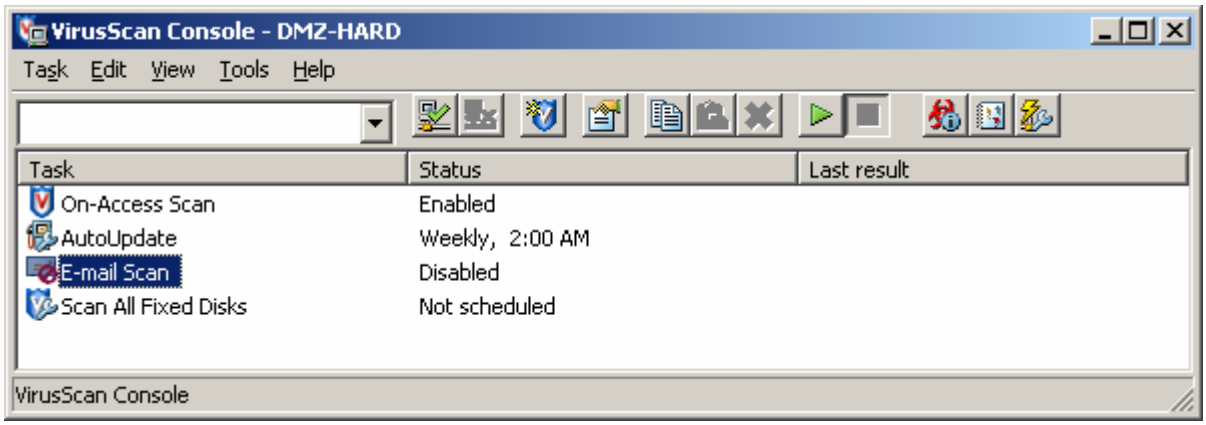


15.9 – Click on the Schedule button



15.10 – Under the **Schedule** Tab you should schedule the Anti-Virus Update according to your needs.

Click **Apply** then **OK**.



Step 16 – Installing the IIS Lockdown/URLScan toolkit

16.1 – Download the IIS Lockdown toolkit.

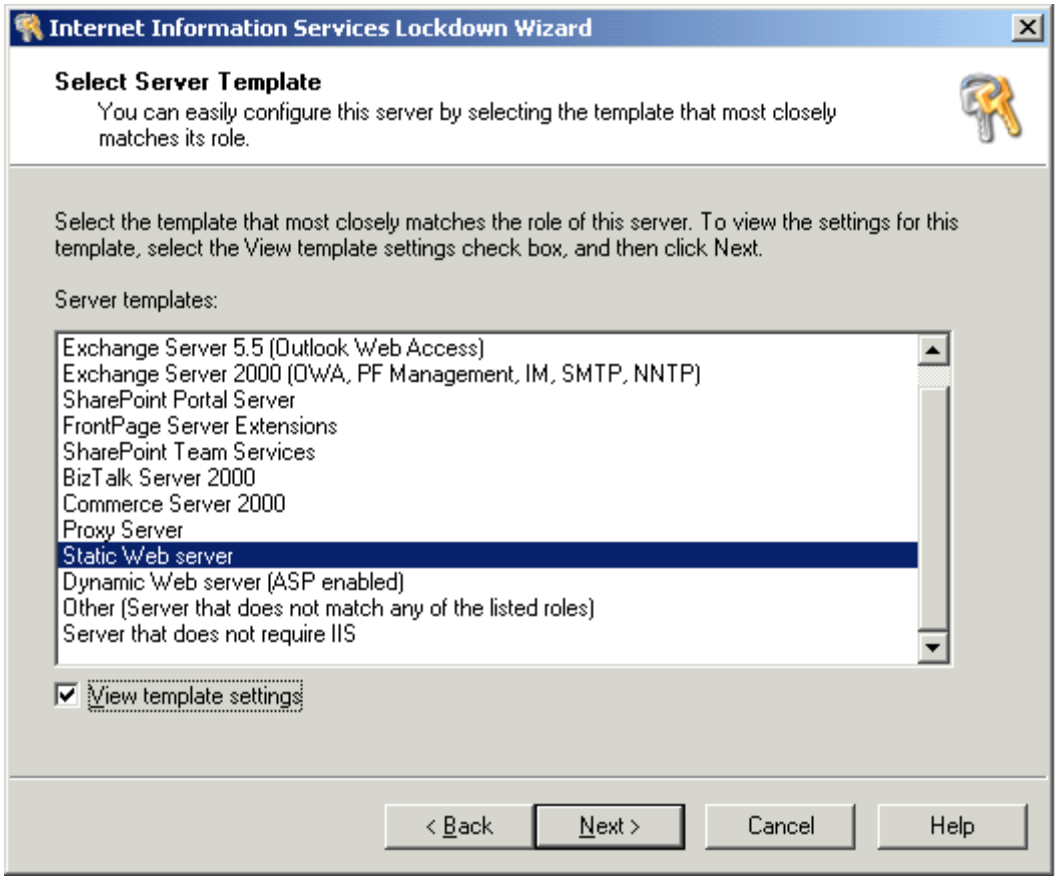
Click on and run the IISLockd.exe

Click **Next**

16.2 – Click "**I agree on the EULA license**" and then click **Next**.

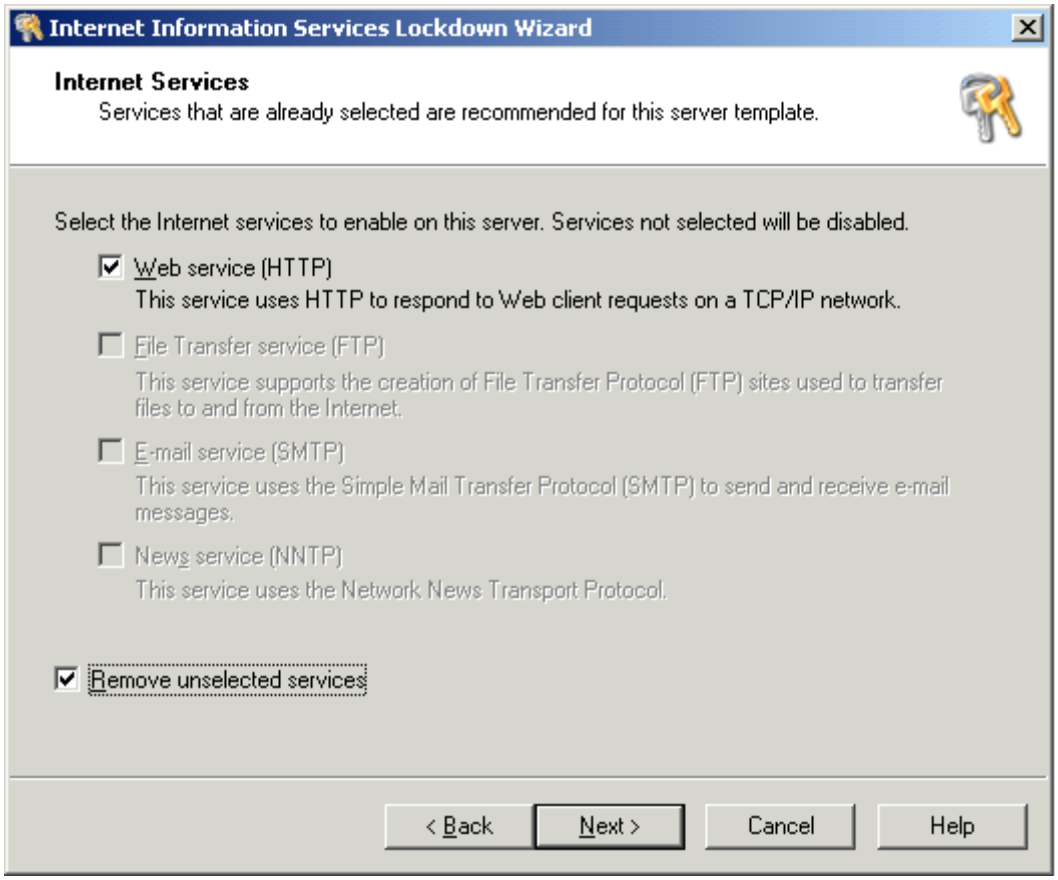
16.3 – The Select Server Type screen will appear. Click the "**View template settings**" box.

16.4 – Highlight Static Web Server



Click **Next**

The Internet Services window will appear.



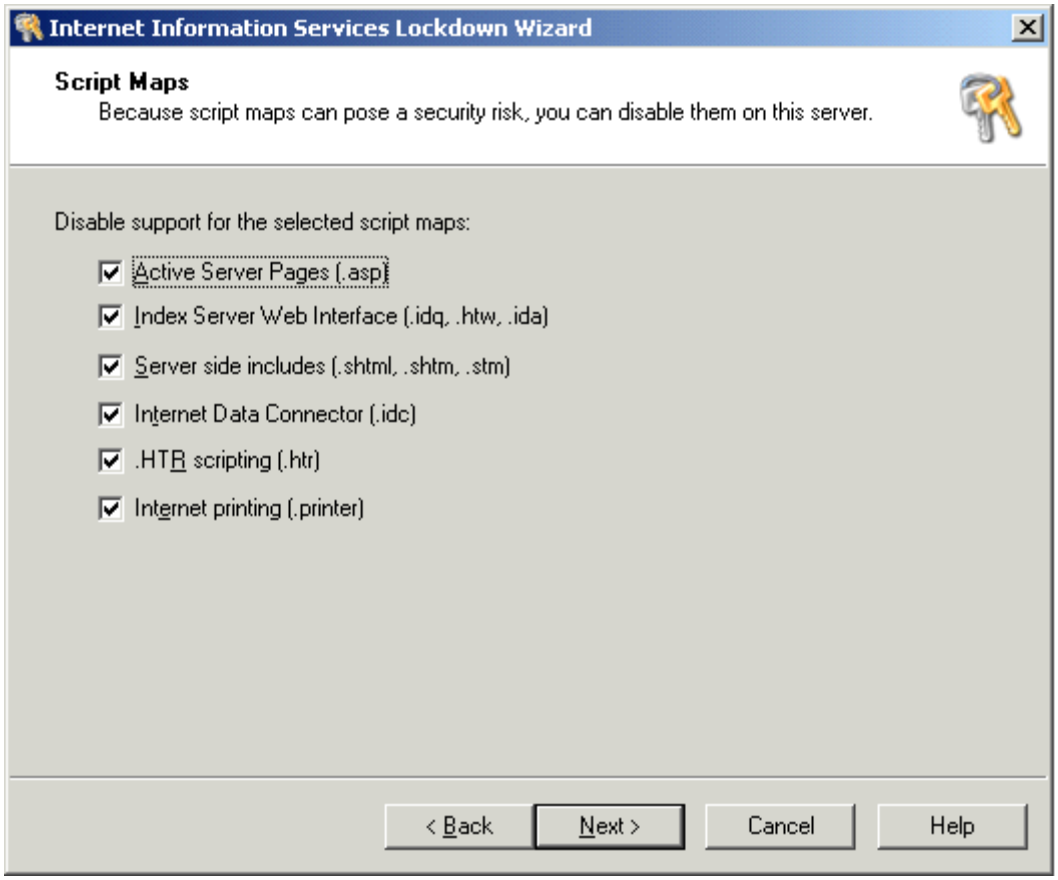
16.5 – Ensure that the **Web service (HTTP)** box is checked and check the "**Remove unselected services**" box.

A box will pop up asking if you want to remove the services

16.6 – Answer **Yes** to the "**Do you want to remove these services**" box.

Click **Next**

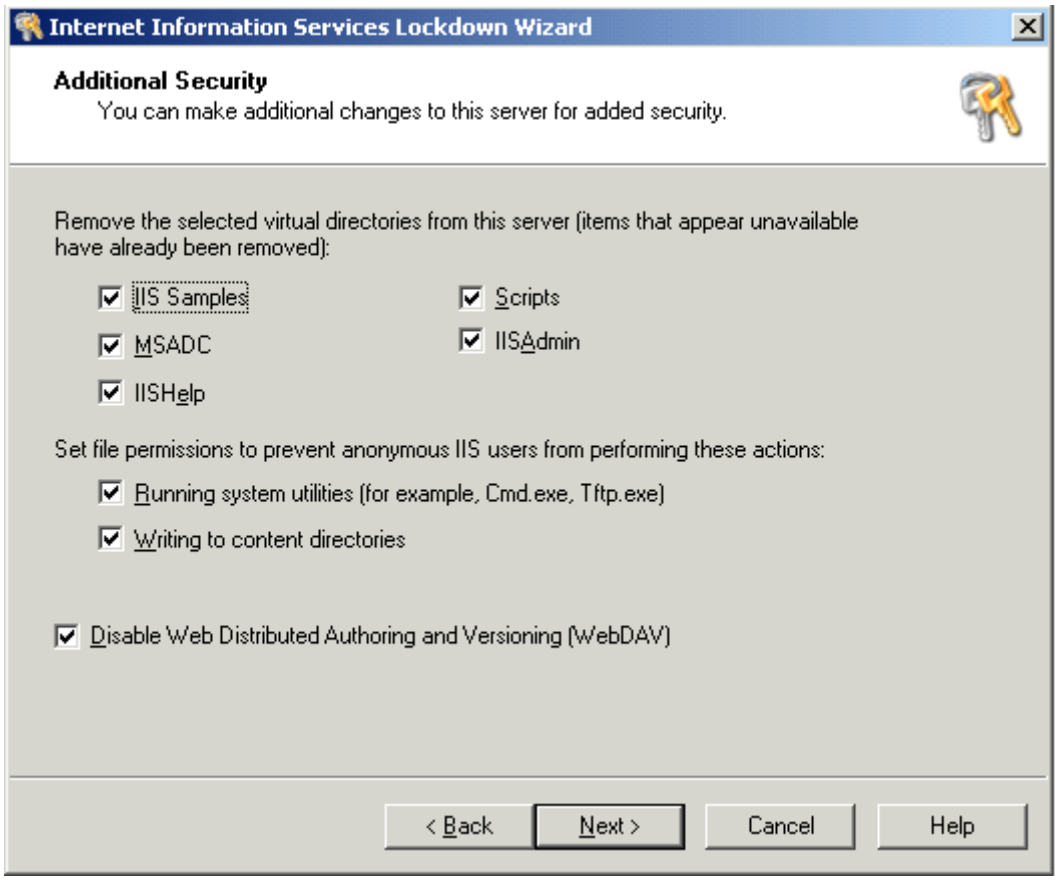
The Script Maps screen will appear



16.7 – Ensure all boxes are checked to set to disable

NOTE: If you plan to run ASP or SSI pages, you will need to uncheck those boxes appropriately.

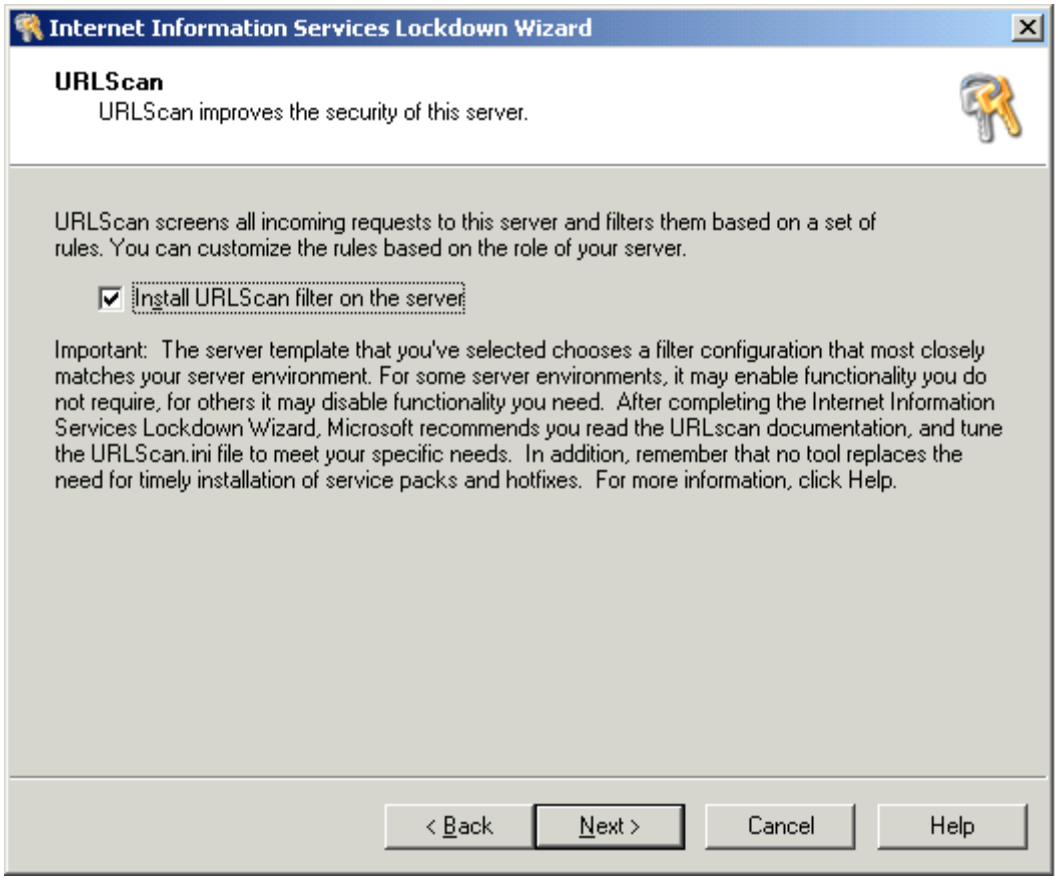
The Additional Security box will appear.



16.8 – Ensure all boxes are checked.

Click **Next**

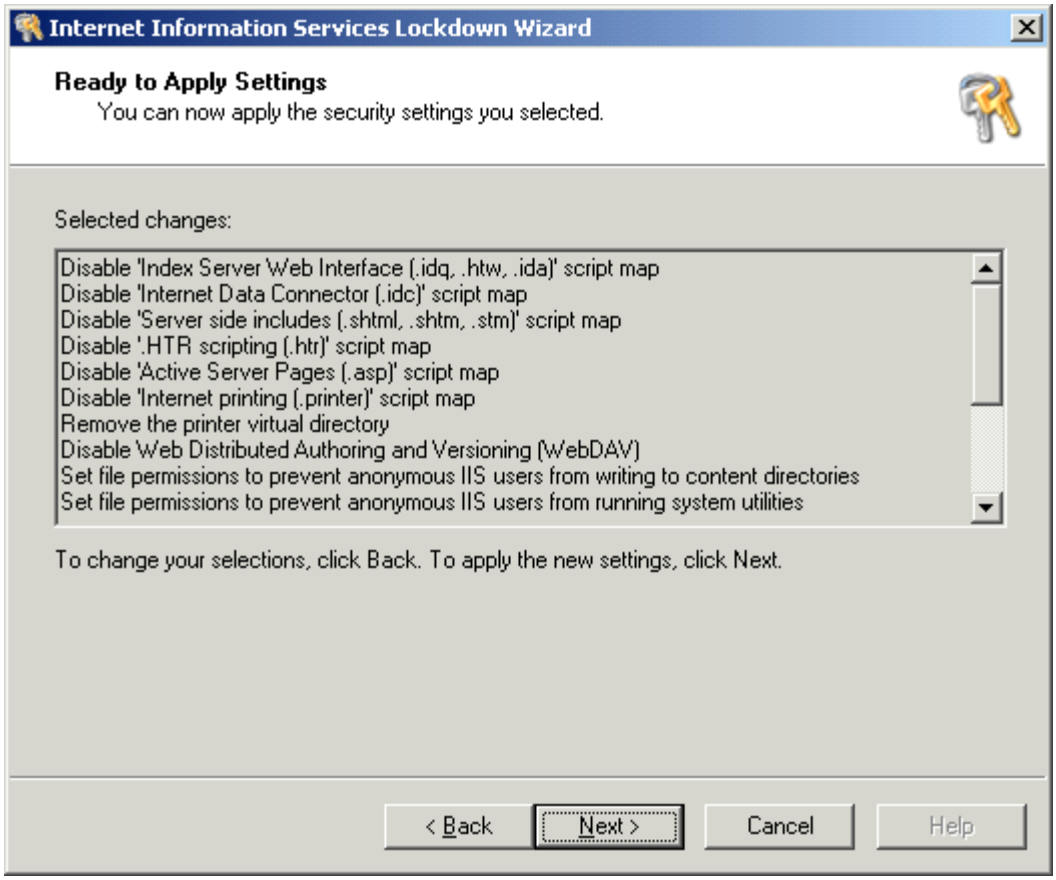
The URLScan screen will appear



16.9 – Ensure the box "**Install URLScan filter on the server**" is checked.

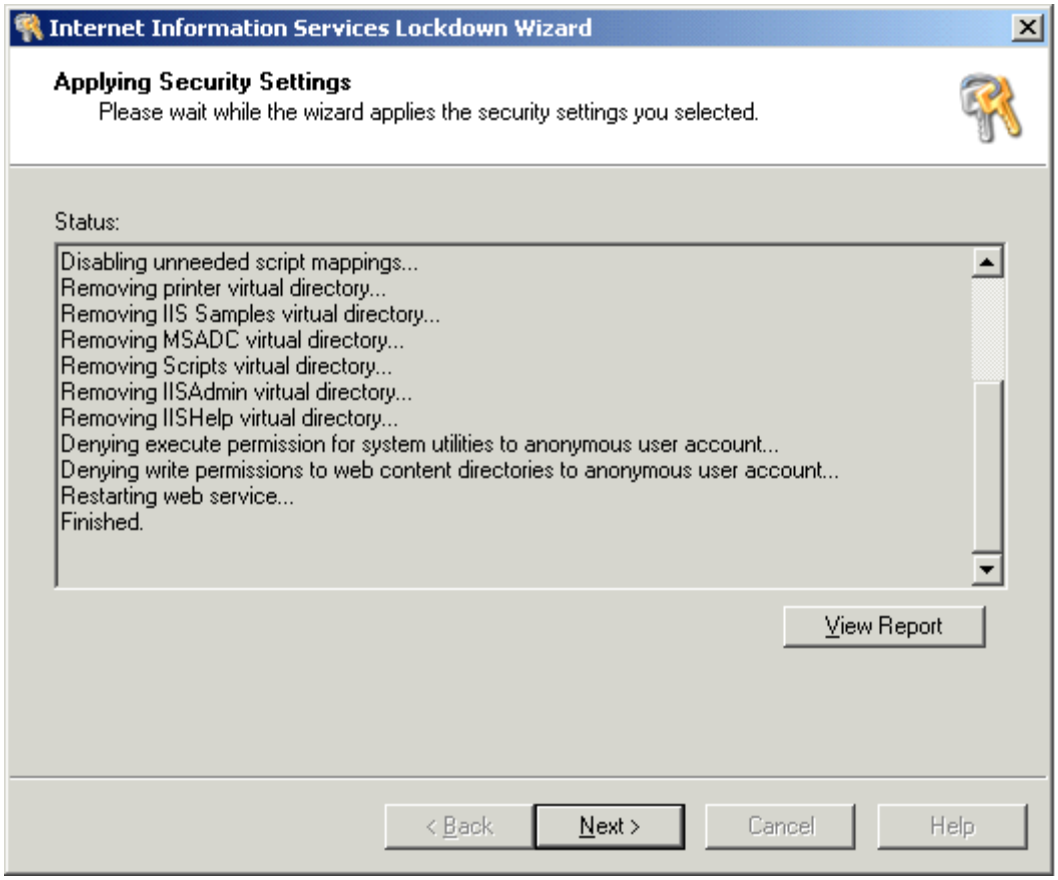
Click **Next**.

The Ready to Apply Settings screen will appear.



Click **Next**

The Applying Security Settings screen will appear.



16.10 – Click **View Report** if you wish to see what changes have been made.

Note: To see exactly what this does, look at this file c:\winnt\system32\inetsrv\oblt-log.log

16.11 – Click **Next**

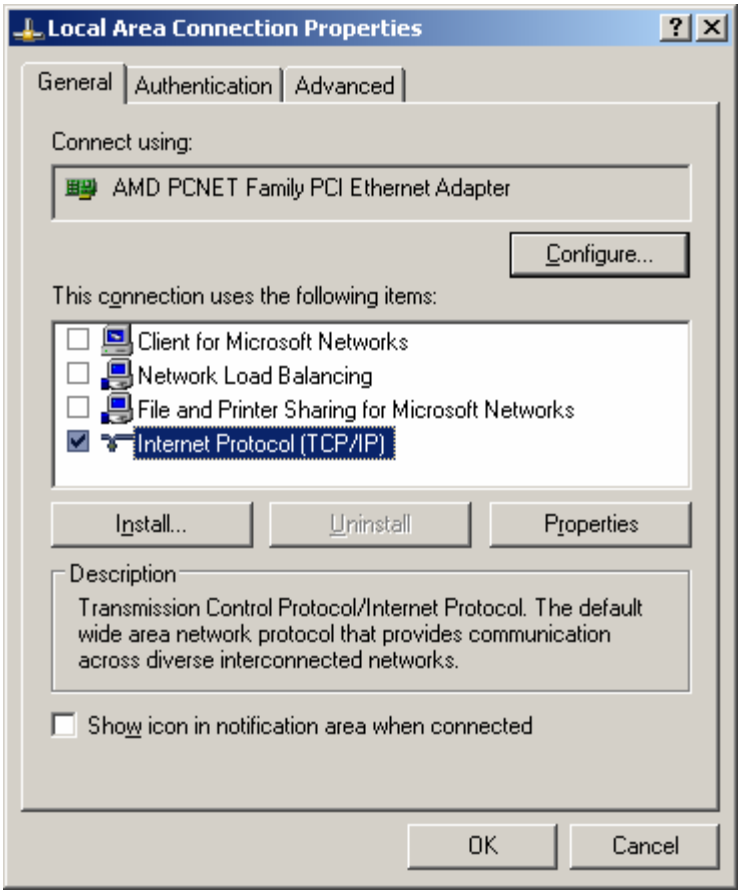
16.12 – Click **Finish**

Note: Most settings that have been applied here are reversible by running the wizard again. The default URLScan configuration file (**C:\winnt\system32\inetsrv\urlscan\urlscan.ini**) should work for you as is. If you need to make any changes, please consult with an Information Security representative.

Step 17 – Disabling Protocols and Setting a Fixed IP for the Server

17.1 – Right click on **My Network Places** and choose **Properties**.

17.2 – Right click on **Local Area Connection** and choose **Properties**. Choose the appropriate Local Area Connection and right click on it and choose **Properties**.



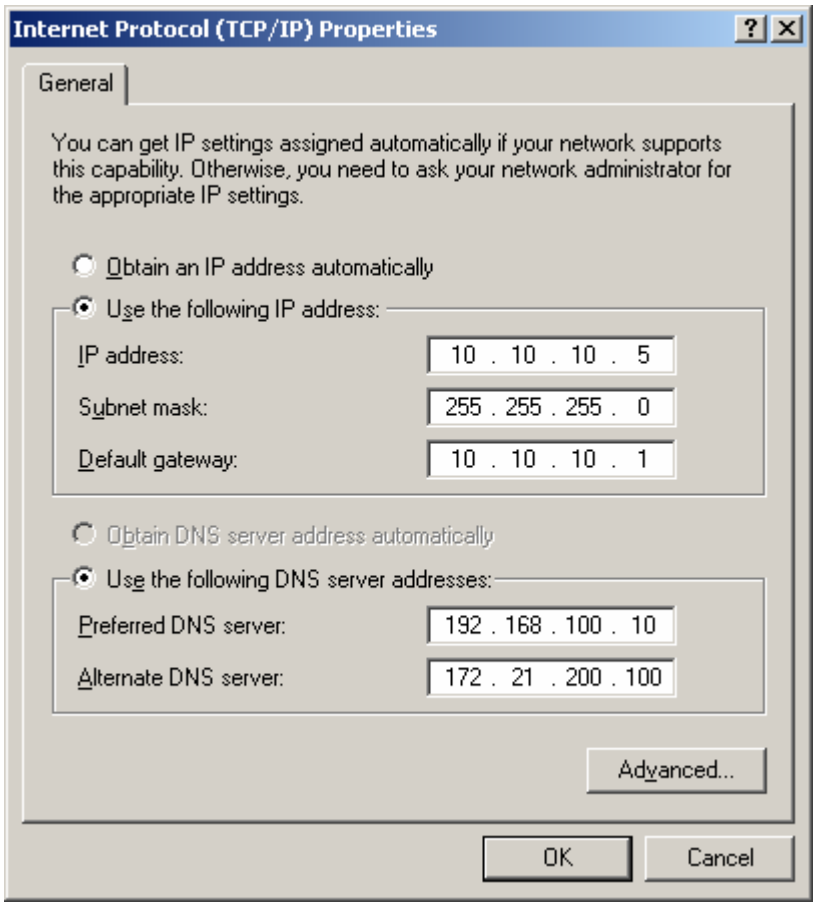
17.3 – Uncheck **Client for Microsoft Networks**

17.4 – Uncheck **File and Printer Sharing for Microsoft Networks**

17.5 – Select **Internet Protocol (TCP/IP)** and click on the **Properties** button.

17.6 – Choose **Use the Following IP Address** and input your static IP address, Subnet Mask and Default Gateway.

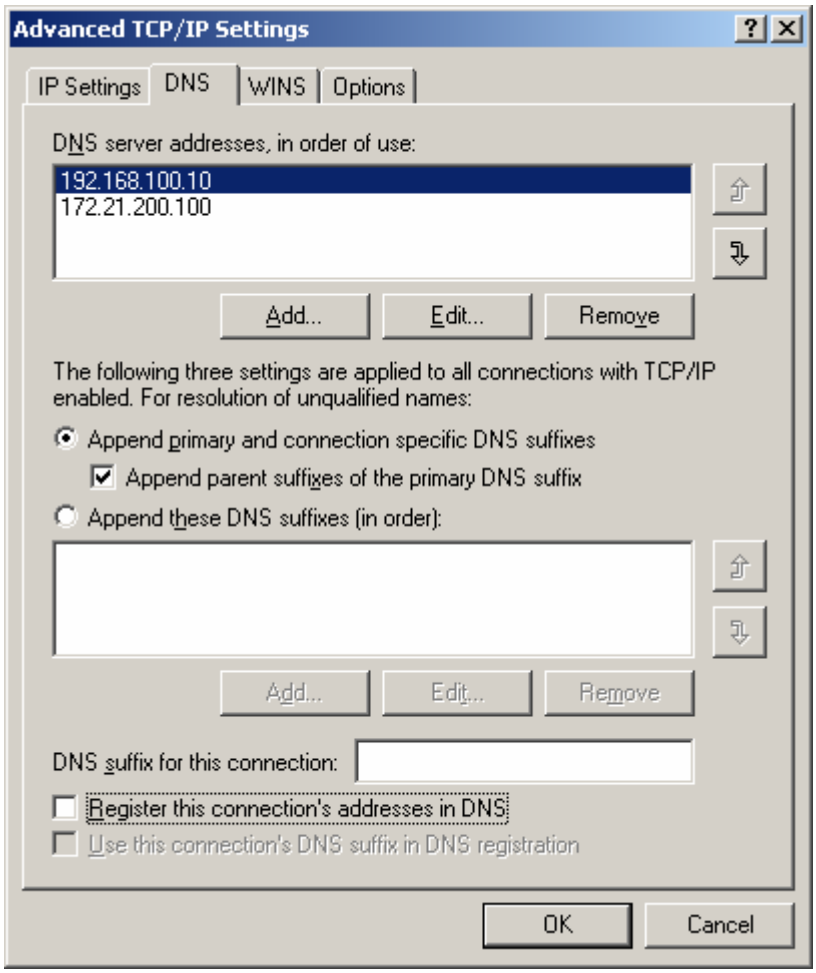
17.7 – Choose **Use the following DNS Server Addresses** and input your DNS Addresses. (**NOTE**: The DNS addresses in the below example are for illustration purposes only.)



17.8 – Click on the **Advanced** button.

Under the DNS Tab

17.9 – Uncheck **Register this connection's address in DNS**.

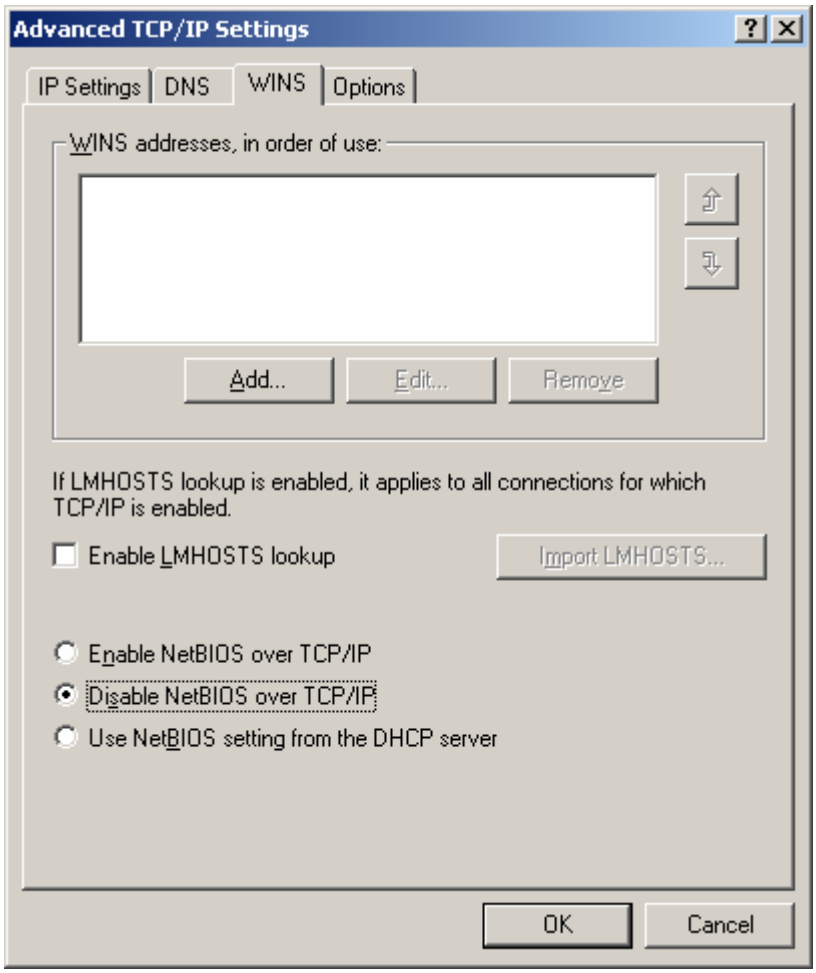


Under the **WINS** Tab

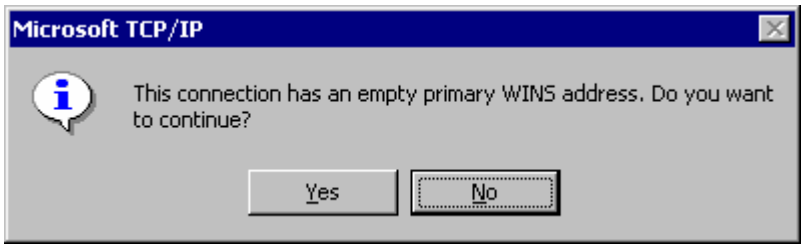
17.10 – Remove any **WINS** entries if they exist.

17.11 – Uncheck **Enable LMHOSTS lookup**

17.12 – Choose **Disable NetBIOS over TCP/IP**



You may get a pop-up box warning you that a WINS address is not available, like this one.



Click **Yes** to continue.

Under the **Options** Tab

17.13 – Choose **TCP/IP Filtering** and click on the Properties button

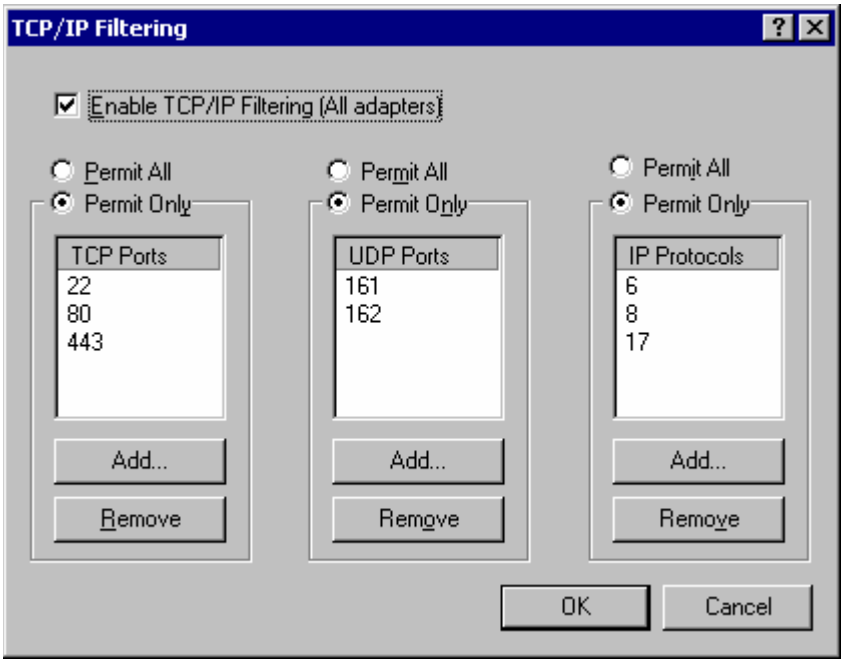
17.14 – Click on **Enable TCP/IP Filtering (All adapters)**

17.15 – Change the Permit All radio buttons to **Permit Only**

17.16 – Add **ONLY** the explicitly needed ports and protocols.

TCP Port	UDP Port	IP Protocol
22 – SSH	161 – SNMP	6 – TCP
80 – HTTP	162 – SNMP Trap	8 – ICMP

443 – HTTPS		17 – UDP



17.17 – Click **OK** to apply the filters.

17.18 – Click **OK** to return to Internet Protocol (TCP/IP) Properties

17.19 – Click **OK** to finalize all configurations.

17.20 – Click **Close** to close the Local Area Connection Properties.

17.21 – Select **Yes** when prompted to reboot.

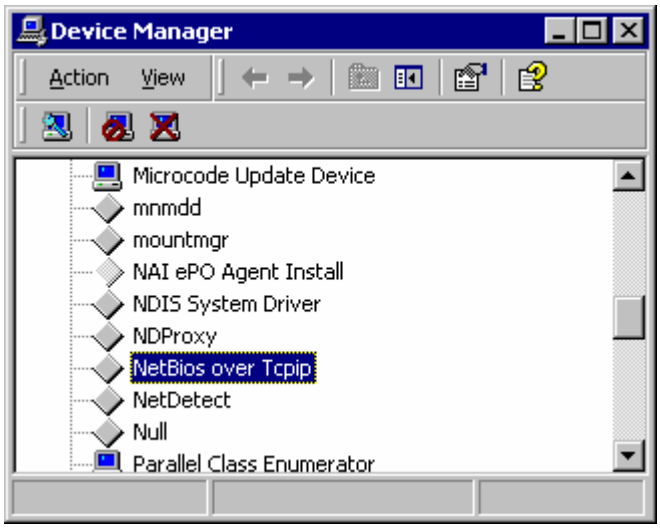
Step 18 - Disable NetBIOS over TCP/IP

18.1 – Click on **Hardware** Tab **> Device Manager** box.

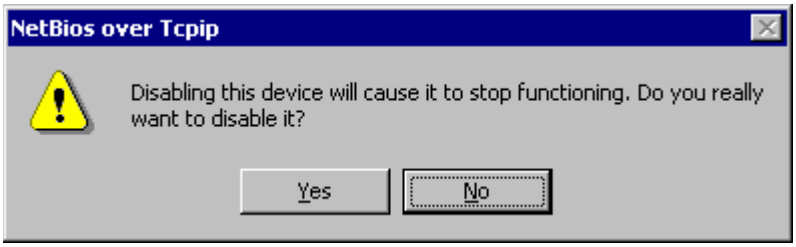
18.2 – Click on **View > Show Hidden Devices**

18.3 – Click on **View > Devices by Connection**

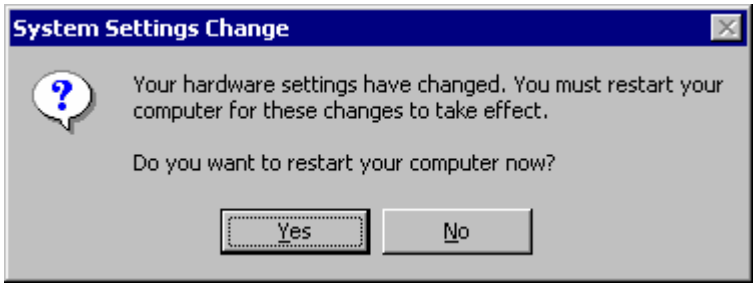
18.4 – Right click on **NetBios over Tcpip** > **Properties > Disable**



A pop up window should open that looks like this:



18.5 – Choose **Yes**

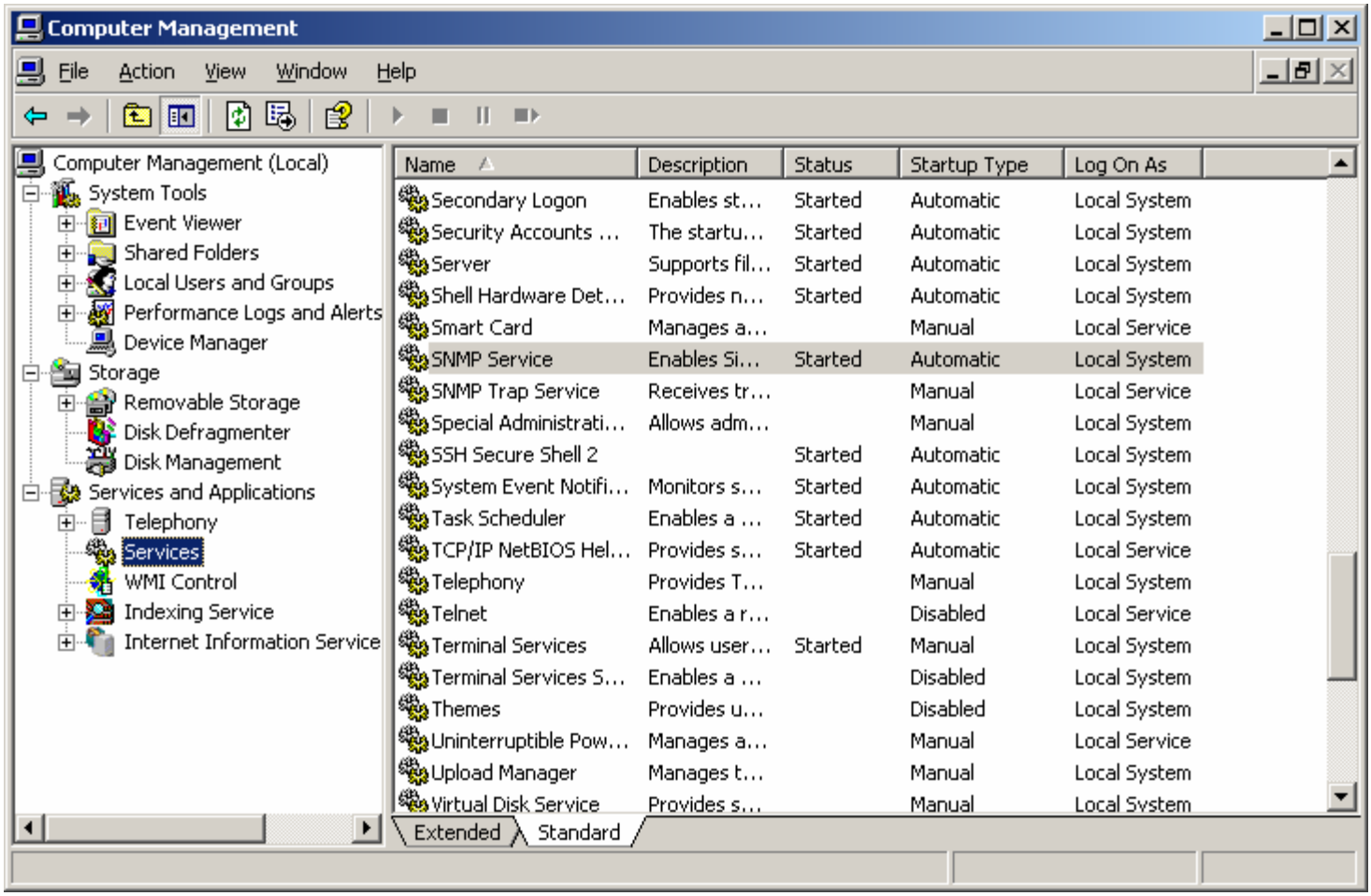


18.6 – Choose **Yes** when prompted to reboot.

Step 19 - SNMP Community String

19.1 – Right Click on **My Computer** > **Manage**

19.2 – Under **Services and Applications**, select **Services**



Step 19.3 – Scroll Down and right click on **SNMP Service** and select **Properties**

Under the **Security** Tab

Step 19.4 – Ensure that **Send authentication trap** is selected.

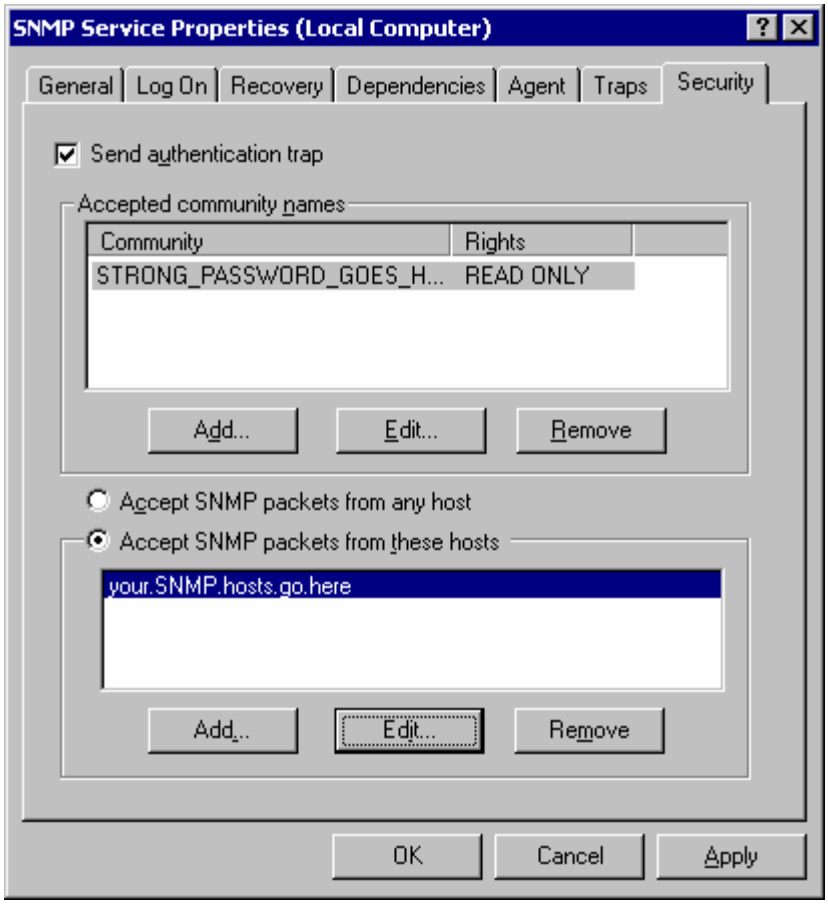
Step 19.5 – Click **Add**

Step 19.6 – Select **READ ONLY** for Community Rights

Step 19.7 – For Community Name (aka Community String), choose a strong password and type it into the box. This community string (password) will need to be provided to anyone requesting SNMP access to this machine.

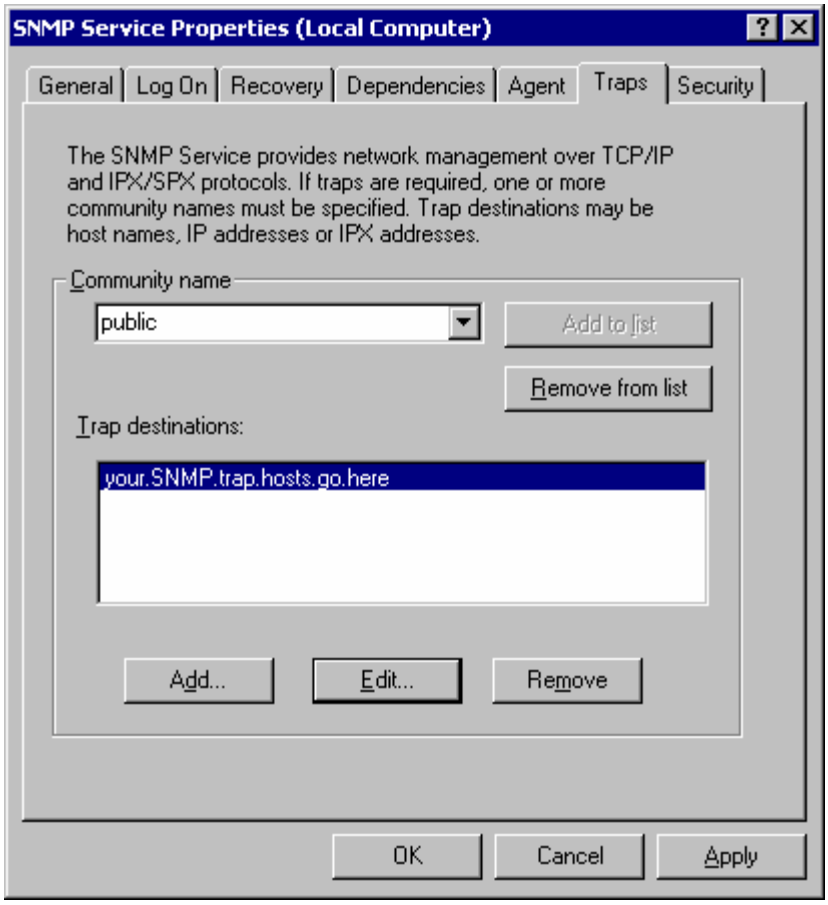
Step 19.8 – Choose **Accept SNMP packets from these hosts**.

Step 19.9 – Click **Add** and add the SNMP hosts as supplied by your Network Admin.



Step 19.10 – Click on the **Traps** Tab and in the Community Name white-space, type: **public**

Step 19.11 – Click on the **Add** button and add your trap destinations as provided by your Network Admin.



Step 19.12 – Click **Apply** then click **OK** to exit.

Step 19.13 – Close the Computer Management window.

Step 20 – Setup the IPSec Policy to allow only necessary ports.

20.1 – Place ipsecpol.exe, ipsecutil.dll and text2pol.dll in your **C:\winnt\system32** directory.

20.2 – Download the IPSec Policy File.

20.3 – Review the file and remove any IPSec filters that you do not explicitly need.

By default, the following services are configured in the IPSec Policy file:

IIS 5.0 DMZ Server IPSec Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
SSH	TCP	ANY	22	ANY	ME	ALLOW	YES
DNS	TCP	ANY	53	ANY	ME	ALLOW	YES
DNS	UDP	ANY	53	ANY	ME	ALLOW	YES
HTTP	TCP	ANY	80	ANY	ME	ALLOW	YES
SNMP	UDP	ANY	161	ANY	ME	ALLOW	YES
SNMP TRAP	UDP	ANY	162	ME	ANY	ALLOW	YES
HTTPS	TCP	ANY	443	ANY	ME	ALLOW	YES
SYSLOG	UDP	ANY	514	ANY	ME	ALLOW	YES
NetBackup	TCP	ANY	13700	ANY	ME	ALLOW	YES

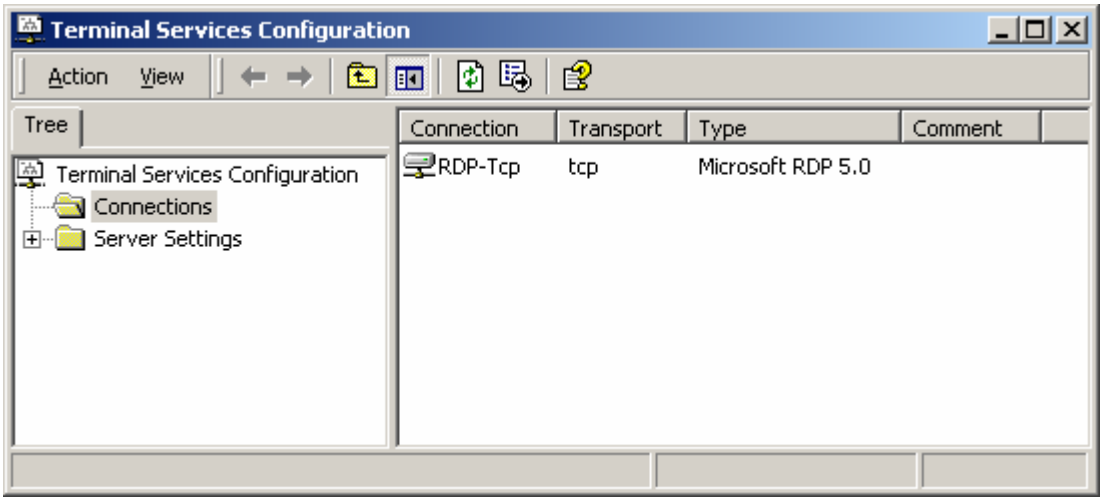
NetBackup	TCP	ANY	13782	ANY	ME	ALLOW	YES
ICMP	ICMP	ANY	ANY	ANY	ME	ALLOW	YES
All Other Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

20.3 – You can copy and paste the lines from the IPSec Policy file into a command shell window to install the policy.

Step 21 – Configure Terminal Services

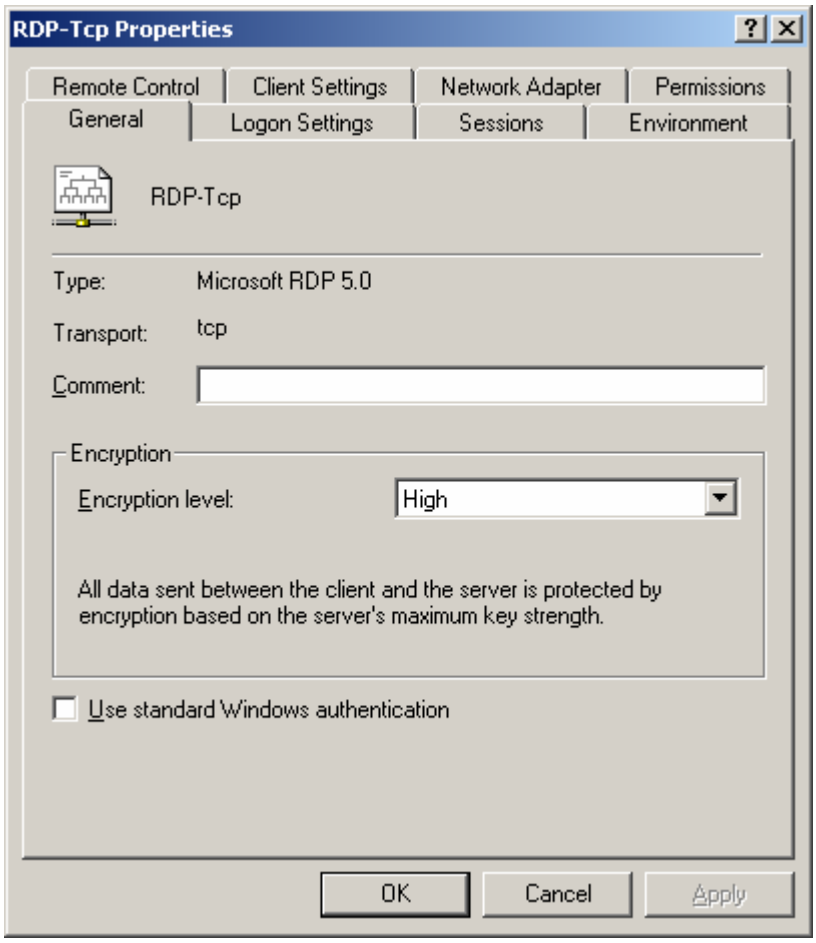
21.1 – Go to **Start > Programs > Administrative Tools > Terminal Services Configuration (TSC).**

21.2 – Over in the right panel, right mouse click on **RDP-Tcp** and choose **Properties**.



Under the General Tab:

21.3 – Change the Encryption Level to **High**.

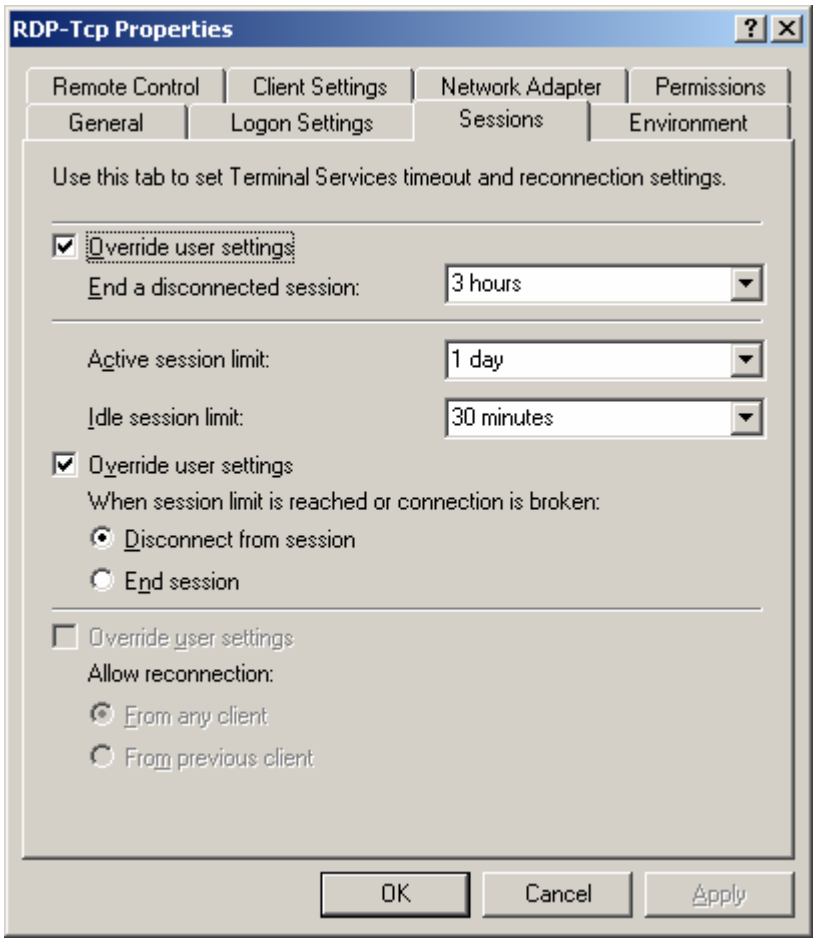


Under the **Sessions** Tab

21.4 – Check the first **Override User Settings**, then choose:

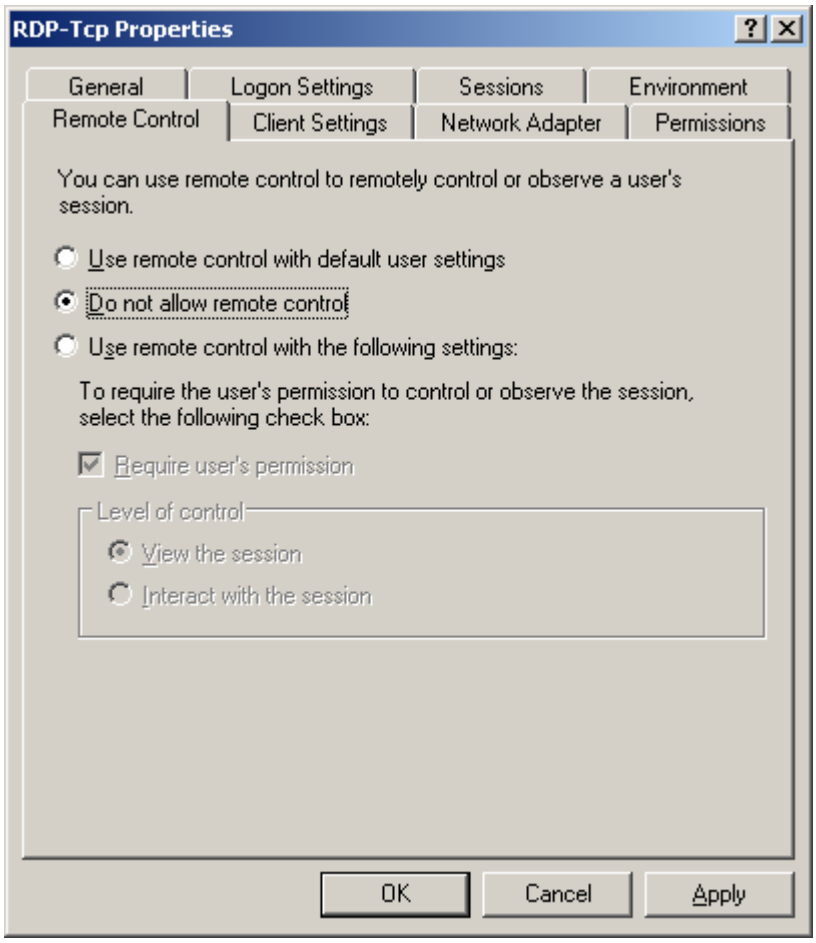
End a Disconnected Session: 3 Hours
Active Session Limit: 1 Day
Idle Session Limit: 30 Minutes

21.5 – Check the second **Override User Settings** and choose: **Disconnect from Session.**



Under the **Remote Control** Tab

21.6 – Choose **Do not allow remote control**

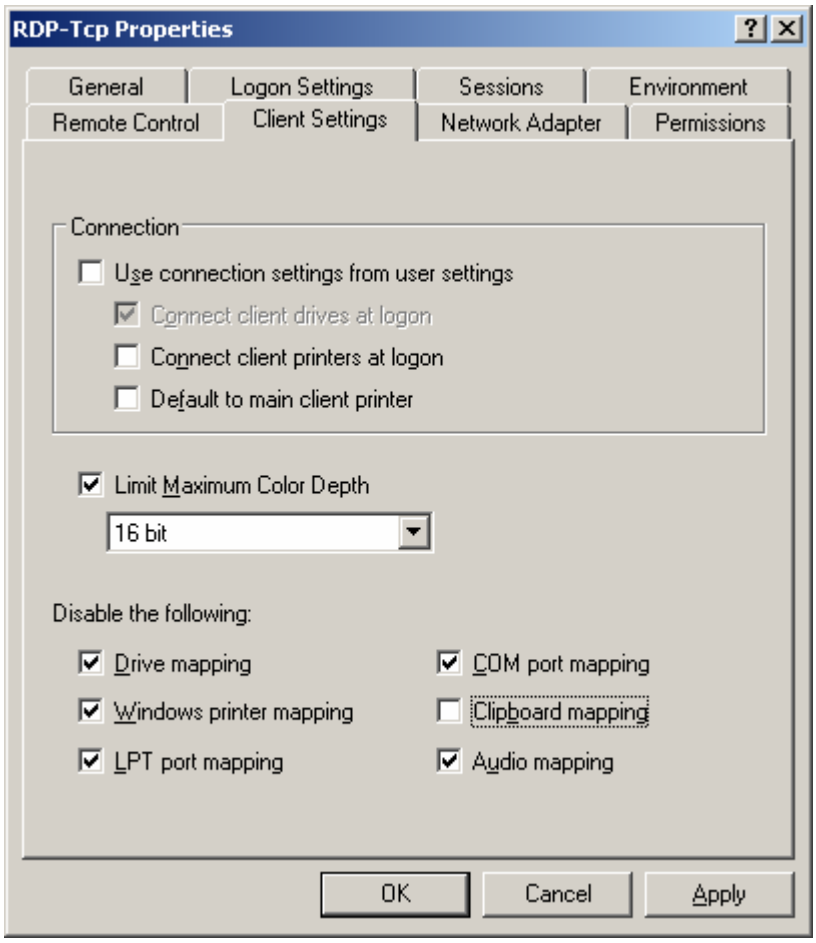


Under the Client Settings Tab:

21.7 – Uncheck **Use Connection Settings From User Settings**
21.8 – Uncheck **Connect Client Printers at Logon and Default to Main Client Printer**

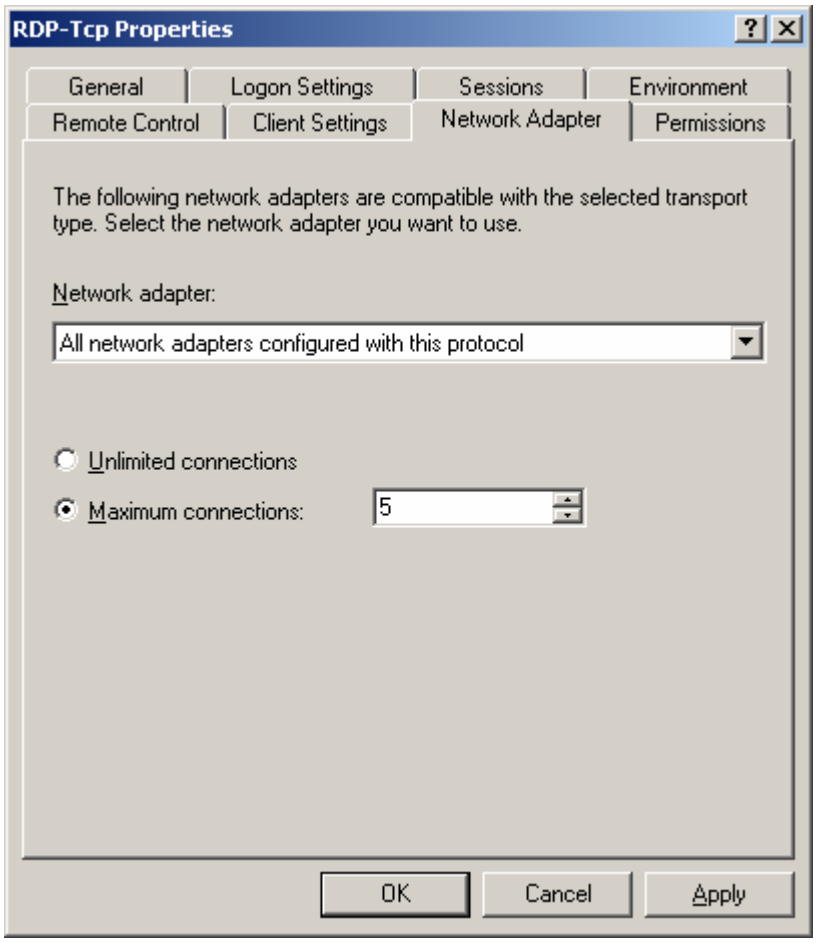
Under the Disable subsection:

21.9 – Check all boxes except **Clipboard Mapping**.



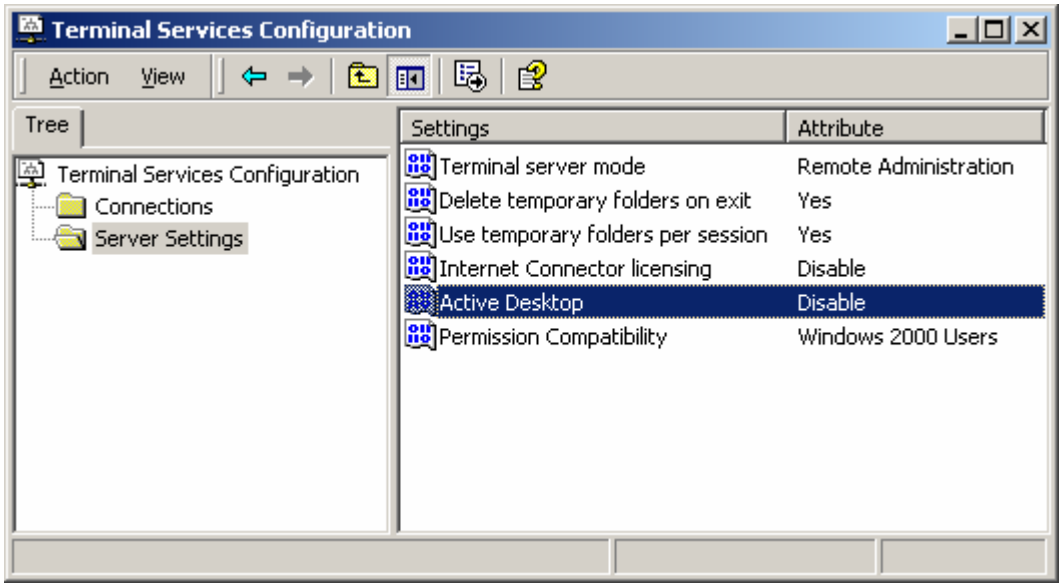
Under the Network Adapter Tab:

21.10 – Click on the **Maximum Connections** radio button and ensure the number is set to no more than 5.



21.11 – Click **Apply** and then close the window.

21.12 – In the left hand panel, under **Server Settings**, change Active Desktop to **Disable**

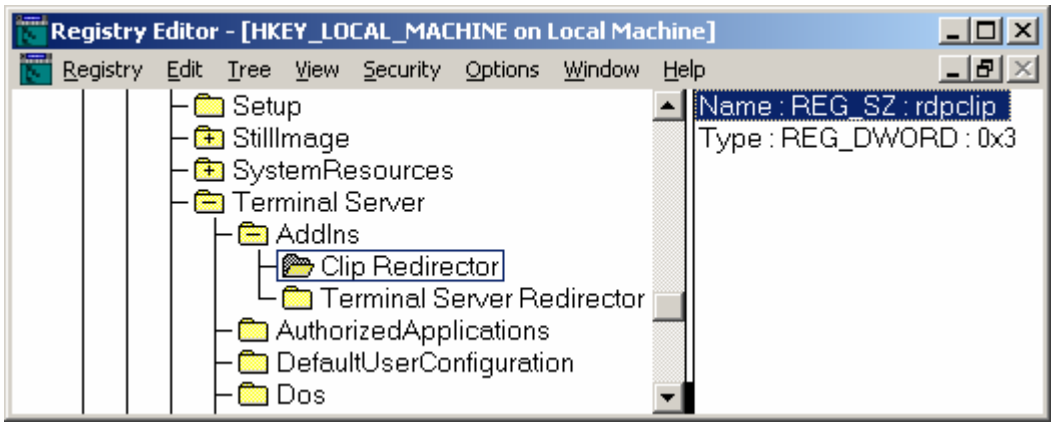


21.13 – (Optional) If you wish to enable clipboard file transfer between client and server, do the following steps (**Steps 21.14** – **21.23**). Otherwise skip to Step 22.

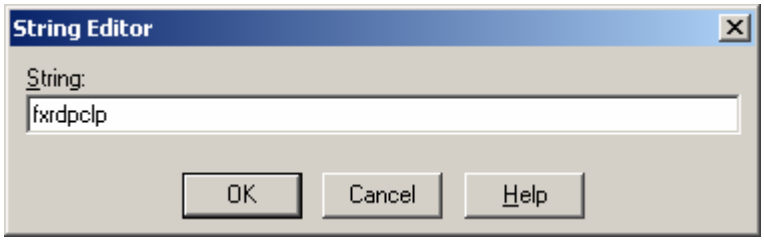
On the Server:

21.14 – Open **Start** > **Run** > **Regedt32**

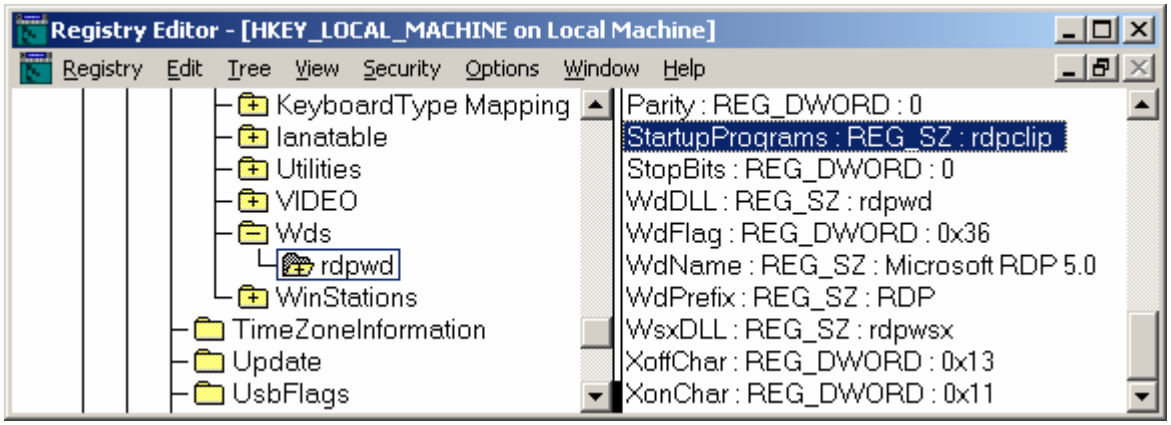
21.15 – Navigate to **HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\AddIns\Clip Redirector**



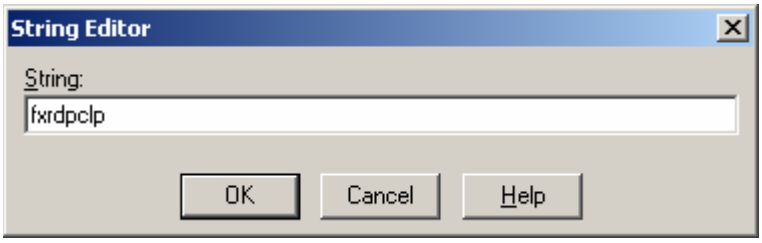
21.16 – Change the value data in the **Name Value** from **RDPCLIP** to **FXRDPCLP**



21.17 – Navigate to **HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd**



21.18 – Change the value data in the Startup Programs from **RDPCLIP** to **FXRDPCLP**



21.19 – Copy the file, fxrdpclp.exe to the **C:\WINNT\System32** folder.

21.20 – Copy the file, fxfr.dll to the **C:\WINNT\System32** folder.

On the Client:

21.21 – Copy the file, fxfr.dll to the **C:\Program Files\Terminal Services Client** folder on the client PC.

21.22 – Rename the rdpdr.dll file in the **C:\Program Files\Terminal Services Client** folder to **rdpdr.pss**

21.23 – Copy the file, rdpdr.dll to the **C:\Program Files\Terminal Services Client** folder.

Step 22 – Set up Terminal Services to run over SSH

22.1 – Open the SSH Secure Shell Client

22.2 – Select the folder named **Profiles** > **Add Profile**

22.3 – Give the Profile a Name and then click the **Add to Profiles** button.

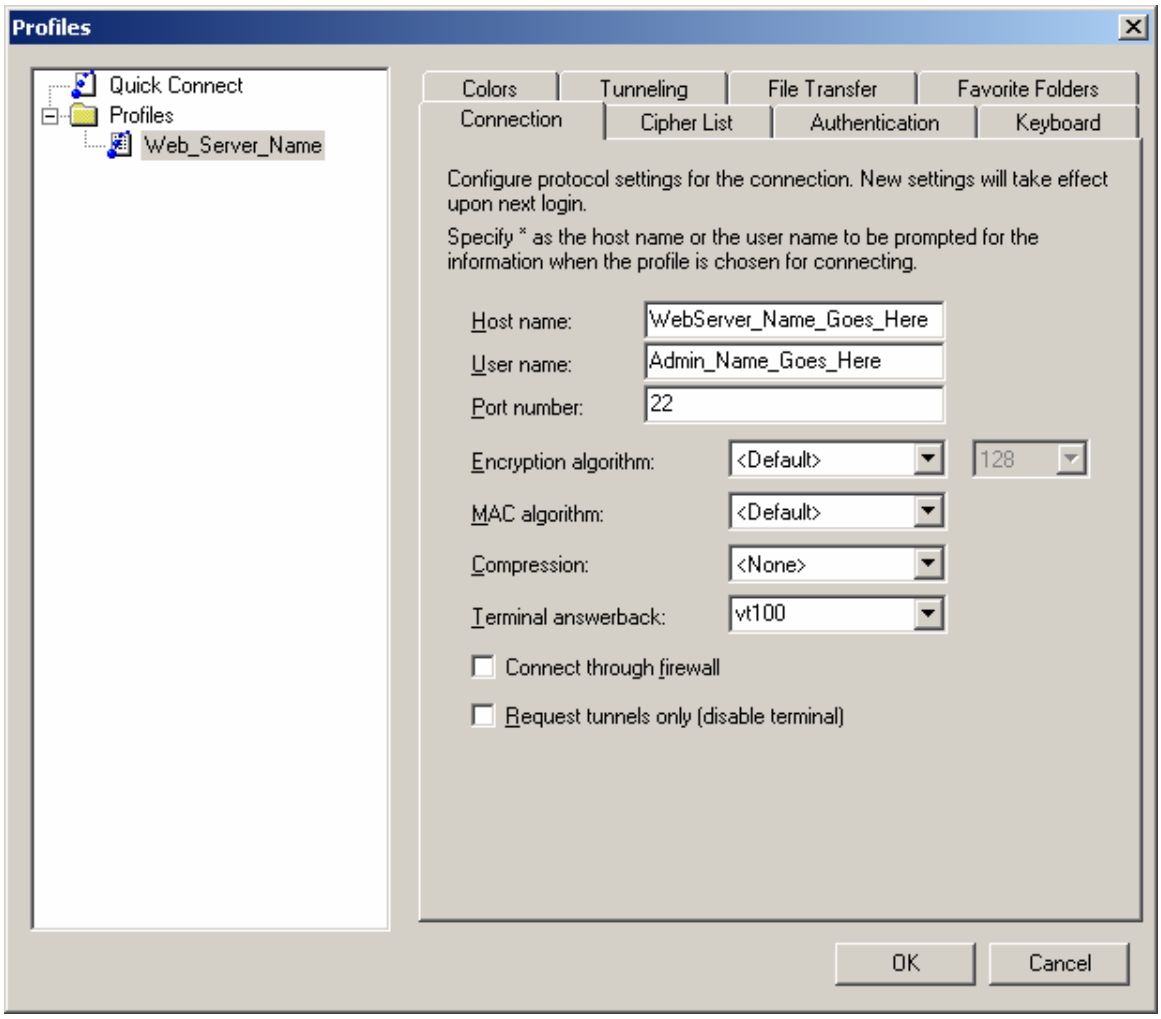
22.4 – Select **Profiles** folder again and select **Edit Profile**.

22.5 - In the left window, choose the Server profile that you wish to edit.

Under the Connection Tab:

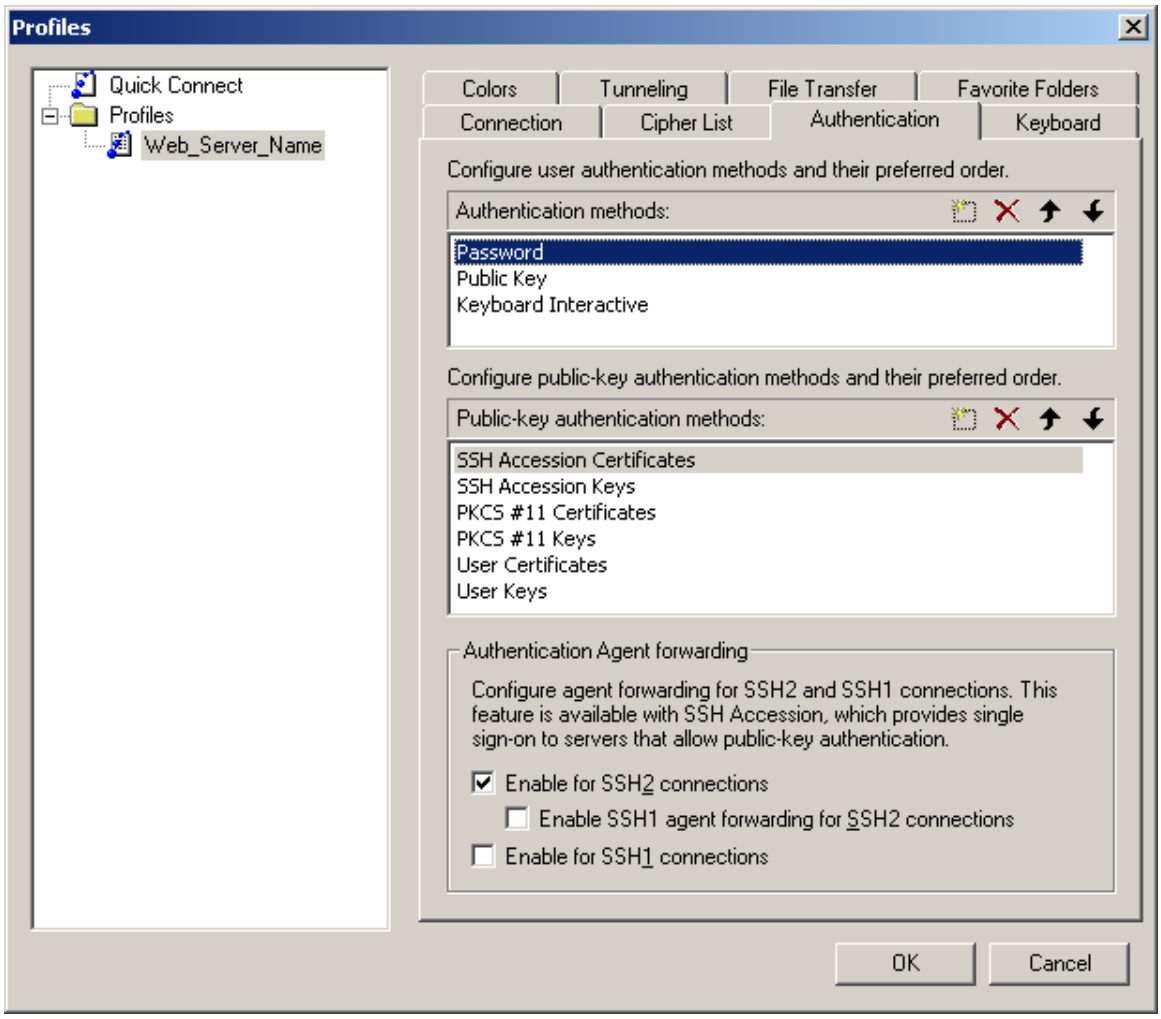
- Enter Hostname of your server.
- Enter User name that you are authenticating with.

NOTE: This User Name will have to be changed to match that of the name in step **[number here]**



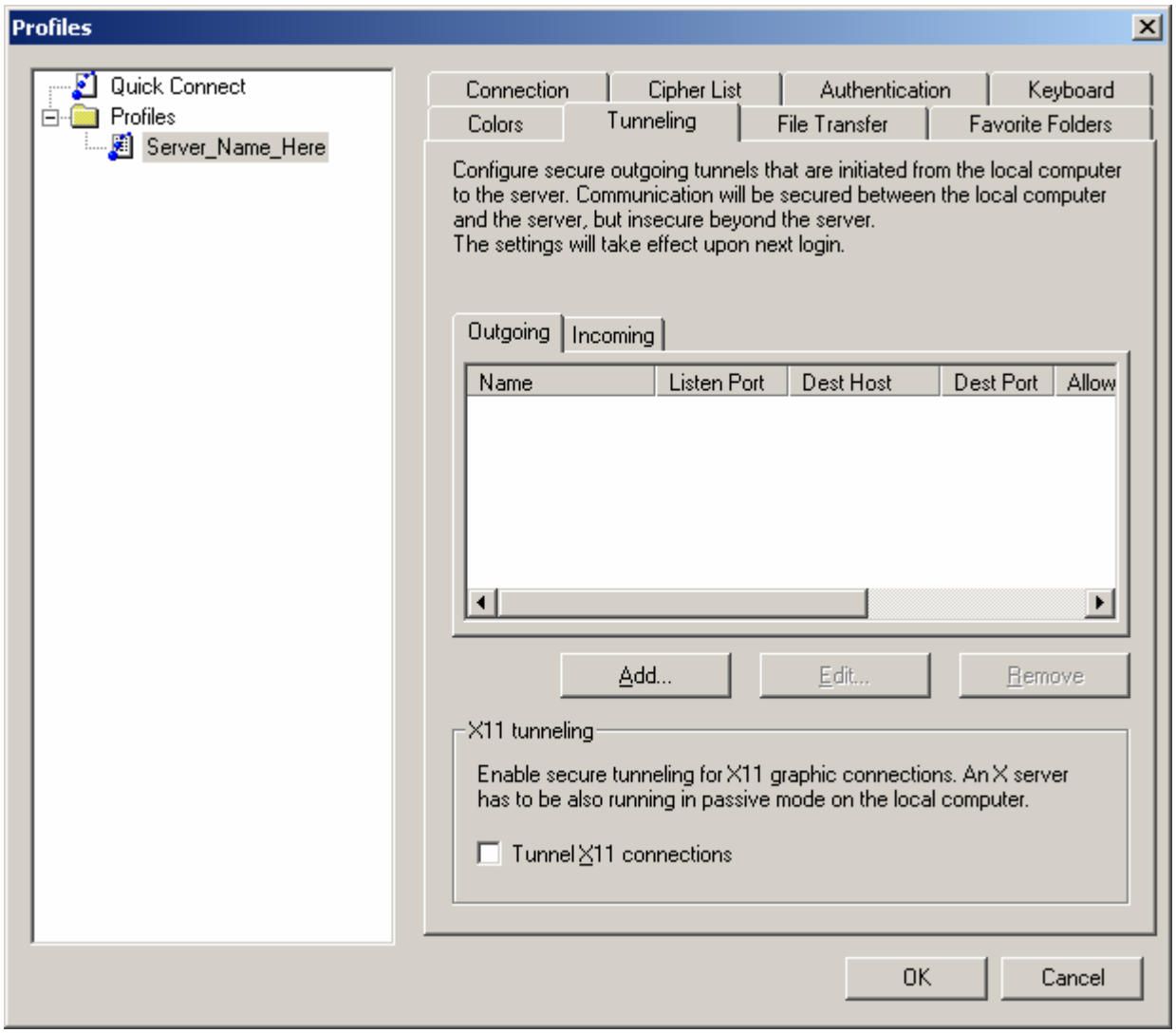
Under the Authentication Tab:

22.6 – Under **Authentication methods**, choose **Password**. Move Password to the TOP of the list using the black arrows.



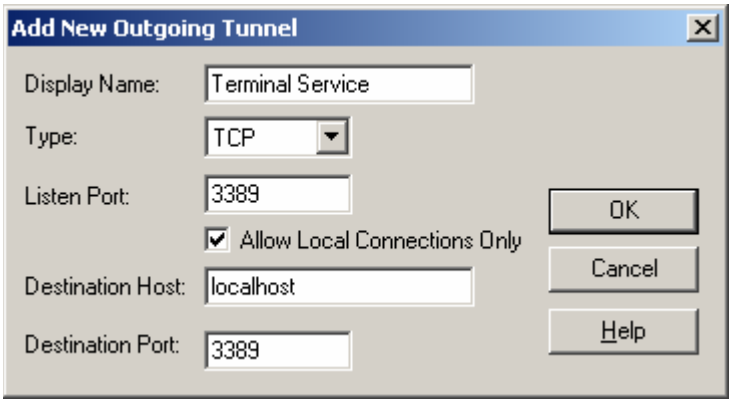
Under the Tunneling Tab:

22.7 – Ensure that the **Outgoing** frame is selected and click on the **Add** button.



22.8 - When the **Add New Outgoing Tunnel** prompt comes up fill in the following information:

Display Name: Terminal Services
Listen Port: 3389
Destination Port: 3389



Click **OK** to complete the Profile Setup.

22.9 – Open the **Profiles** folder and choose the profile that you just created to connect to your server.

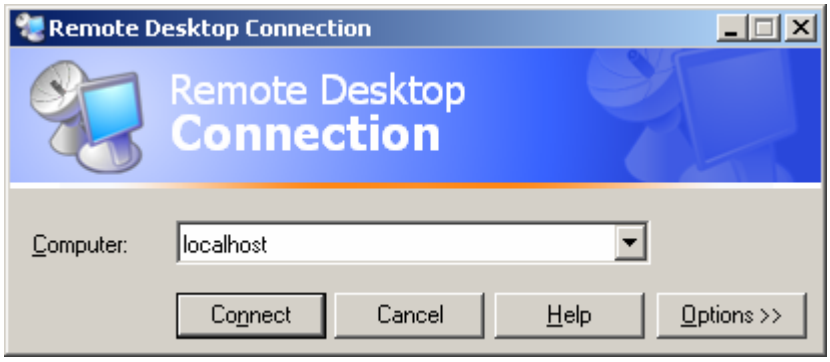
After secure key negotiation, the warning box below will pop up.

Click **OK** to continue.

The Password prompt box will pop up.

22.10 – Enter the correct password and click **OK** to continue.

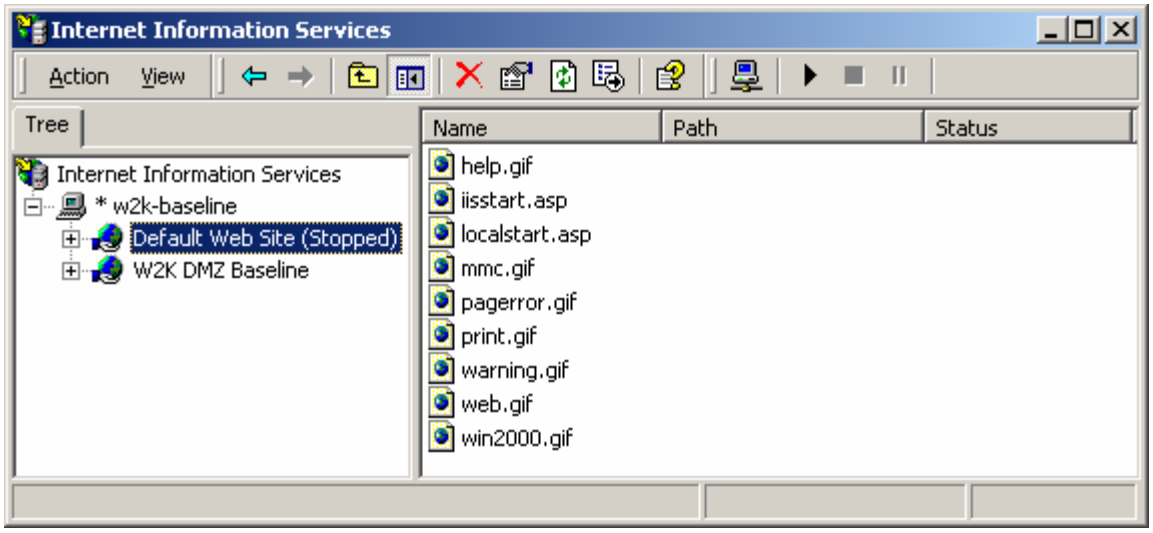
22.11 – After you have successfully authenticated and logged in, open your Terminal Services Client and connect to **Localhost**.



You will now be running Terminal Services over one of the most security-scrutinized protocols ever. This is our **only** approved remote management for W2K Servers in the DMZ.

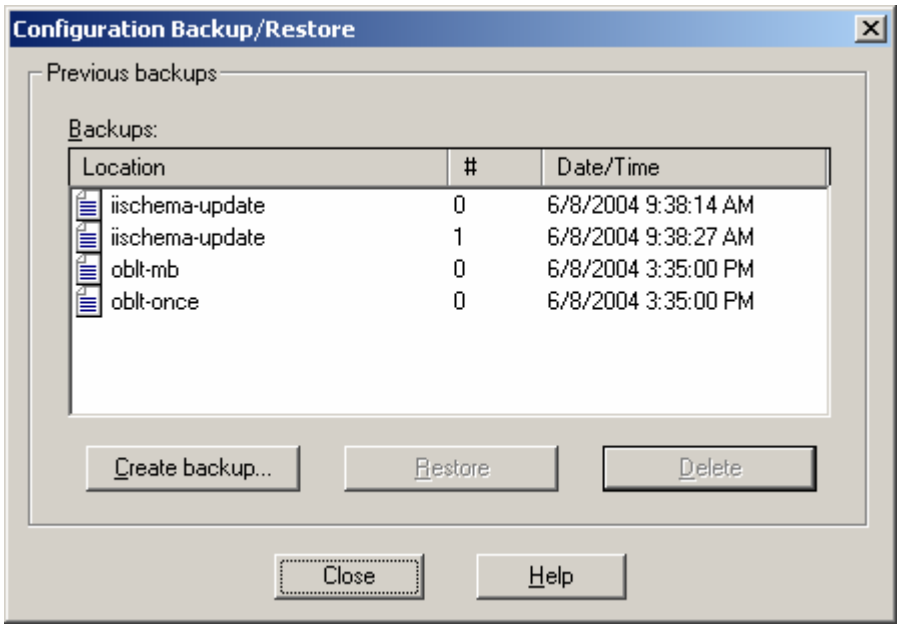
Step 23 – IIS 5.0 Configuration

23.1 – Go to **Start > Programs > Administrative Tools > Internet Service Manager**.



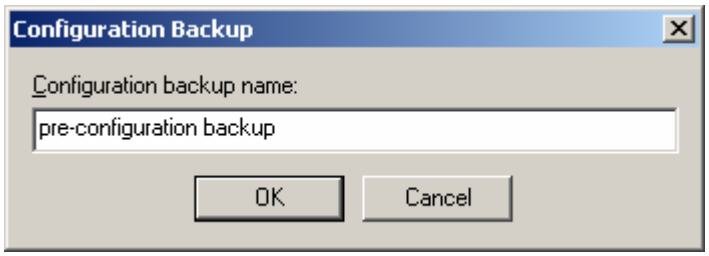
23.2 – Choose the **Default Web Site** and **Stop** it by clicking on the black square on the taskbar.

23.3 – Right click on the PC Icon above and choose **All Tasks > Backup/Restore Configuration**.



23.4 – Select **Create Backup**, name your backup file and click **OK** to complete the task.

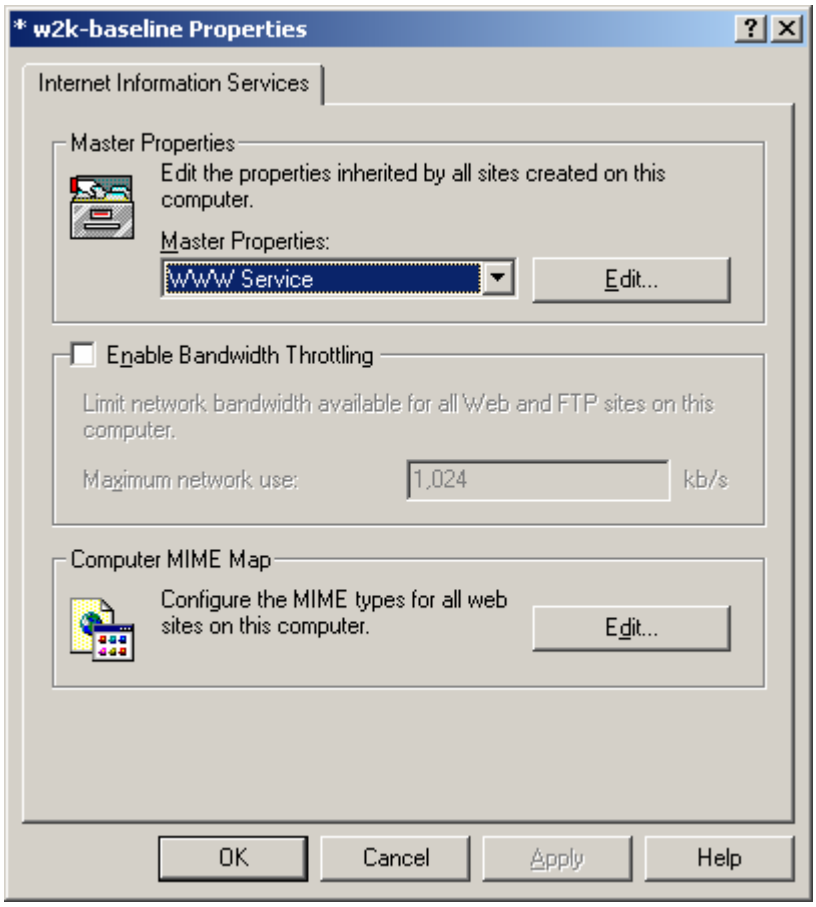
Once completed, you should see the file that you just created in the list.



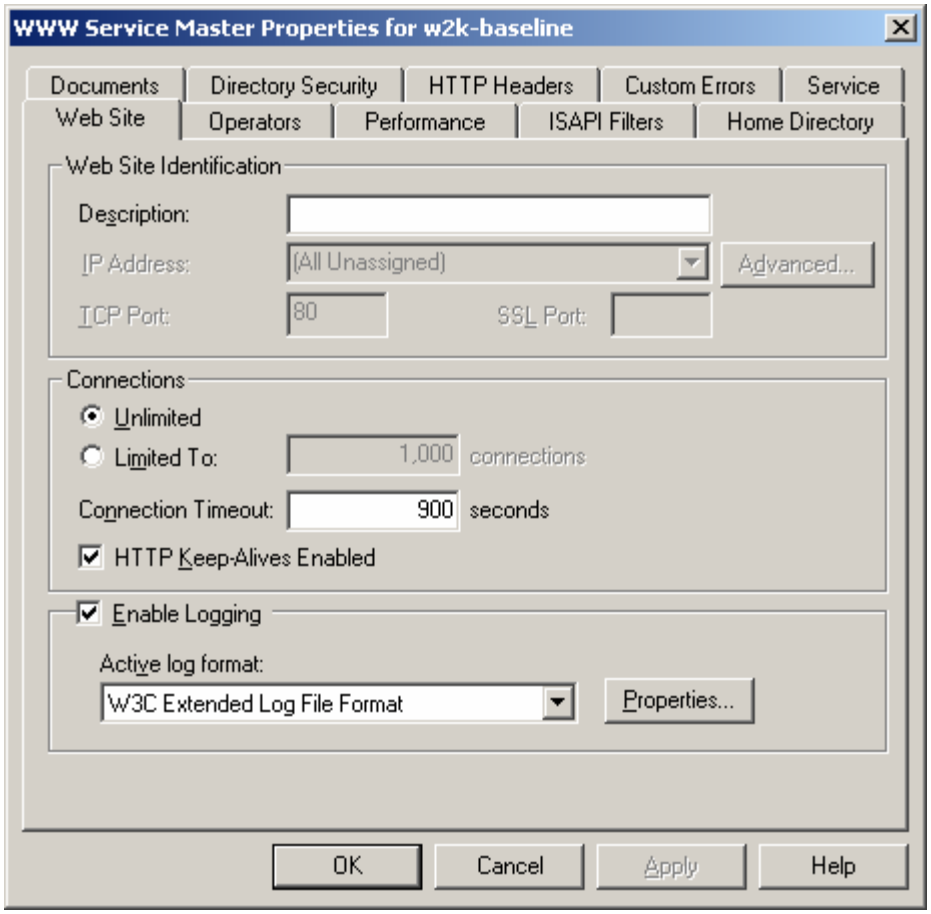
Click **Close** to complete the task and continue.

23.5 – Right click on the computer name within the Internet Services Manager

23.6 – Choose **Properties** and under the Master Properties subsection, ensure that **WWW Service** is selected and click **Edit**.



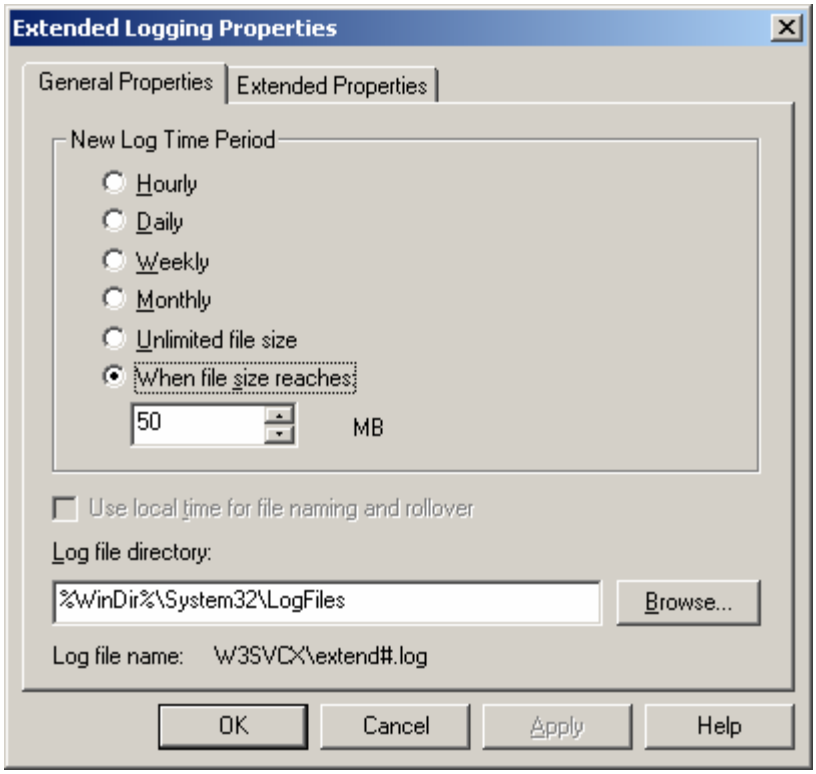
23.7 – Choose **Properties** > Edit The Master Properties For The **WWW Service**.



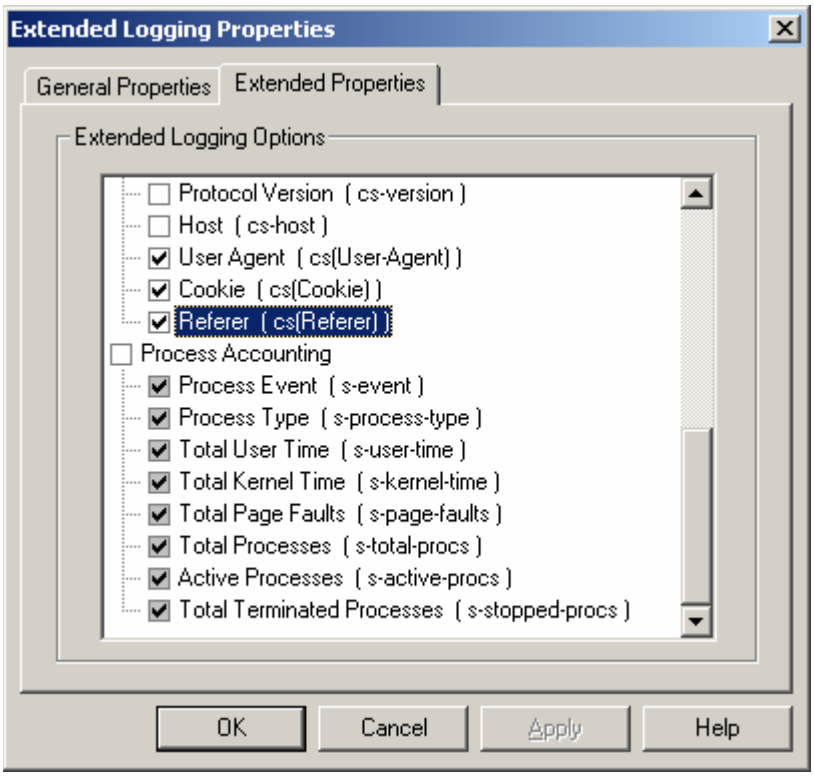
Under the Web Site Tab:

23.8 – Ensure that the **Enable Logging** box is checked and is in **W3C Extended Log File Format.** Click on **Properties.**

23.9 – Change the **New Log Time Period** to **When The File Reaches 50** MB and click **OK**.

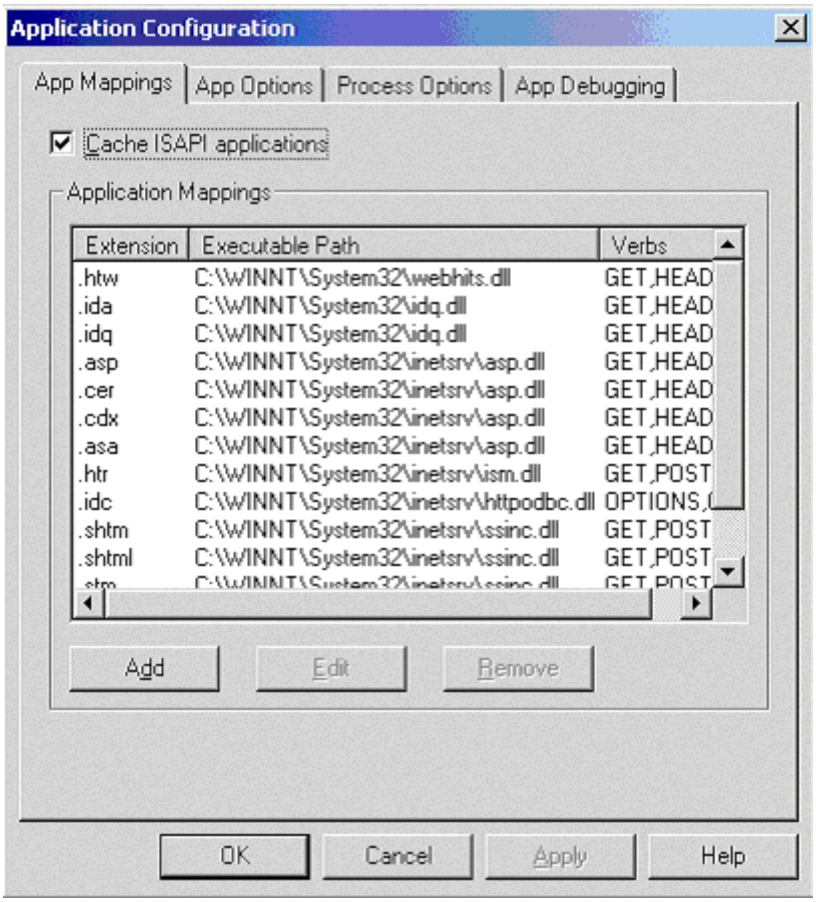


23.10 – Click on the **Extended Properties** Tab and add checks for **Cookie** and **Referrer** and click **OK**.



Under the **Home Directory** Tab

23.11 – Under the **Application Settings** subsection, choose **Configuration**.



23.12 - Remove all Application Extensions, as referenced below:

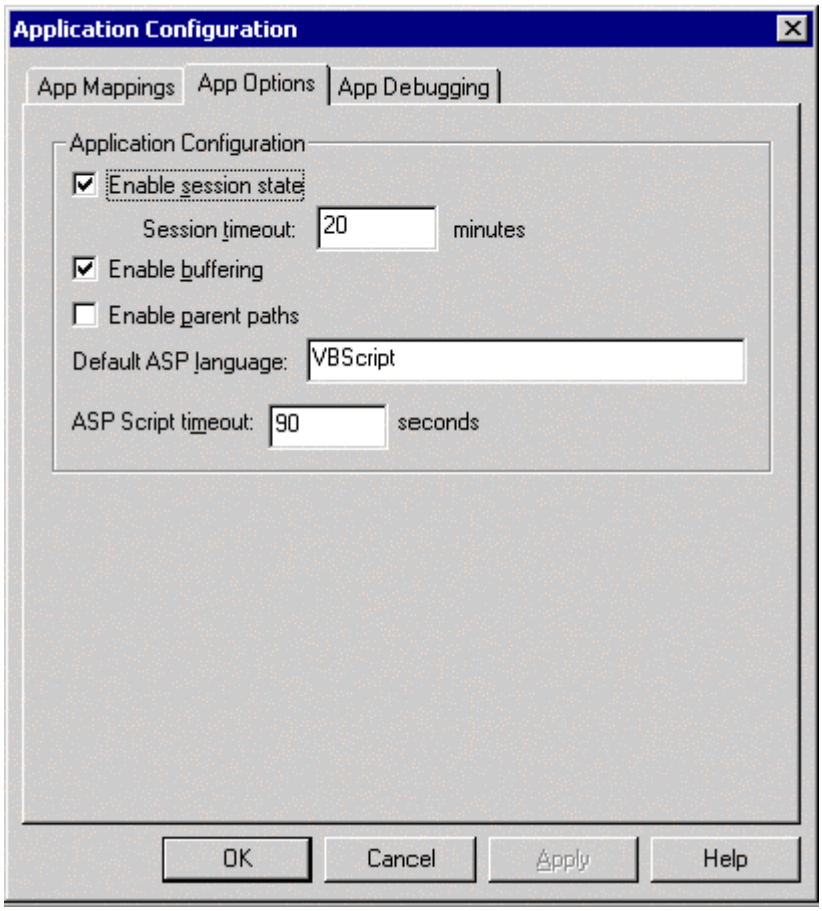
Extension	Filetype
.asa	ASP files to declare objects with session or application scope
.asp	Active server pages
.bat	Batch files
.cdx	Scripts to create Channel Definition files
.cer	Scripts for digital certificates
.htr	Scripts for remote password change
.htw	Index server hit highlighting
.ida	Index server performance monitoring
.idc	Internet Dbase connection
.idq	Index server query definition
.printer	Internet Printing
.shtm , .shtml, .stm	Server Side Includes

NOTE: Remove them **ALL** and add back in as needed but only for a known specific purpose.

23.13 – For the remaining extensions, consider limiting the HTTP verbs the extension will accept. Instead of using all the verbs (DELETE, GET, HEAD, PUT, and TRACE), use only GET for static Web pages and PUT if you have forms on your site; this way we explicitly allow only the minimum actions needed per extension.

Under the **App Options** Tab

23.14 - Uncheck **Enable parent paths**.



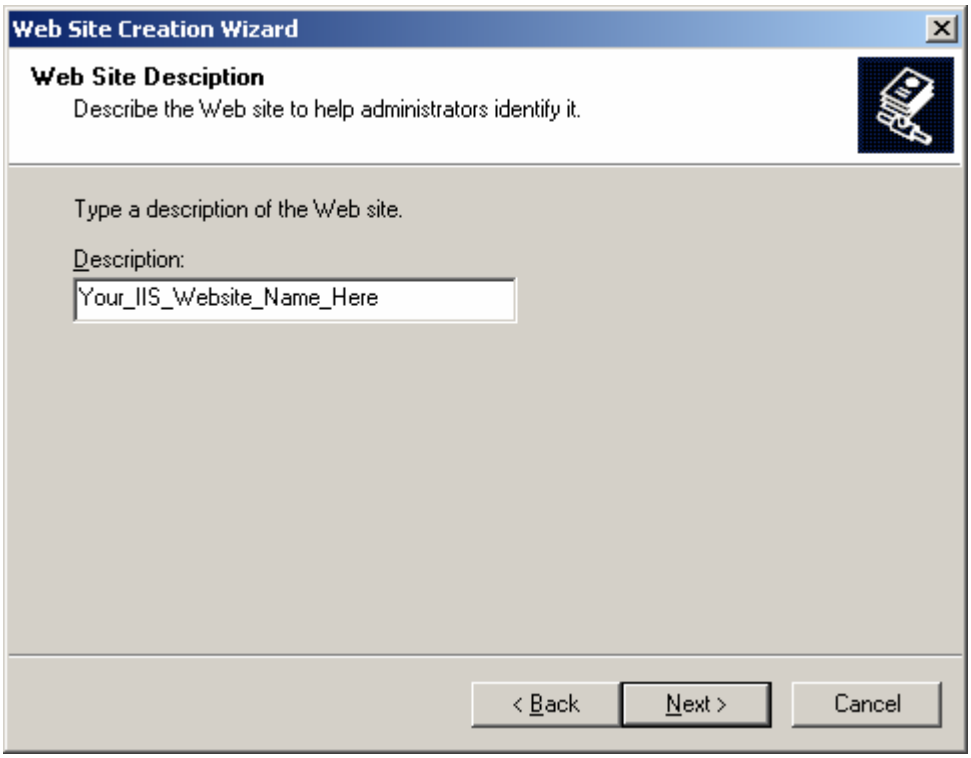
23.15 – Click **OK** to close the Website Properties window.

23.16 – Click **OK** to get out of edit mode.

23.17 – Highlight the PC icon, right mouse click and select **New** > **Web Site**.

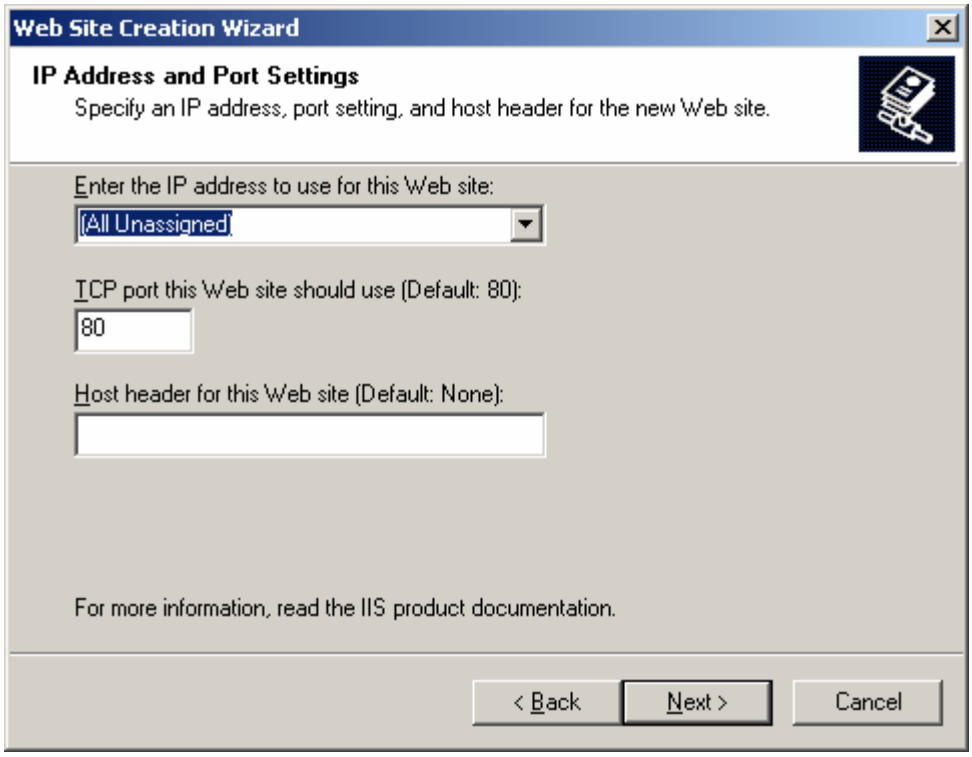
Click **Next** to continue

23.18 - Give your Web Site a Description



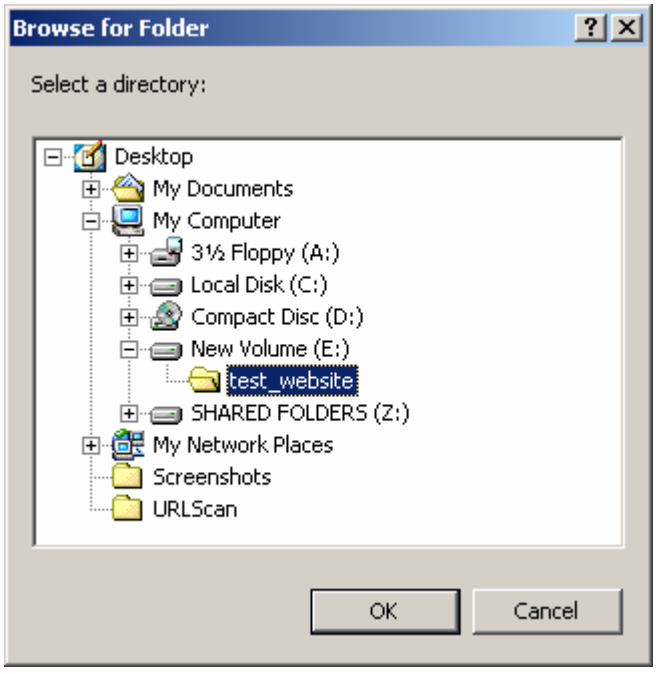
Click **Next** to continue

23.19 – Add the **IP address** and **Port Number** (the defaults are usually appropriate).

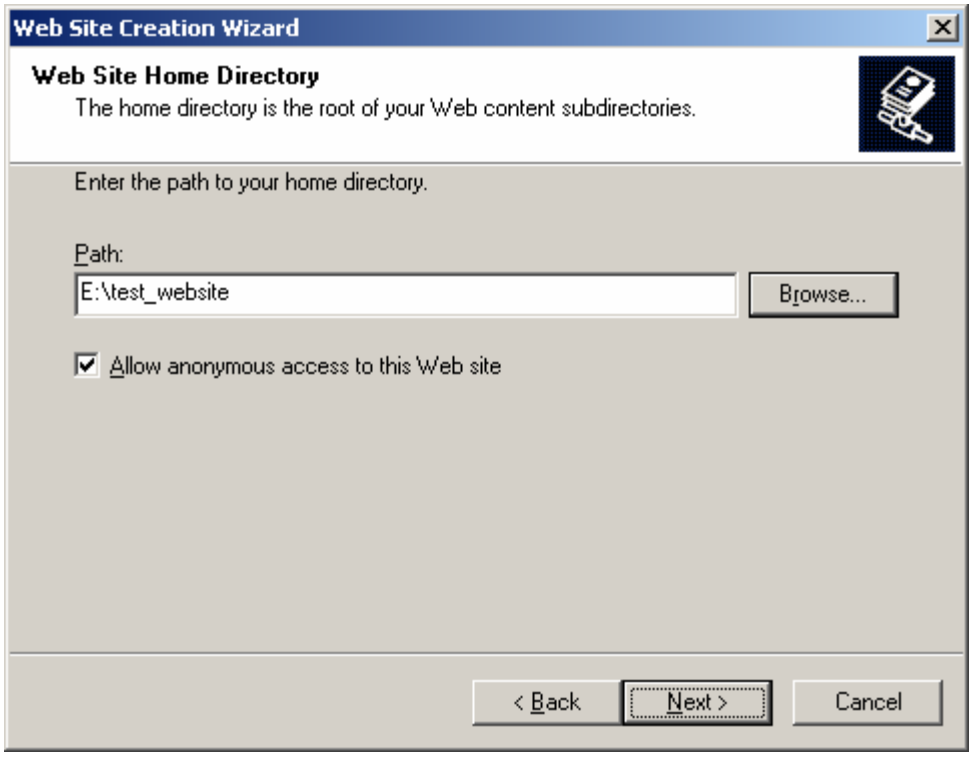


Click **Next** to continue

23.20 – Choose a drive that is **NOT** your system partition for the path of your new web site. You will have to click on **Browse**, **select the drive** and **create a new directory**.

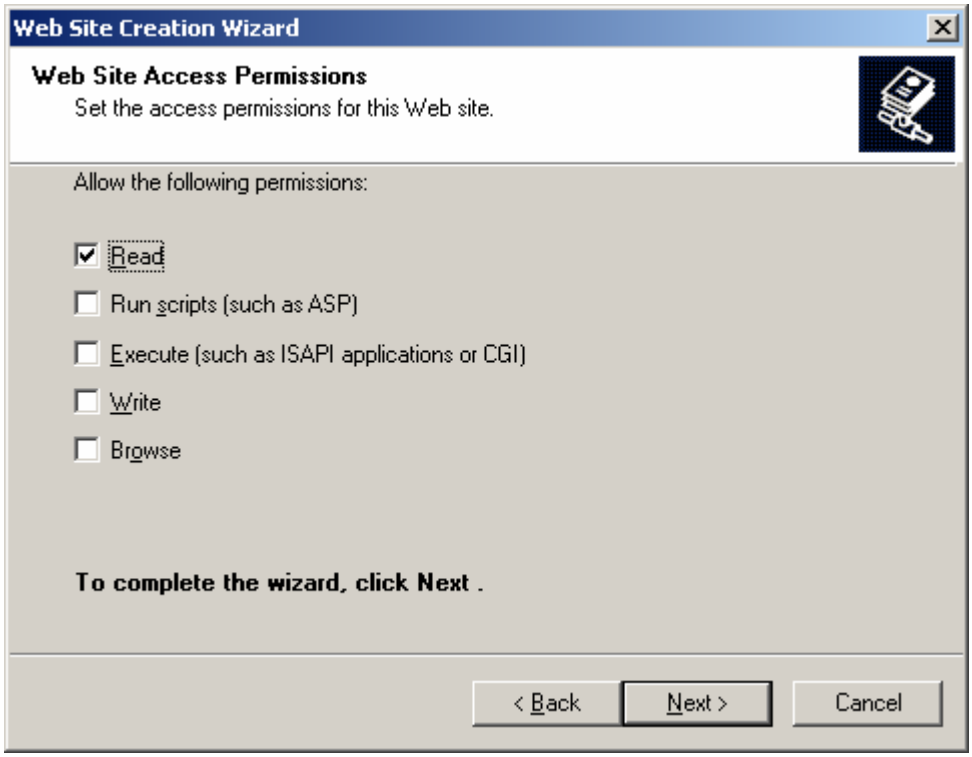


23.21 – Click **OK** to select the newly created directory.



Click **Next** to continue

23.22 – Choose the minimum set of permissions here for your web site by un-checking the **Run scripts (such as ASP)** box.



Click **Next** to continue

23.23 – Click **Finish** to complete the Web Site Creation Wizard

23.24 – (**Optional**) Microsoft recommends configuring a separate directory for each file type so that you can easily set ACLs. Best Practice:

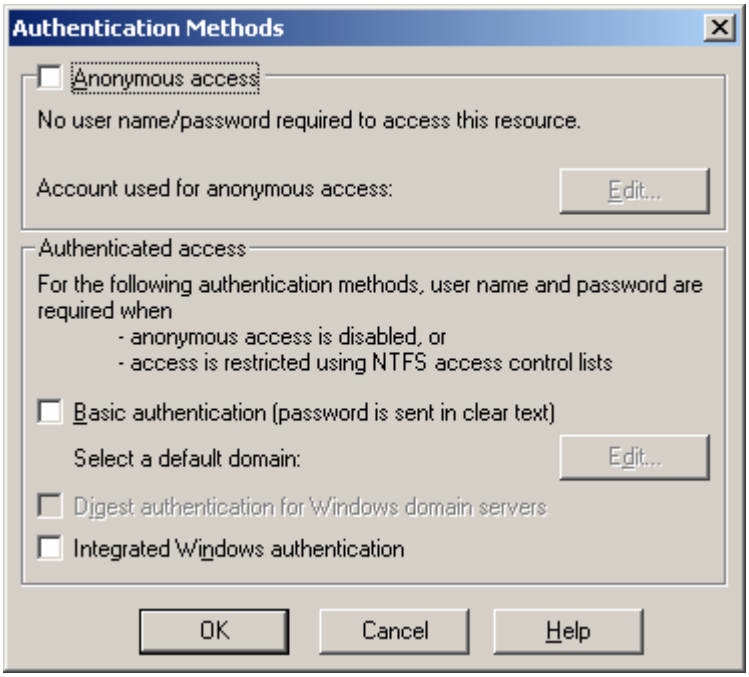
This is a good idea if you have the ability to do so. For example, if your website base directory was E:\test_website then you would setup your web site such as:

E:\test_website\static (.htm, .html)
E:\test_website\include (.inc)
E:\test_website\script (.asp, .pl, .cgi)
E:\test_website\bin (.dll) - VisualStudio likes bin when building projects.
E:\test_website\images (.gif, .jpg, .jpeg)

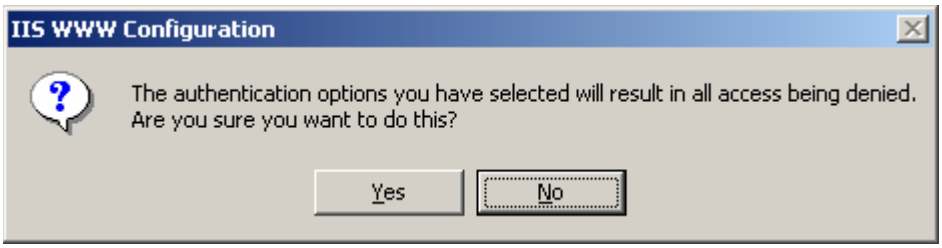
23.25 – Disable the Default Web Site. It is better to disable the default web site rather than remove it as it may come in handy later.

23.26 – Right click on the **Default Web Site**. Select **Properties > Directory Security > Authentication and Access Control > Edit**

23.27 – **Uncheck** all the boxes.



You will receive a warning box as shown:



23.28 – Select **Yes**

23.29 – Click **OK** to complete the task.

23.30 – Check for and remove all IIS Sample Directories

- **Admin Scripts** C:\InetPub\AdminScripts
- **IIS Help** C:\Windows\help\iisHelp
- **IIS admpwd** C:\Windows\System32\inetsrv\iisadmpwd

Remove Internet Printing

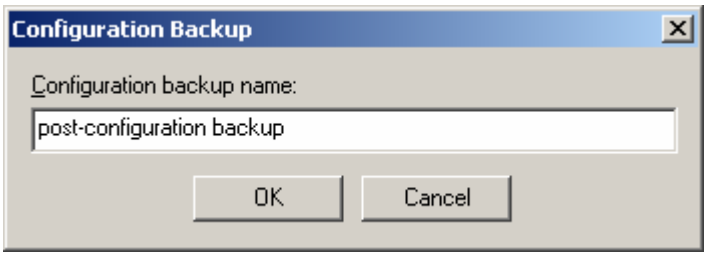
23.31 – Delete the printer's virtual directory at C:\Windows\web\printers

Back up the Metabase again

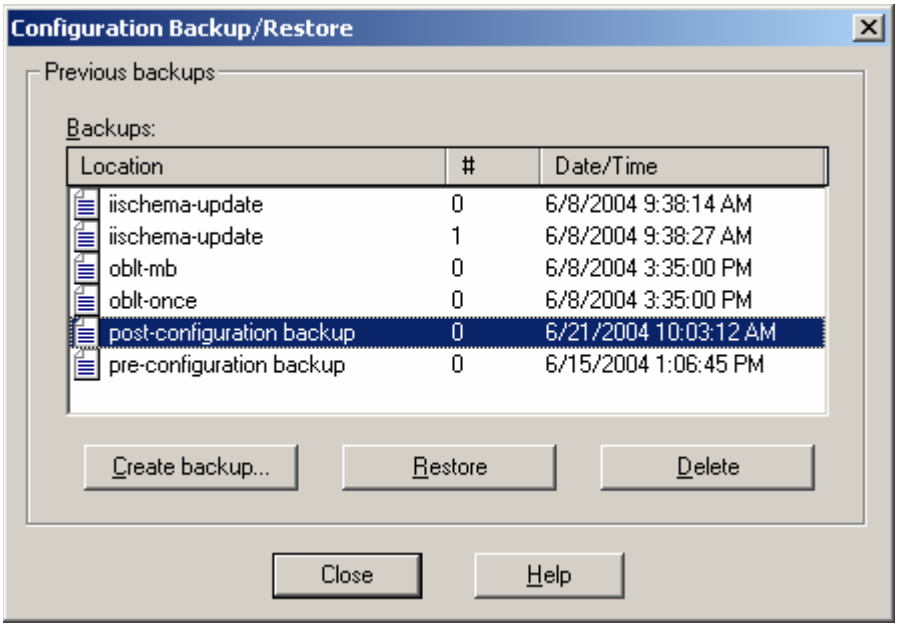
23.32 - Go to **Start > Programs > Administrative Tools > Internet Service Manager**.
[ss]

23.33 – Right click on the PC Icon above and choose **All Tasks > Backup/Restore Configuration**.
[ss]

23.34 – Select **Create Backup**, name your backup file and click **OK** to complete the task.



Once completed, you should see the pre and post configuration files that you created in the list.



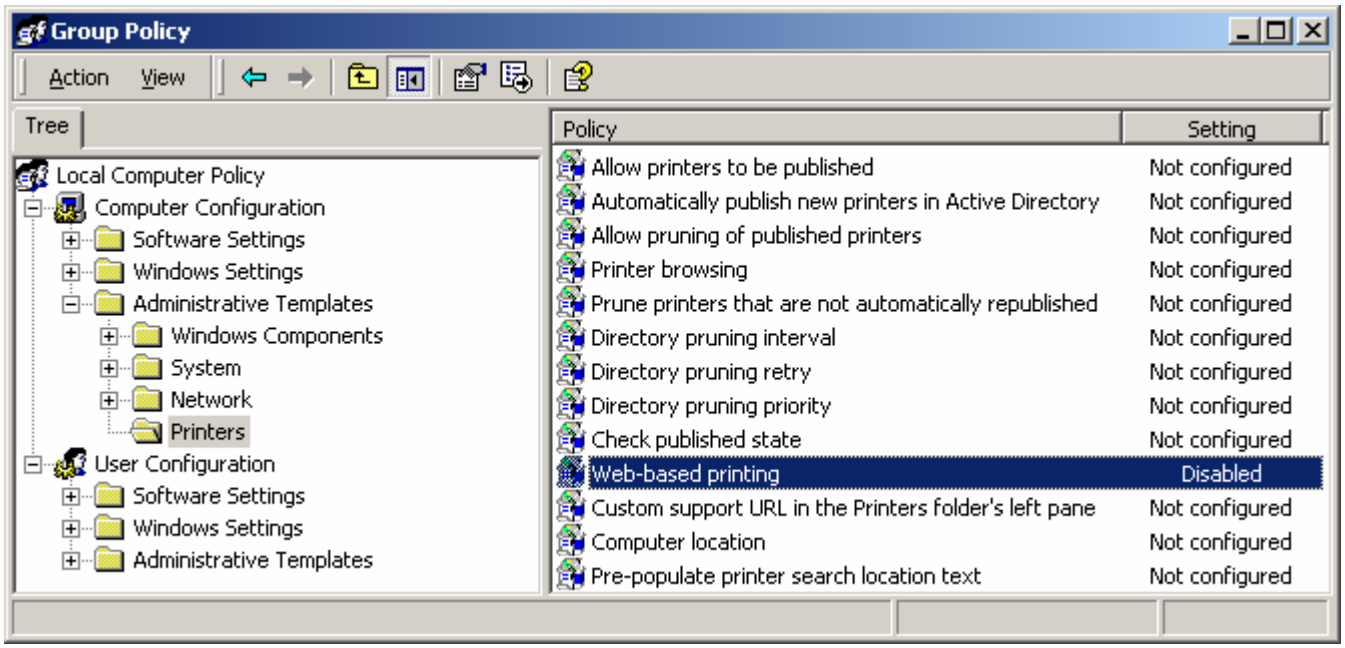
Click **Close** to complete the task and continue.

Disable Web Based Printing - Internet printing can automatically re-appear. To stop this,

23.35 – Go to **Start** > **Run** > **gpedit.msc**

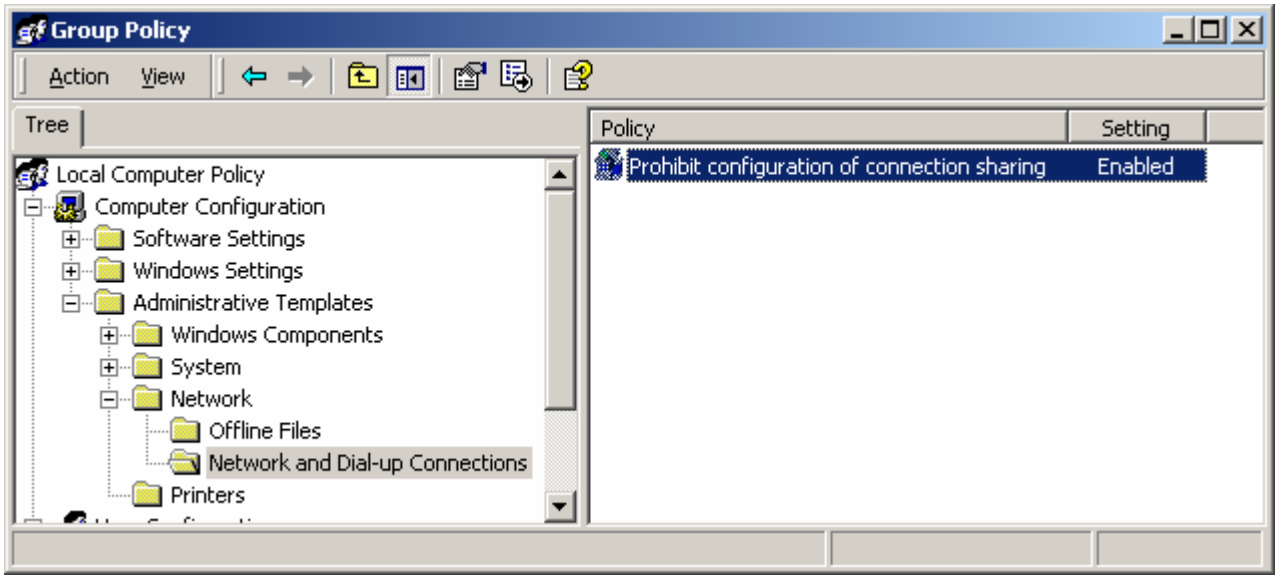
Under **Computer Configuration > Administrative Templates > Printers**

23.36 – Change **Web Based Printing** to disabled.



Under **Network** > **Network Configuration**

23.37 – Change the value for **Prohibit use of Internet Connection Sharing on your DNS Domain Network** to enabled by right clicking and choosing **Enable**.



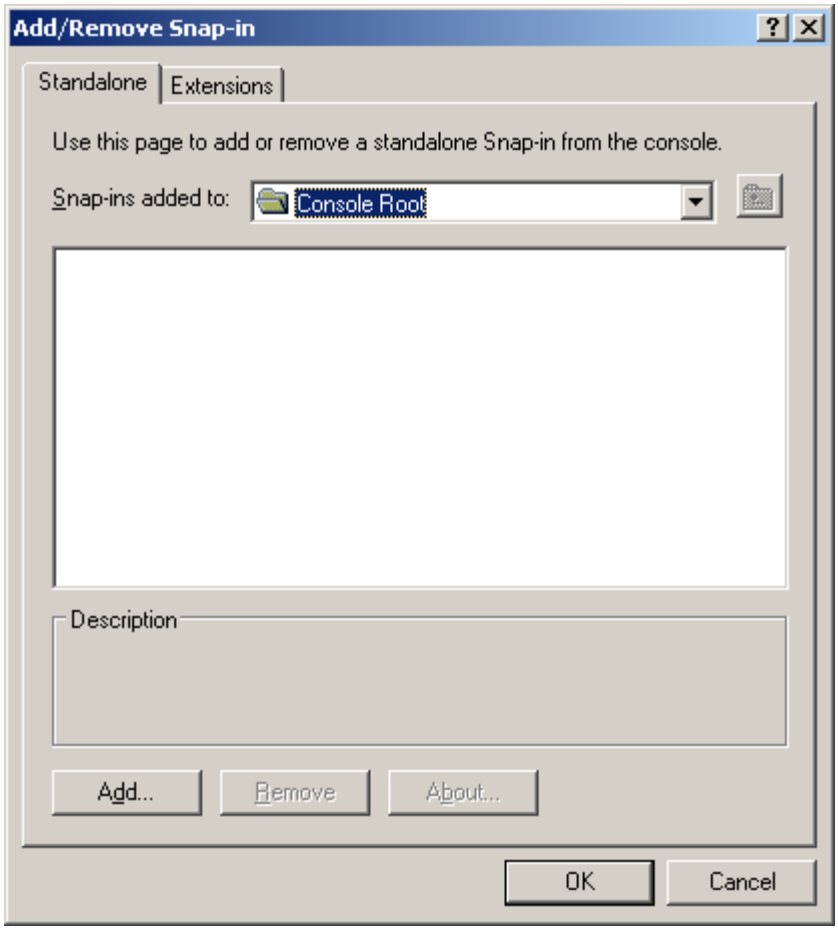
Right click on **My Computer > Manage**

Step 24 – Applying the High Security Web Server .inf file

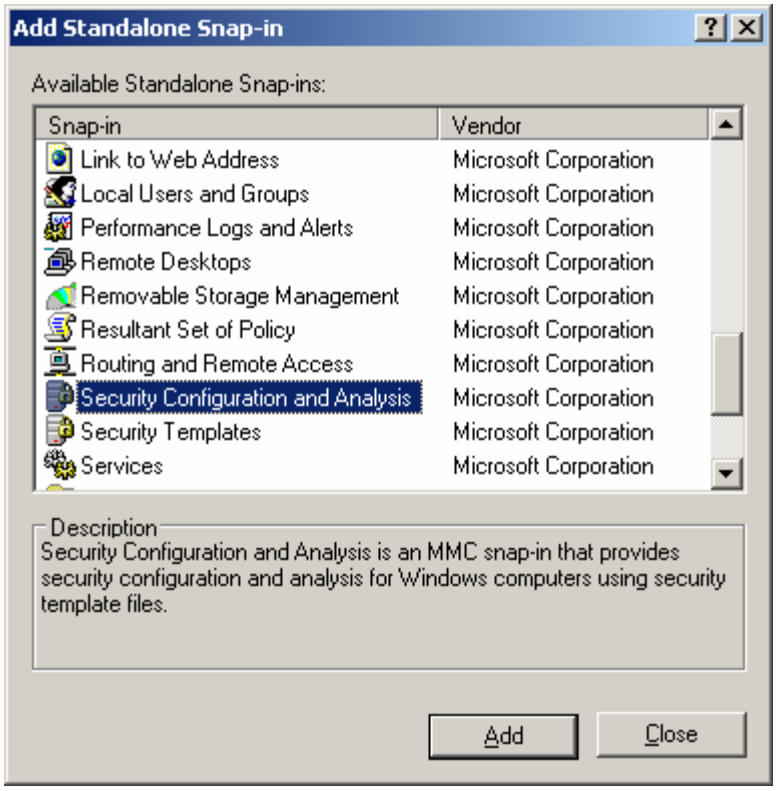
24.1 – Download the www-w2k-dmz.inf file to your desktop.

24.2 – Go to **Start** > **Run** > **MMC**

24.3 – Click on **File > Add/Remove Snap In**



24.4 – Click on the **Add** button and scroll down to **Security Configuration and Analysis**

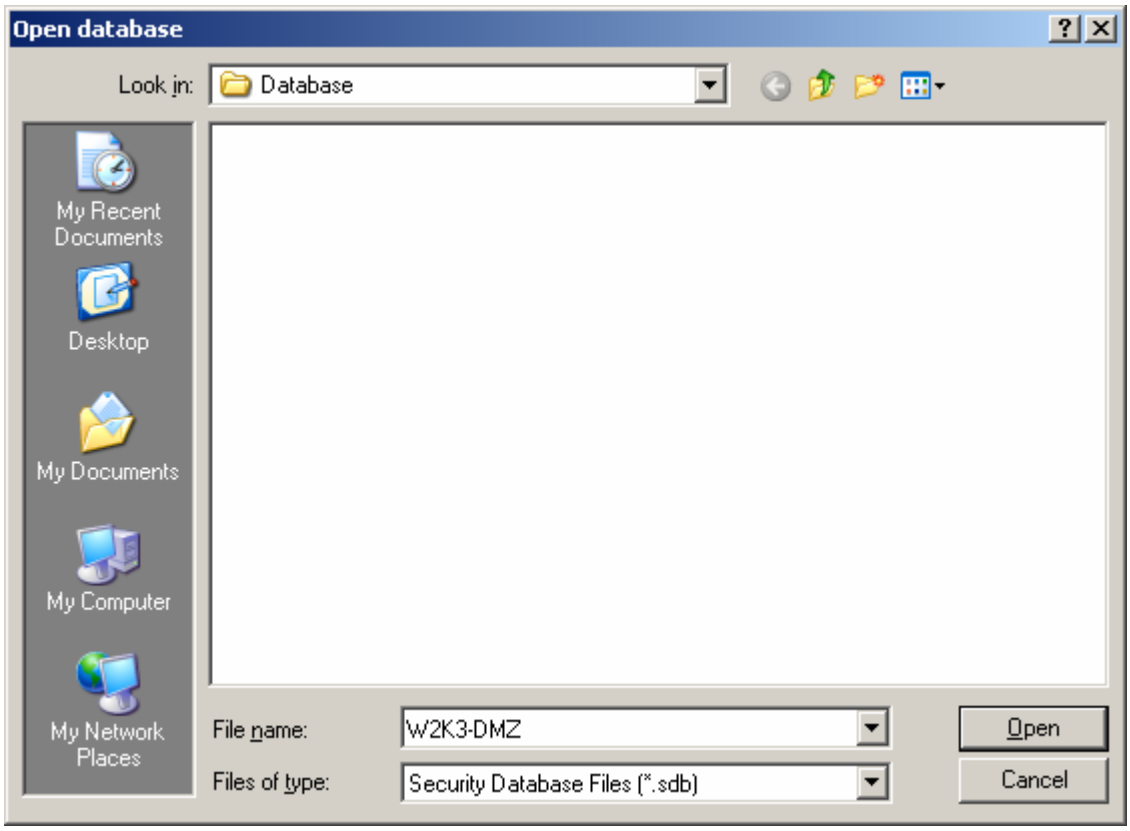


24.5 – Click the **Add** button then Click the **Close** button

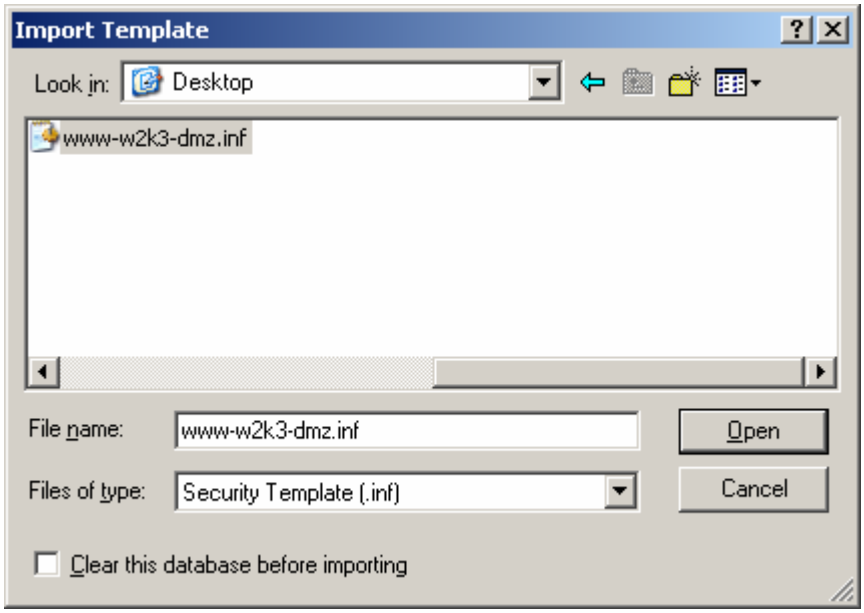
24.6 – Click the **OK** button on the **Add/Remove Snap In** window to continue.

24.7 – In the Left Pane, right click on **Security Configuration and Analysis** and choose **Open Database**

21.8 – Navigate to the **C:\WINNT\Security\Database** directory and give your database a name in the form ***LOCALSERVERNAME_SECPOL_LGPO*** and click **Open**



This will open another pop-up box asking for the template file.

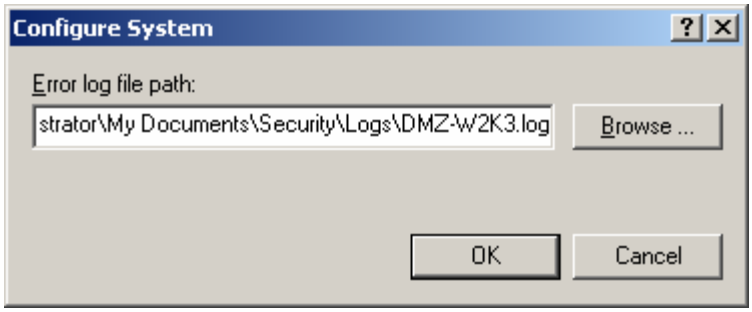


24.9 – Navigate to your Desktop and type in the name of the .inf file that you previously downloaded.

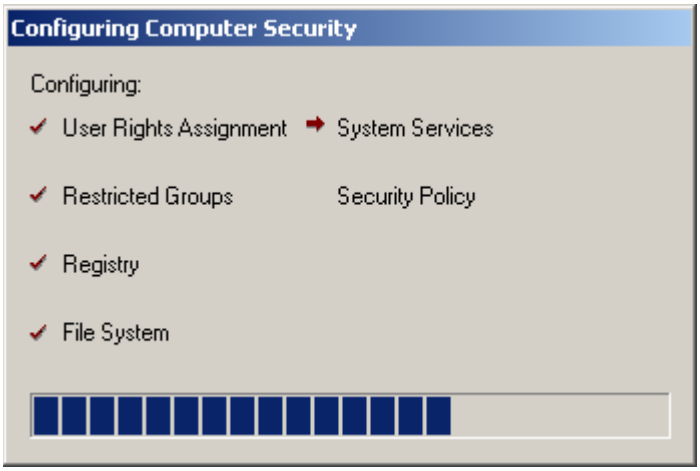
24.10 – Click **Open** to continue.

24.11 – Right click on **Security Configuration and Analysis** and choose **Configure computer now**.

24.12 – This will pop up a box asking where you wish to write the log file. You can choose the default and click ok.



The computer will now apply the INF file



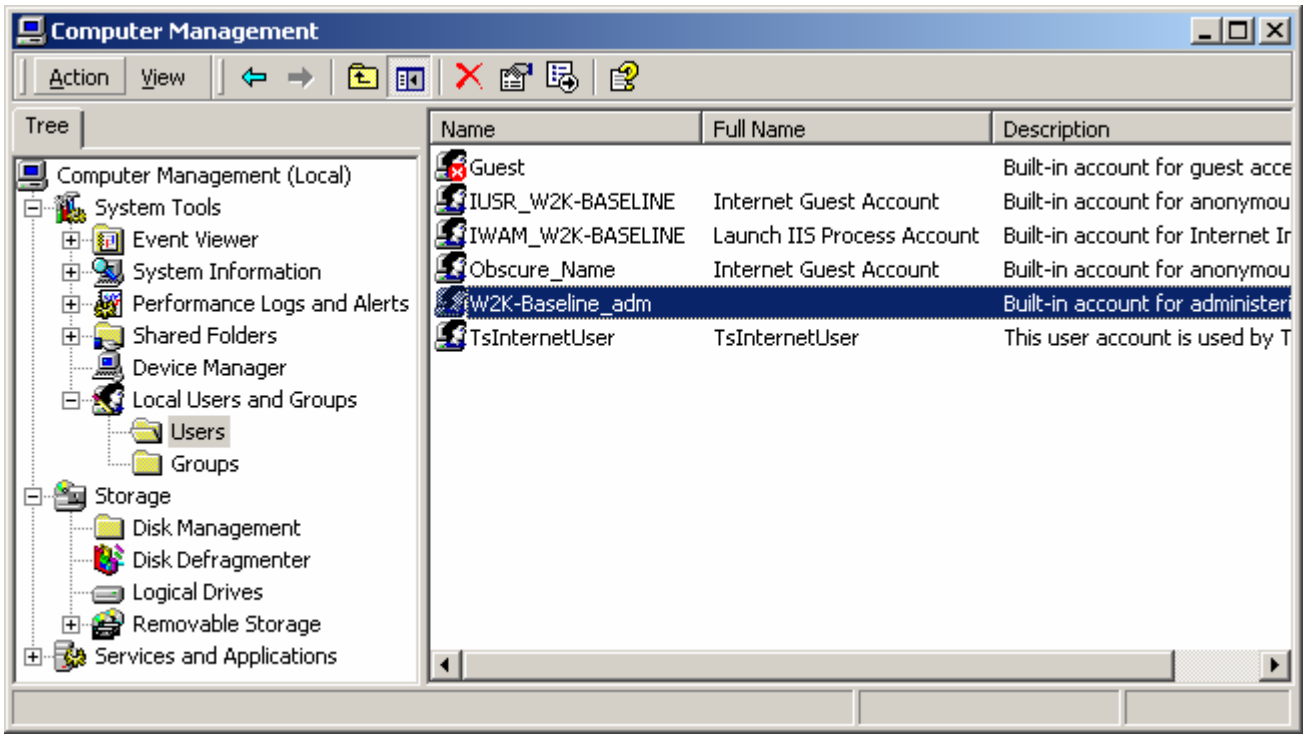
24.13 – When the configuration is done, you can close the Console1 window.

Step 25 - Rename and change the password to the IUSR_<*machinename*> account.

25.1 – From the Desktop, right click on **My Computer > Manage**

25.2 – Double click on **Local Users and Groups** and choose the **Users** folder. In the right pane, choose the **Administrator** account. Right click and rename this account using the syntax **<*machinename*>_adm**

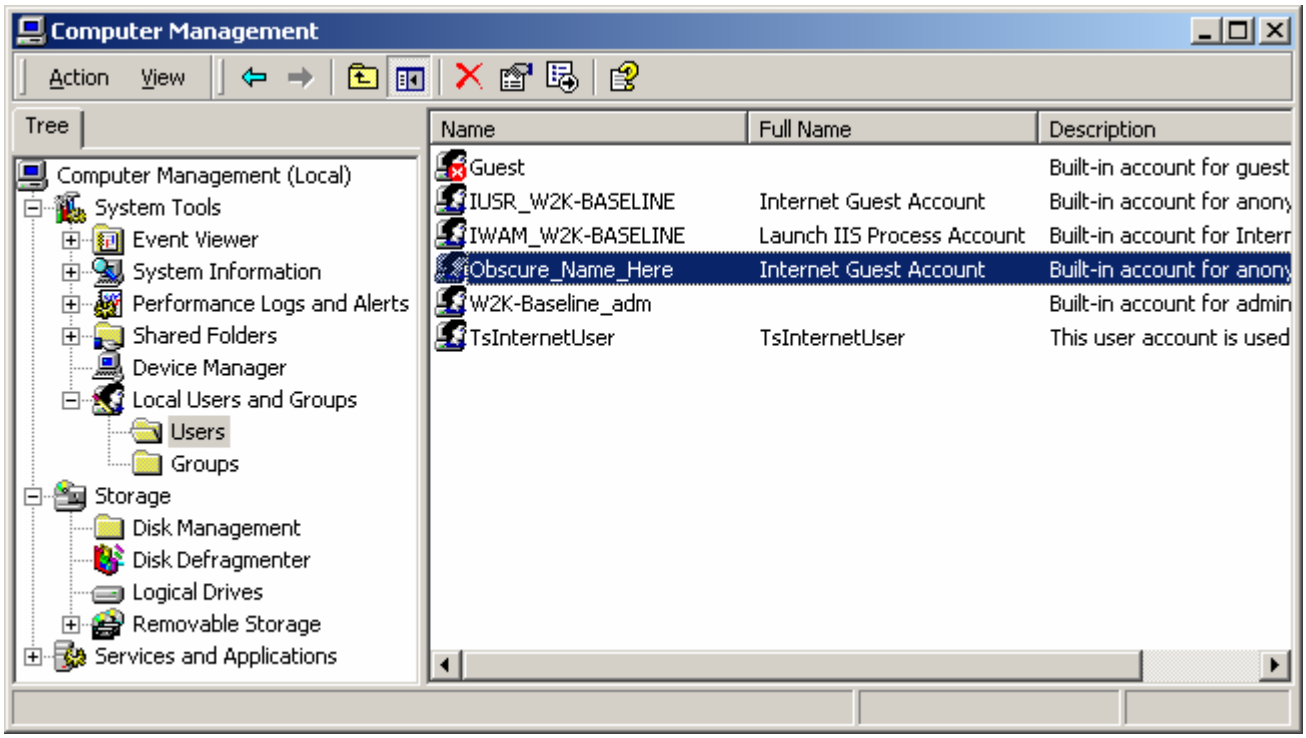
Example: the name of the machine is DMZ-Baseline, so the newly renamed Administrator account would be **DMZ-Baseline_adm**



25.3 – Choose the **IUSR_<*machinename*>** account.

25.4 – Right click and **rename this account to an obscure name**. (Remember this new name, you will need it later in **Step 27.6**). Note that, even though you rename the **IUSR_<*machinename*>** account, it will show up again in the list of local users. You should right click on the regenerated **IUSR_<*machinename*>** account, and disable it. It is safe to ignore it after performing this step.

25.5 – Refer back to **22.5** and change the **User name** to match the name in **Step 25.2**.



25.6 – Right click on this newly renamed account and choose **Set Password**. (Remember this password, you will need it later in **Step 27.7**).

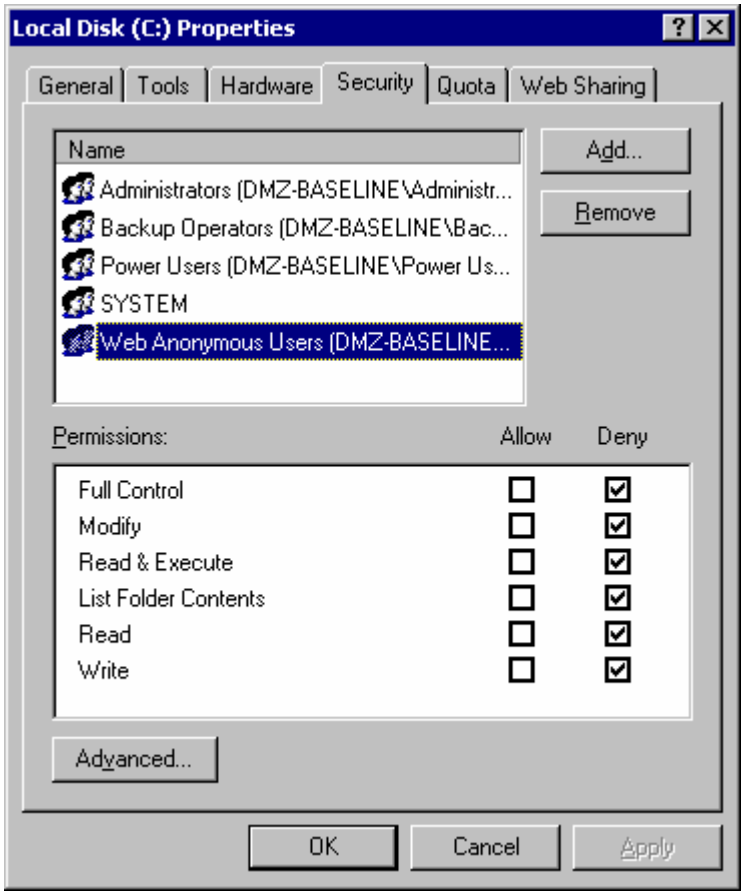
25.7 – You can now close the Computer Management window.

Step 26 - NTFS Permissions

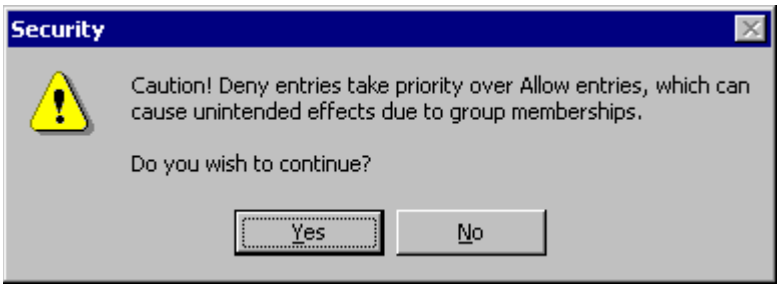
26.1 – Double click on **My Computer**

26.2 – Right click on the C:\ drive and choose **Properties > Security**

26.3 – Ensure that the **Web Anonymous Users** Group is highlighted

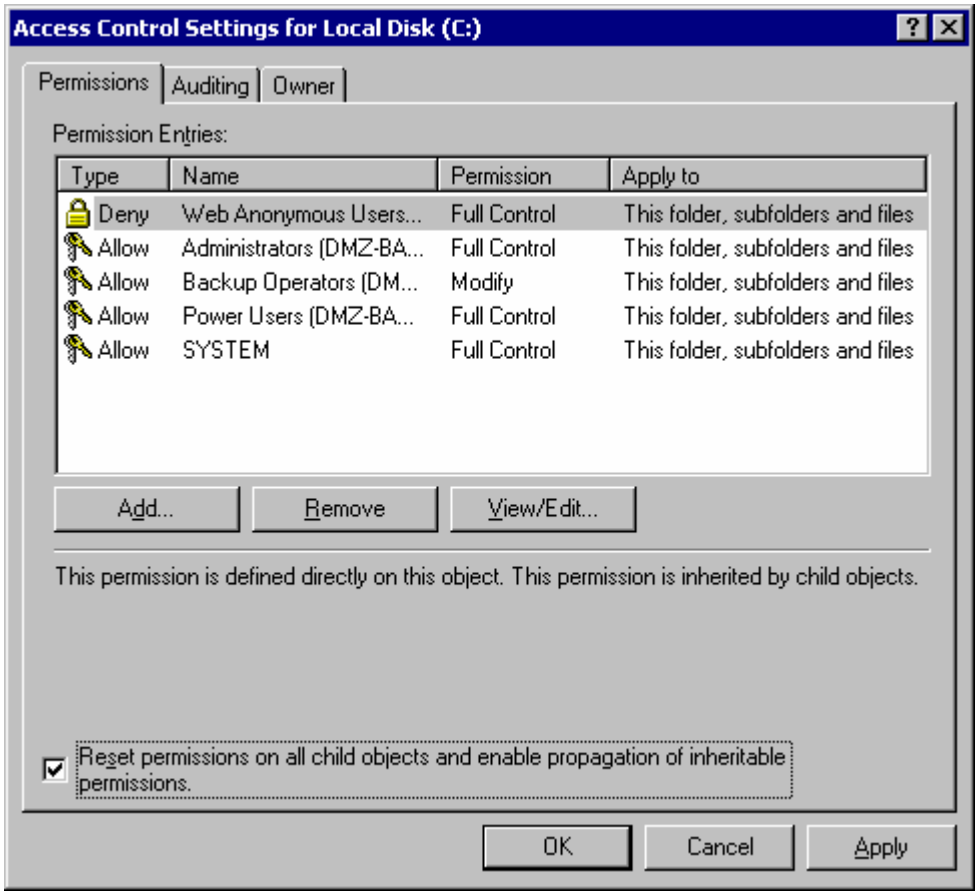


26.4 – Choose **Deny Full Control**. A pop up box will appear:



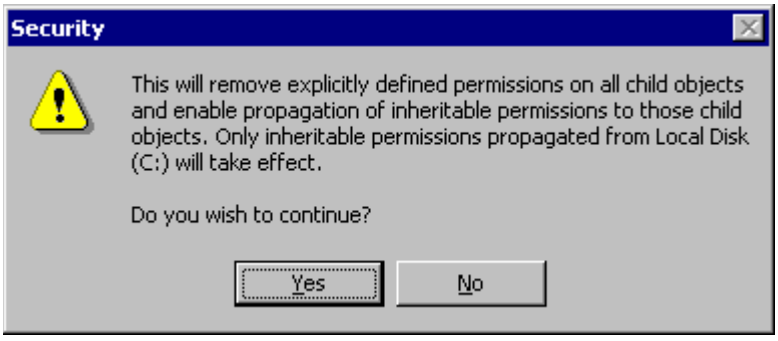
26.5 – Choose **Yes** and then click on the **Advanced** button.

This will bring up the Access Control Settings for Local Disk C:\



26.6 – Place a check mark in the "**Reset permission on all child objects and enable propagation of inheritable permissions**."

This will bring up another pop-up warning box:



Click **Yes** to continue. You can ignore any Pagefile warnings.

26.7 – Repeat these steps for all other volumes.

26.8 – For each path in the below table, repeat the **Steps 26.9 – 26.18** below.

IMPORTANT: Note which folders to apply the permissions to. The 1st column is the directory that you should navigate to and the 2nd column is the collection of folders and files that you should apply these permissions onto.

Directory	**Apply onto**

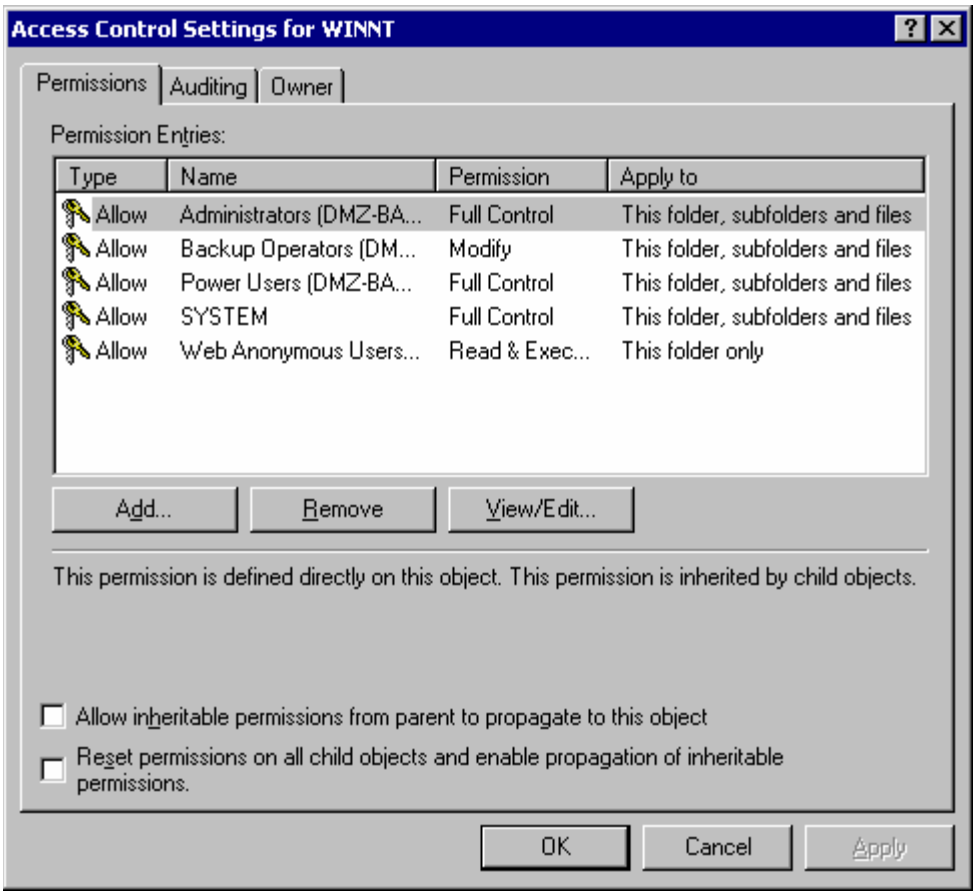
C:\WINNT	This Folder Only
C:\WINNT\System32	This Folder Only
C:\WINNT\System32\inetsrv	This Folder Only
C:\Program Files\Common Files	This Folder, Subfolders and Files
E:*path_to_your_IIS_installation*	This Folder, Subfolders and Files

I'll walk you through the first instance:

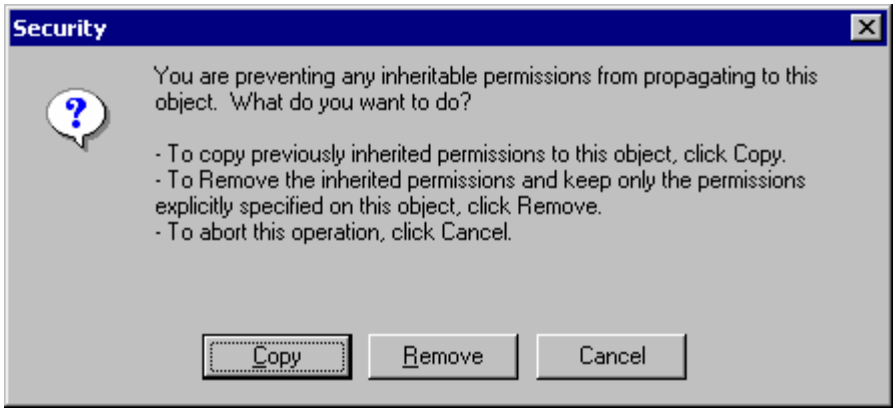
26.9 – Navigate to **C:\WINNT**, **Right click** on the Directory and select **Properties**

26.10 – Click the **Security** Tab and then click on the **Advanced** button

26.11 – Uncheck the "**Allow inheritable permissions to propagate to this object**" box.



This will bring up a **Security** box.



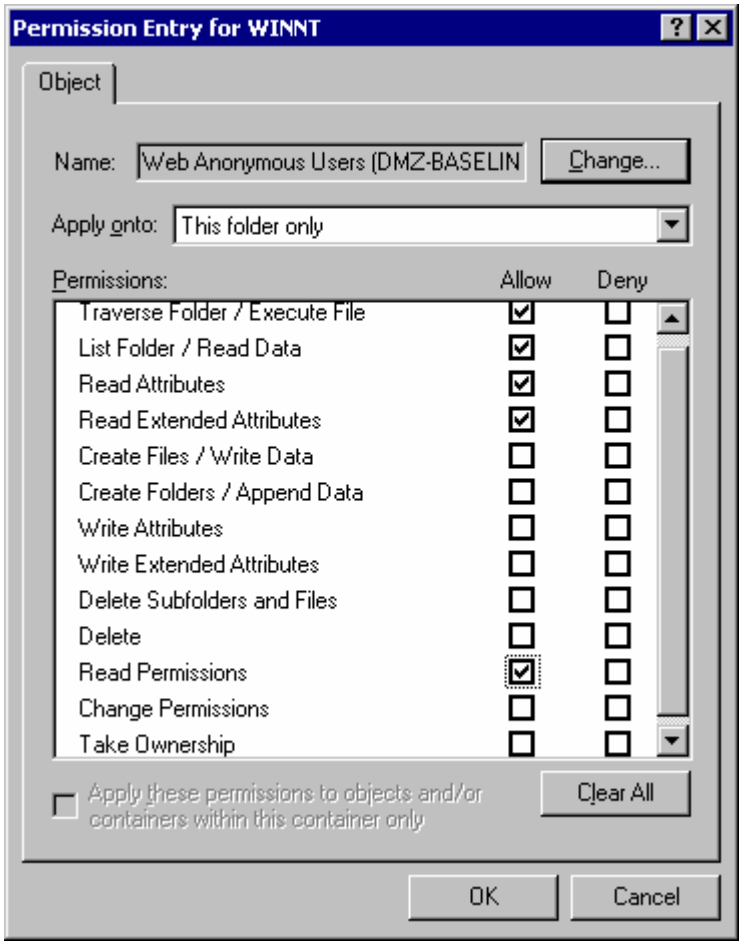
Choose **Copy** and you will be able to edit the permissions

26.12 – Highlight the **Web Anonymous Users** group and click **View/Edit**

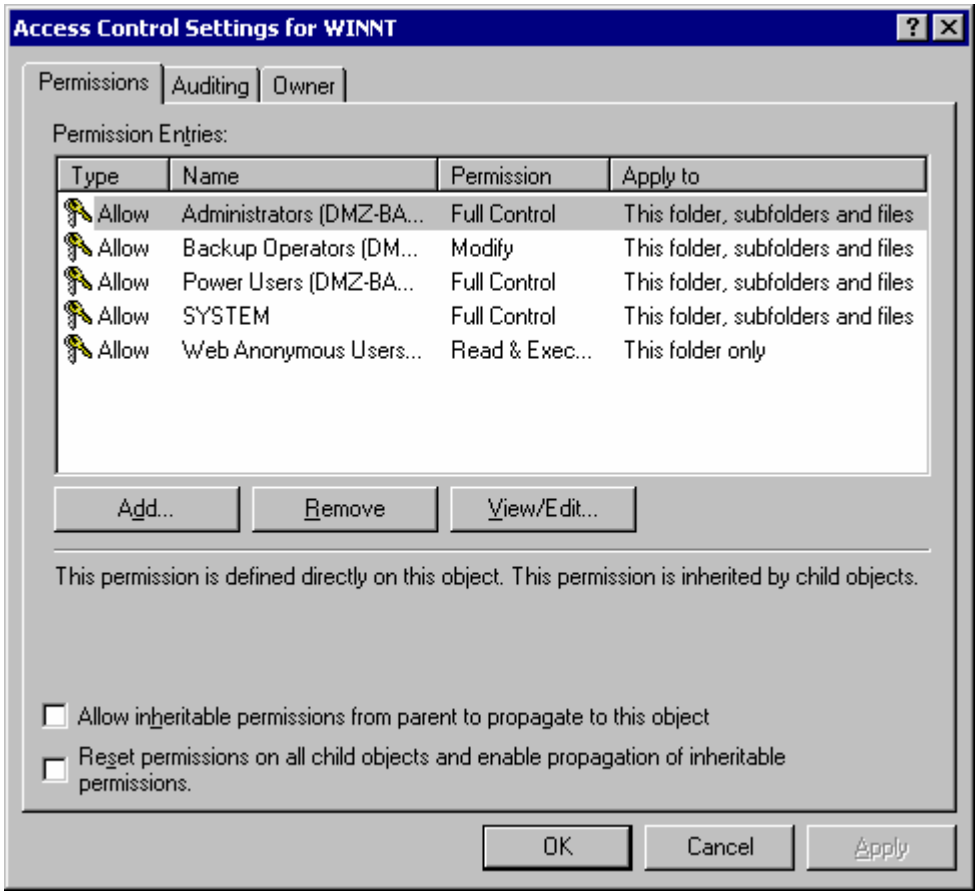
26.13 – Under **Apply onto:** select **This folder only** from the drop down box

26.14 – Click the **Clear All** button and give individual permissions to:

- Traverse Folder / Execute File
- List Folder/ Read Data
- Read Attributes
- Read Extended Attributes
- Read Permissions



26.15 – Click **OK** and your resulting screen should resemble the one below.



26.16 – Click **Apply**

26.17 – Click **OK** to exit the editing mode.

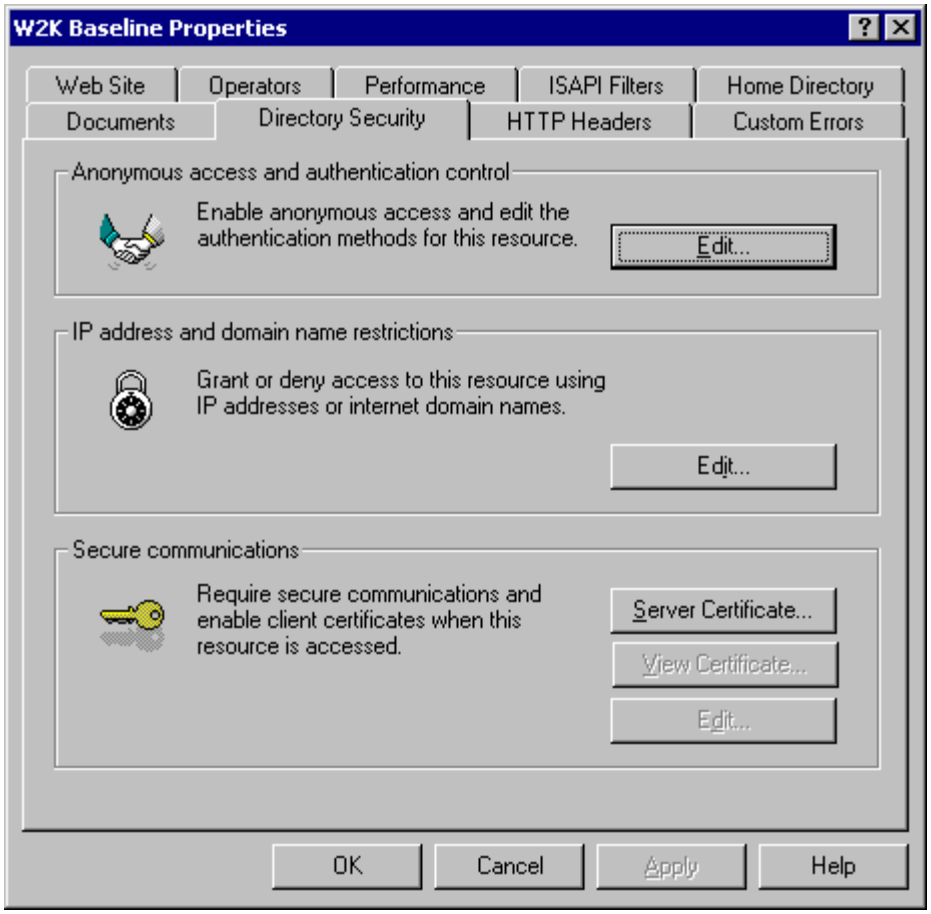
26.18 – Click **OK** to exit the permissions tab.

Remember to complete this for all of the paths and directories listed above.

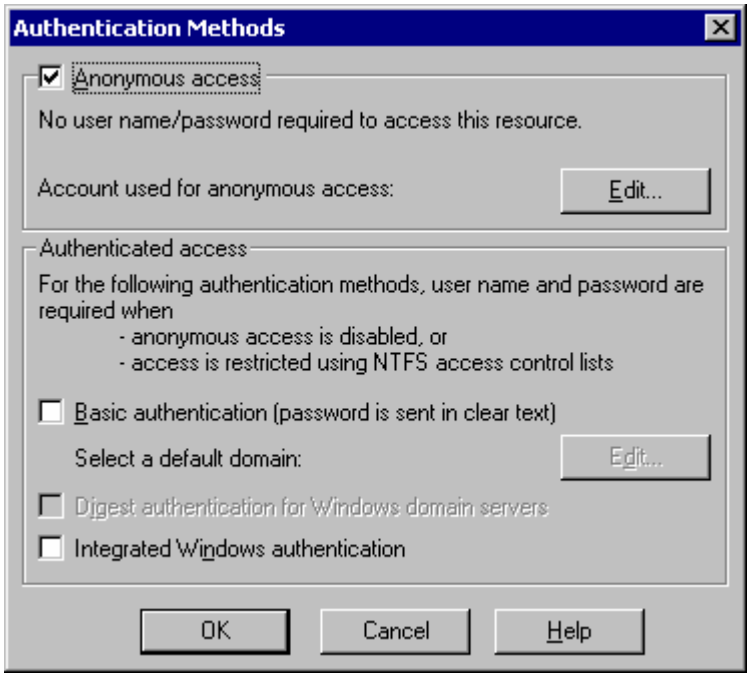
Step 27 - Change the Web Site to use the renamed IUSR account and associated password.

27.1 – Go to **Start** > **Programs** > **Administrative Tools** > **Internet Services Manager.**

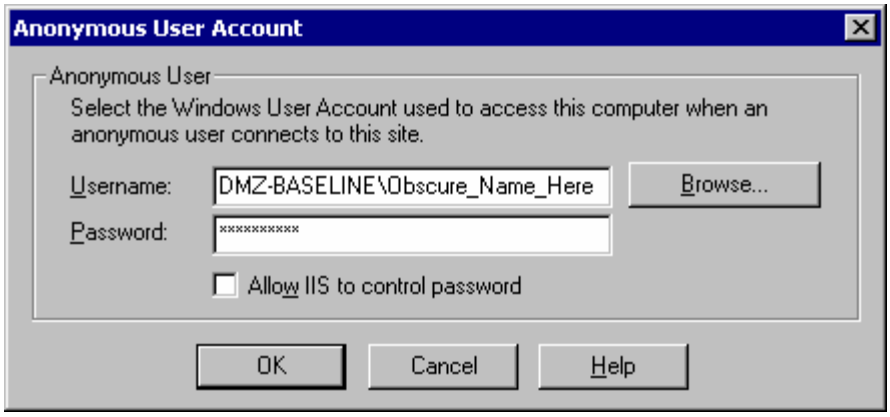
27.2 – Right mouse click on the web site that you created and select **Properties** > **Directory Security**



27.3 – Under the **Anonymous access and authentication control** subsection, select **Edit**.



27.4 – Under the **Anonymous access** subsection, select Edit



27.5 – Uncheck "**Allow IIS to control password**"

27.6 – Browse to your renamed **IUSR_<*machinename*>** (from **Step 25.4**) account and select **OK**.

27.7 – In the **Password:** field, type in the strong password that you previously set for the renamed **IUSR_<*machinename*>** account (in **Step 25.6**)

27.8 – Confirm the new password

27.9 – Click **OK** to return to the Main Menu

27.10 – Click **OK** to exit from editing mode.

Step 28 – Firewall rules

28.1 – Have your Network Administrator set up the proper ACLs to allow traffic to your website.

Example ACL for router to permit SSH, HTTP, HTTPS, SNMP

access-list 150 permit tcp any host yourwebserver eq 80
access-list 150 permit tcp any host yourwebserver eq 443
access-list 150 permit tcp SSH Client networks yourwebserver eq 22
access-list 150 permit udp SNMP Server networks host yourwebserver eq 161
access-list 150 permit udp SNMP Server networks host yourwebserver eq 161
access-list 150 permit udp SNMP Server networks host yourwebserver eq 162
access-list 150 permit udp SNMP Server network host yourwebserver eq 162

Revision History

Date of Change	Responsible Party	Changes Made
November 2000	Gavin Reid	Developed

2 Mar 2001	Infosec	Posted
13 Apr 2001	Sheri Moreau	Minor Updates
23 Apr 2001	Gavin Reid	Replaced Steps 57-60; added new zip download, etc.
09 May 2001	Gavin Reid	Renumbering fix & update to step 34
20 Jul 2001	Gavin Reid	Updated steps 17, 18 & 34
16 Aug 2001	Gavin Reid	Updated step 18
28 Aug 2002	Gavin Reid	Document revised
30 Jun 2004	Jay Ward	Wholesale revision, renumbering, patching updates, .inf policy updated.
08 Oct 2004	Jay Ward	MS Patch update.