This document is applicable ONLY to Microsoft Server 2003 running IIS 6.0. 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 keep the server unplugged from the network until you are told in the guide that it is ok to plug it in.

Step 1.0 – Boot up Windows Server 2003 Standard Edition (Build 3790) CD-ROM to begin installation and configuration.

Step 1.1 – When the Welcome Screen Appears, press Enter to continue

Step 1.2 – Press F8 to accept the 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 as needed, and delete afterwards. If there are any previous versions of operating systems, remove by deleting partitions and repartition.

Step 2.0 – Create a partition for the Operating System.

Step 2.1 – Press C to Create a Partition. In the white space, enter the value of your Operating System partition (this should be at LEAST 6.5GB (6500MB) and more is better) and press Enter to continue.

Step 2.2 – Choose the Partition that you just created with the Up/Down arrows and press Enter to begin the OS installation.

Step 2.3 – Choose “Format the partition using the NTFS file system” and press Enter to continue.

After formatting the hard drive and copying over the necessary files, the OS installation will reboot and continue.

Step 3.0 – Regional Settings

Step 3.1 – Choose regional settings as appropriate

Step 3.2 – Enter the following in the allowed whitespace:

Name of your Organization:
Company:

Step 3.3 – Enter the Product Activation Key

Step 3.4 – Choose the **Per Device or Per User** radio button

Step 3.5 – Give the server a name. Ensure that you follow the current corporate naming constraints for Servers. In general, the server name should consist of 3 letters for the Server function, 3 letters for the Server location and 3 numerals denoting the sequential order of the Server.

> **Example:** The first server for the Web Server Farm, residing in St. Louis – WEB-STL-001

Step 3.6 – Set a strong administrator password. Ensure that you follow your company's guidelines for creating a strong password.

Step 3.7 – Set time and date

Step 4.0 – Network Settings

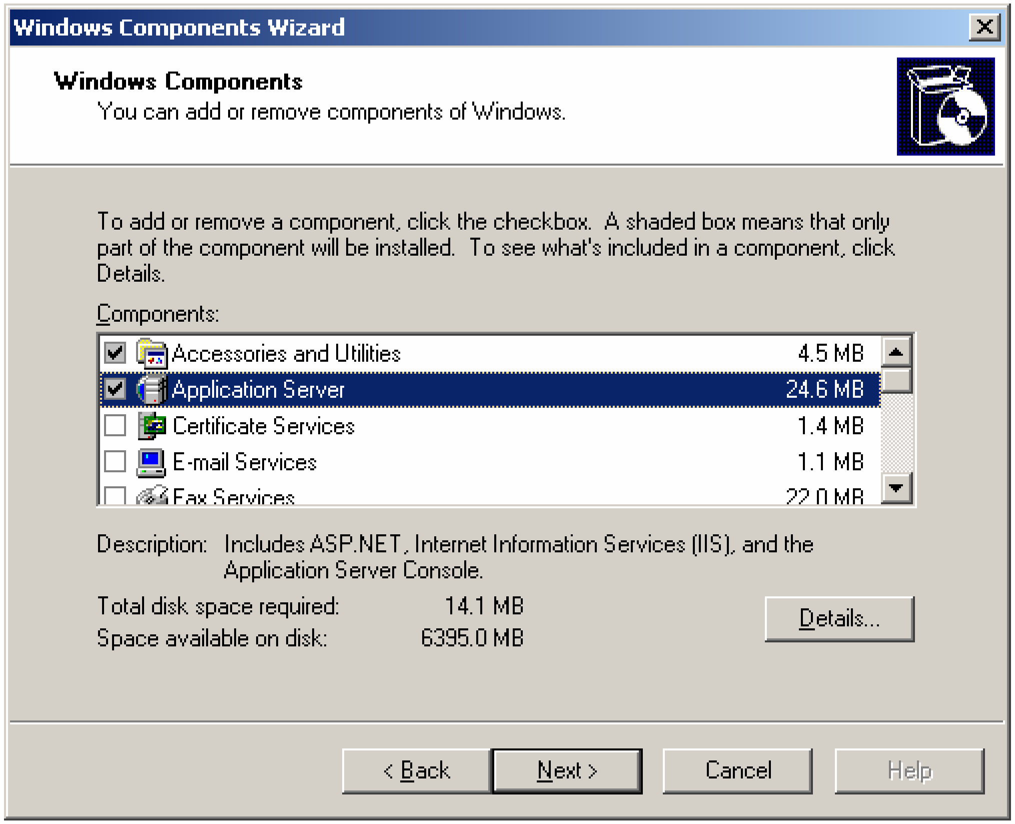
Step 4.1 – Choose Typical Settings

Step 4.2 – For Workgroup or Computer Domain, choose "No, this computer is not on a network…" In the white space, enter a blank workgroup (ALT-255).

The OS will now continue configuration. When it is done, it will bring you the Login Screen. Login with the password that you set in **Step 3.6**. After login, the "Manage Your Server" box will pop up. If you desire, place a check mark in the box labeled "Don't display this page at logon" and close the window.

Step 5.0 – Choose Components

Step 5.1 – Go to **Start > Control Panel > Add/Remove Programs > Add/Remove Windows Components** and select **Application Server**.



Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

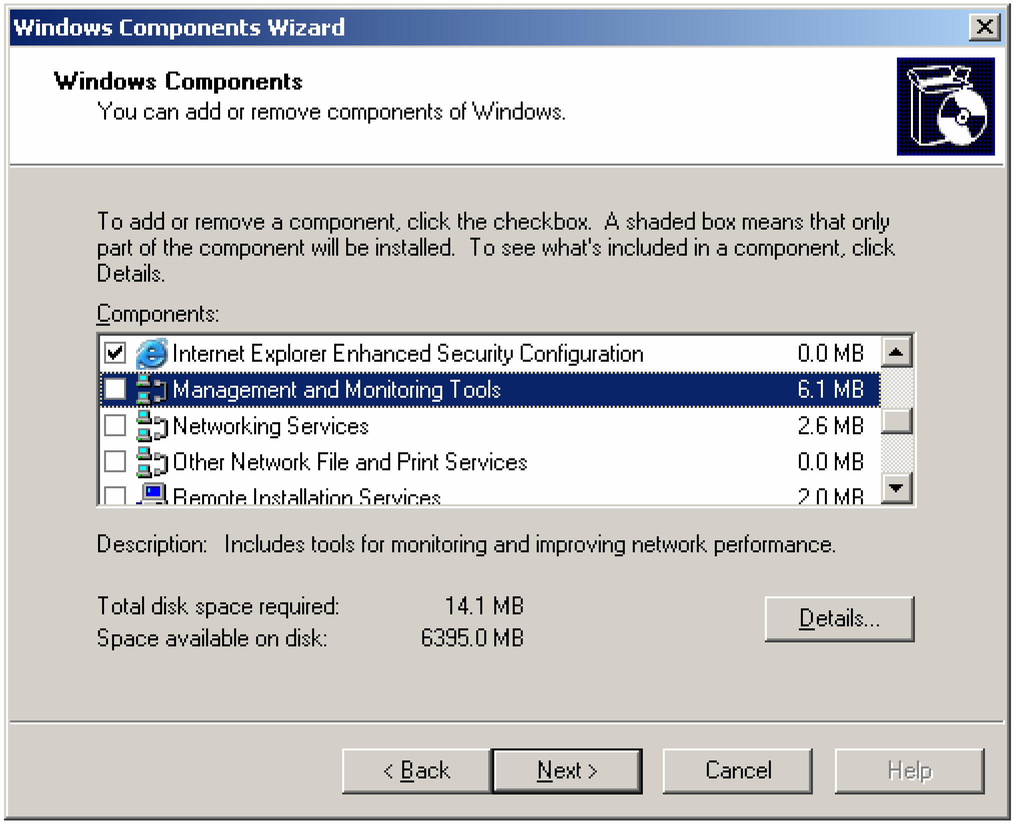
☑	Accessories and Utilities	4.5 MB
☑	Application Server	24.6 MB
☐	Certificate Services	1.4 MB
☐	E-mail Services	1.1 MB
☐	Fax Services	22.0 MB

Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.

Total disk space required: 14.1 MB

Space available on disk: 6395.0 MB

Step 5.2 – If you plan on using SNMP to monitor the Server, scroll down and high-light **Management and Monitoring Tools**


Windows Components Wizard
Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

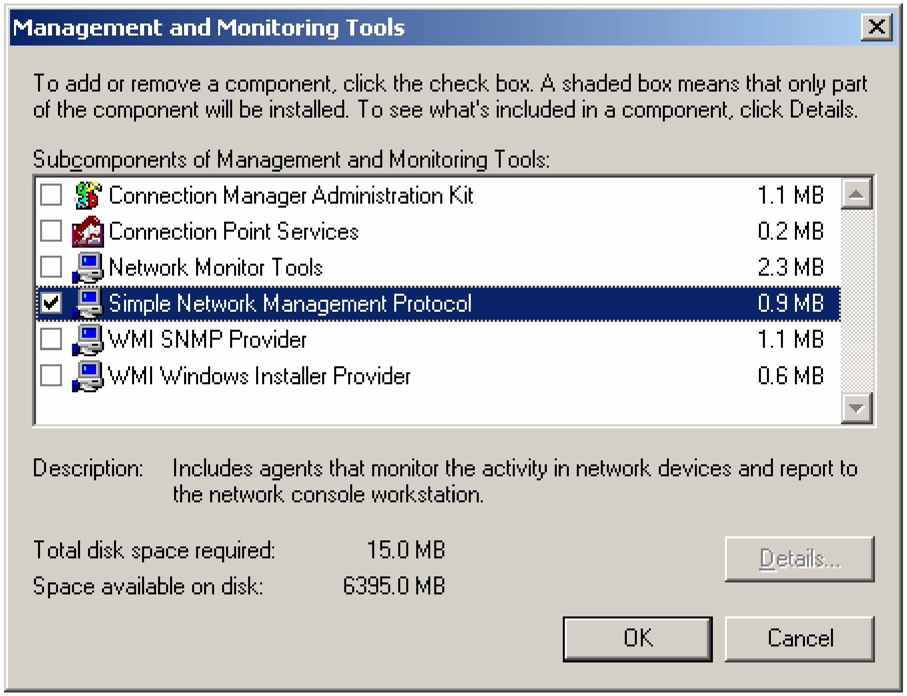
☑	Internet Explorer Enhanced Security Configuration	0.0 MB
☐	Management and Monitoring Tools	6.1 MB
☐	Networking Services	2.6 MB
☐	Other Network File and Print Services	0.0 MB
☐	Remote Installation Services	2.0 MB

Description: Includes tools for monitoring and improving network performance.

Total disk space required: 14.1 MB

Space available on disk: 6395.0 MB

Click on **Details**



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Management and Monitoring Tools:

☐	Connection Manager Administration Kit	1.1 MB
☐	Connection Point Services	0.2 MB
☐	Network Monitor Tools	2.3 MB
☑	Simple Network Management Protocol	0.9 MB
☐	WMI SNMP Provider	1.1 MB
☐	WMI Windows Installer Provider	0.6 MB

Description: Includes agents that monitor the activity in network devices and report to the network console workstation.

Total disk space required: 15.0 MB

Space available on disk: 6395.0 MB

Select only **Simple Network Management Protocol**

Click **OK** to return to the previous menu.

Step 5.3 – Click Next to begin installation of the Application Server Components.

Step 5.4 – When the Application Server has finished installing, you can click the Finish button to complete the installation and then you can close the Add/Remove Programs window.

Step 6.0 – Install the latest Patch Releases

As of 10/15/04:

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

MS04-034 (873376)	October 12, 2004 - Vulnerability in Compressed (zipped) Folders Could Allow Remote Code Execution

MS04-032 (840987)	October 12, 2004 - Security Update for Microsoft Windows

MS04-028 (833987)	September 21, 2004 - Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution

MS04-024 (839645)	August 10, 2004 - Vulnerability in Windows Shell Could Allow Remote Code Execution

MS04-023 (840315)	July 13, 2003 - Vulnerability in HTML Help Could Allow Code Execution

MS03-039 (824146)	September 10, 2003 - Buffer Overrun In RPCSS Service Could Allow Code Execution.

MS03-041 (823182)	November 17, 2003 – Vulnerability in Authenticode Verification Could Allow Remote Code Execution

MS03-043 (828035)	October 15, 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

MS03-048 (824145)	December 11, 2003 - Cumulative Security Update for Internet Explorer

MS04-007 (828028)	February 10, 2004 - ASN.1 Vulnerability Could Allow Code Execution

MS04-011 (835732)	April 13, 2004 - Security Update for Microsoft Windows

MS04-012 (828741)	April 13, 2004 – Cumulative Update for RPC/DCOM

Step 6.1 – You may now plug the server into the network.

Step 7.0 – Installing SSH Server for Remote Management

For remote access we will use SSH as the only transport. The software is available below for the server and the client.

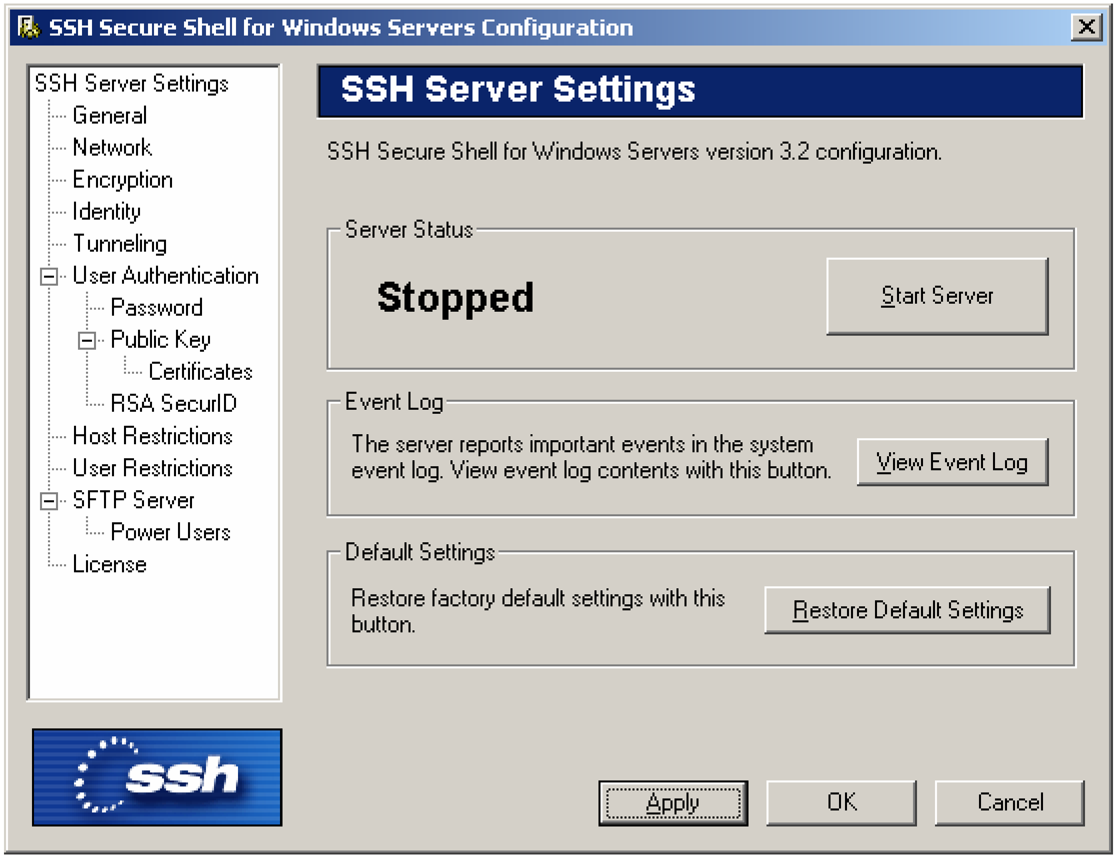
Step 7.1 – Download and install an SSH Server and Client Software

We recommend the server and client from http://www.ssh.com/.

Step 7.2 – 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:



SSH Server Settings

SSH Secure Shell for Windows Servers version 3.2 configuration.

Server Status

Stopped

Event Log

The server reports important events in the system event log. View event log contents with this button.

Default Settings

Restore factory default settings with this button.

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

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

Step 7.3 – Create a new text file called **BannerMSG.txt** and place it in:

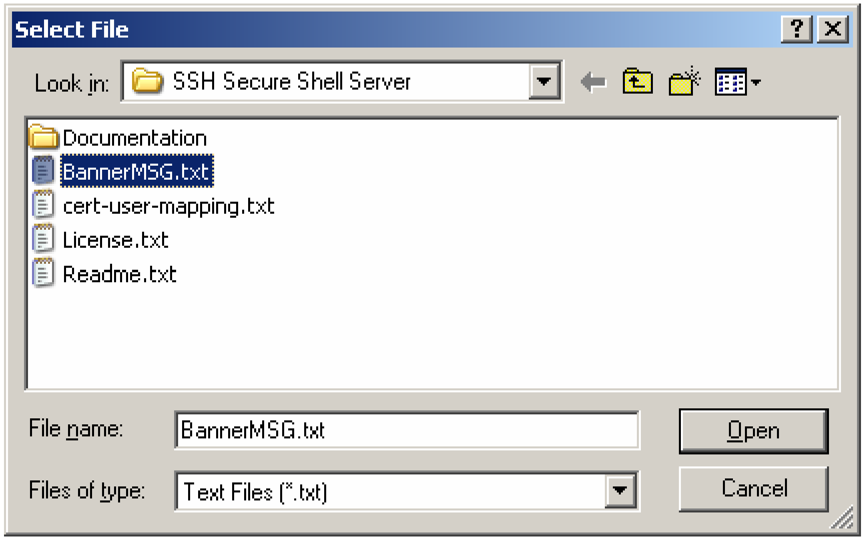
C:\Program Files\SSH Communications Security\SSH Secure Shell Server directory

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.
```

Step 7.4 – 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.



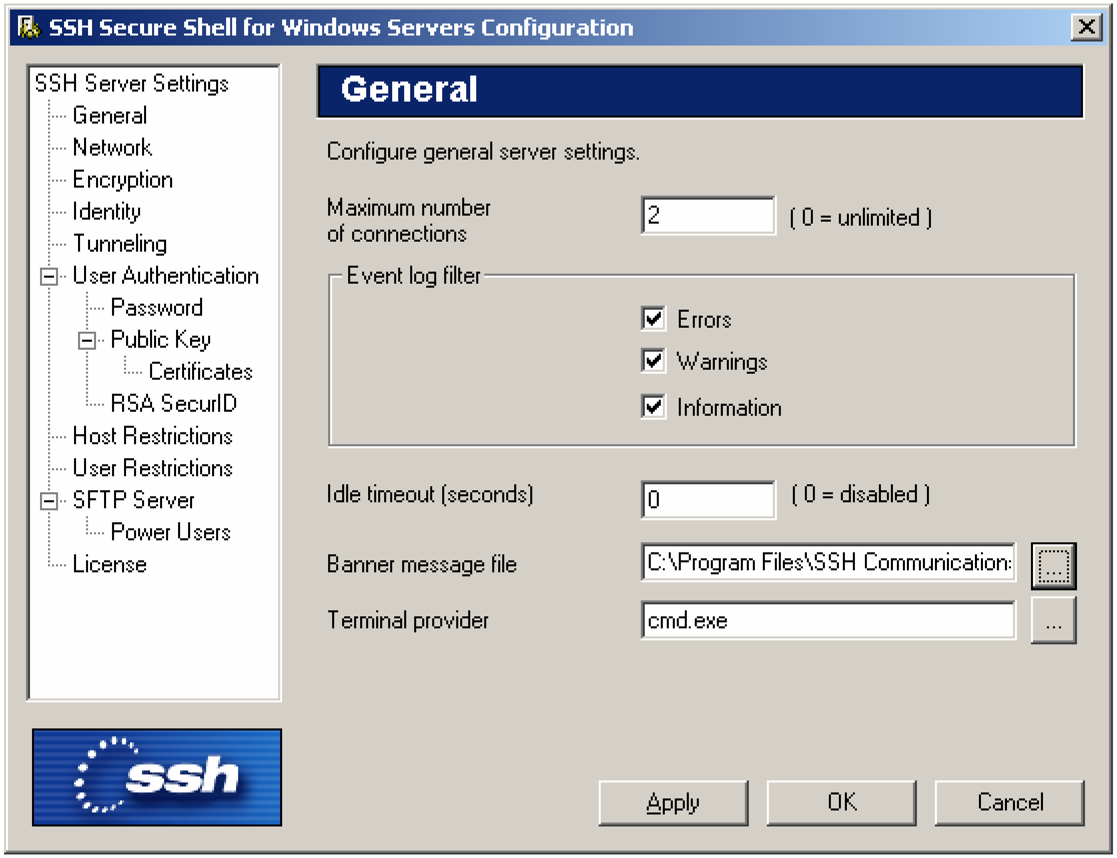
Look in: SSH Secure Shell Server

Documentation
BannerMSG.txt
cert-user-mapping.txt
License.txt
Readme.txt

File name: BannerMSG.txt

Files of type: Text Files (*.txt)

The resulting screen should look like this:



General

Configure general server settings.

Maximum number of connections: 2 (0 = unlimited)

Event log filter

☑ Errors
☑ Warnings
☑ Information

Idle timeout (seconds): 0 (0 = disabled)

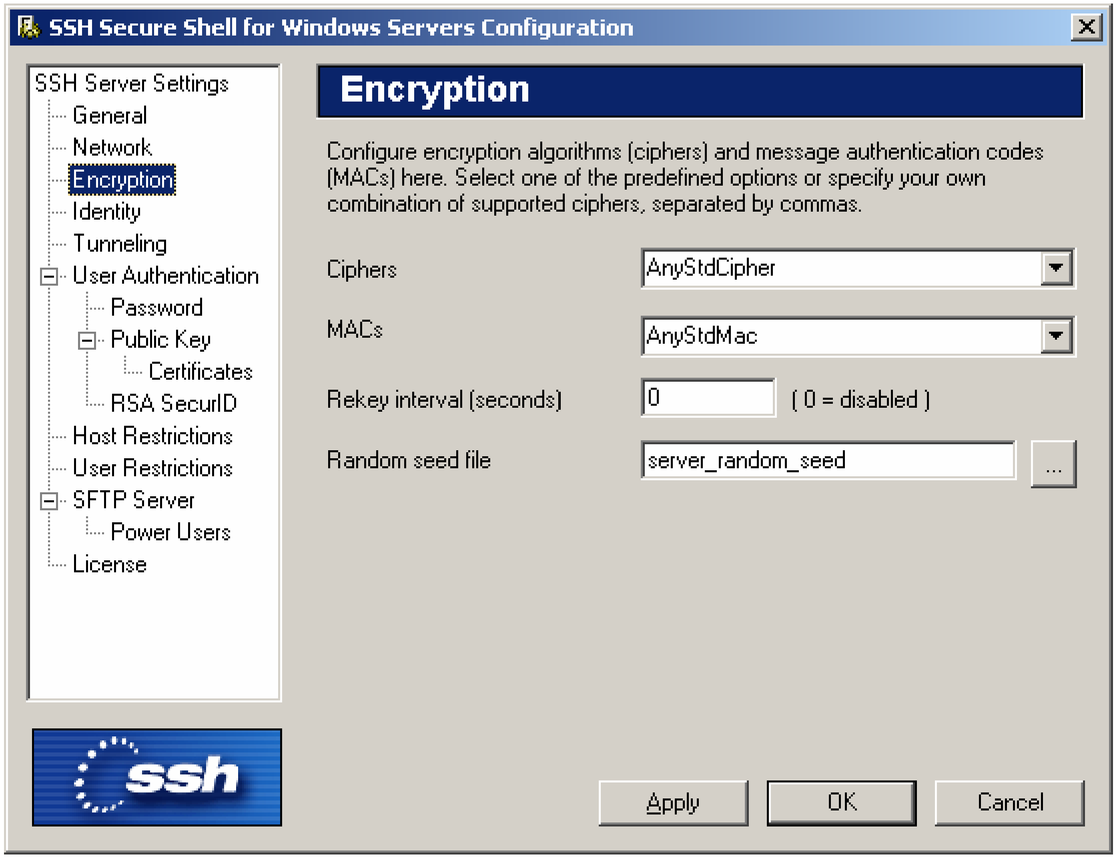
Banner message file: C:\Program Files\SSH Communication:

Terminal provider: cmd.exe

Step 7.5 - Under the **Encryption** Tab**:**

Ensure that the following settings are selected:

Ciphers: AnyStdCipher
MACs: AnyStdMac



Configure encryption algorithms (ciphers) and message authentication codes (MACs) here. Select one of the predefined options or specify your own combination of supported ciphers, separated by commas.

Ciphers: AnyStdCipher

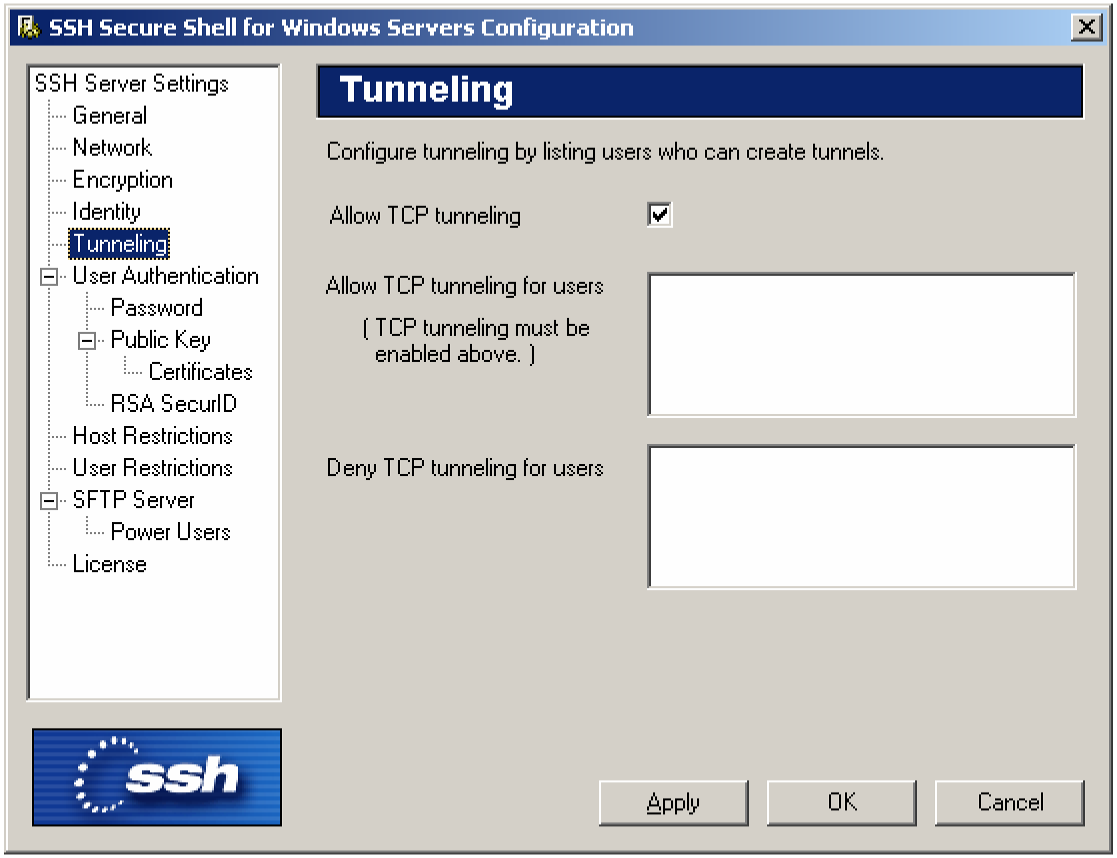
MACs: AnyStdMac

Rekey interval (seconds): 0 (0 = disabled)

Random seed file: server_random_seed

Step 7.6 - Under the **Tunneling** Tab**:**

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



SSH Secure Shell for Windows Servers Configuration

Tunneling

Configure tunneling by listing users who can create tunnels.

Allow TCP tunneling ☑

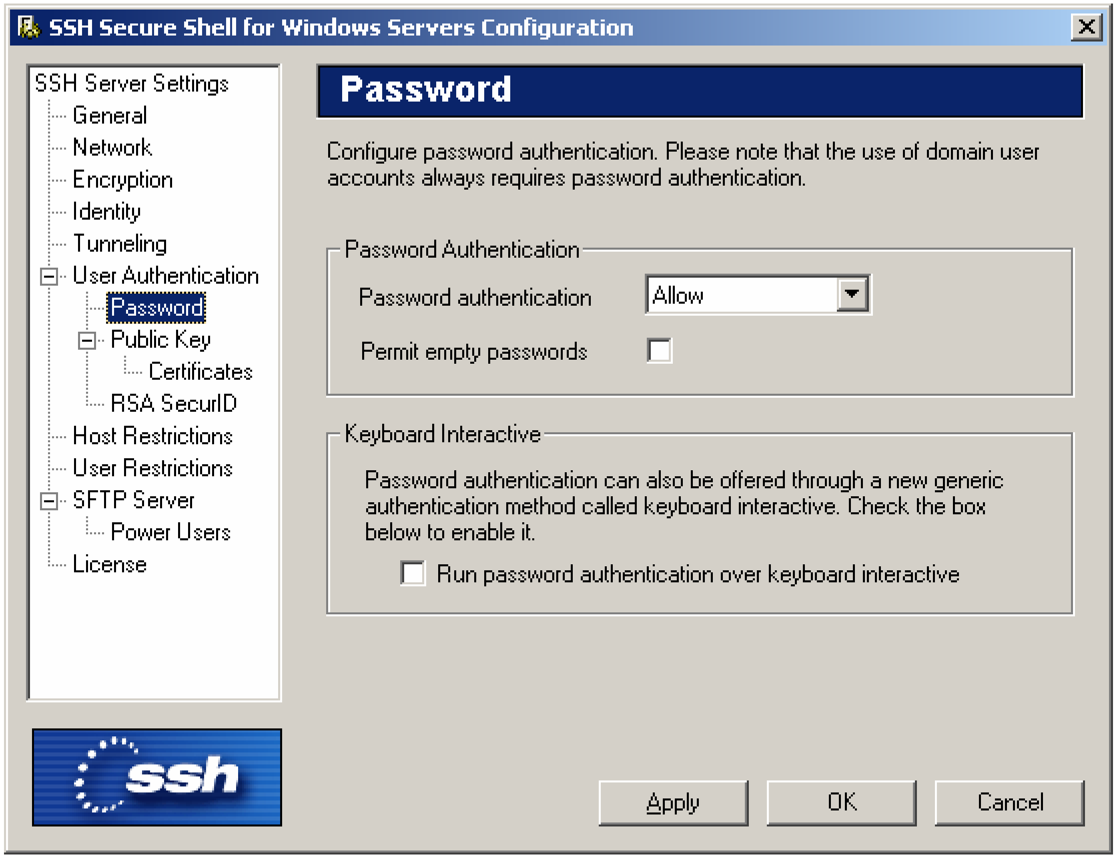
Allow TCP tunneling for users

(TCP tunneling must be enabled above.)

Deny TCP tunneling for users

Step 7.7 – Under the **User Authentication > Password** Tab

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



Password

Configure password authentication. Please note that the use of domain user accounts always requires password authentication.

Password Authentication

Password authentication: Allow

☐ Permit empty passwords

Keyboard Interactive

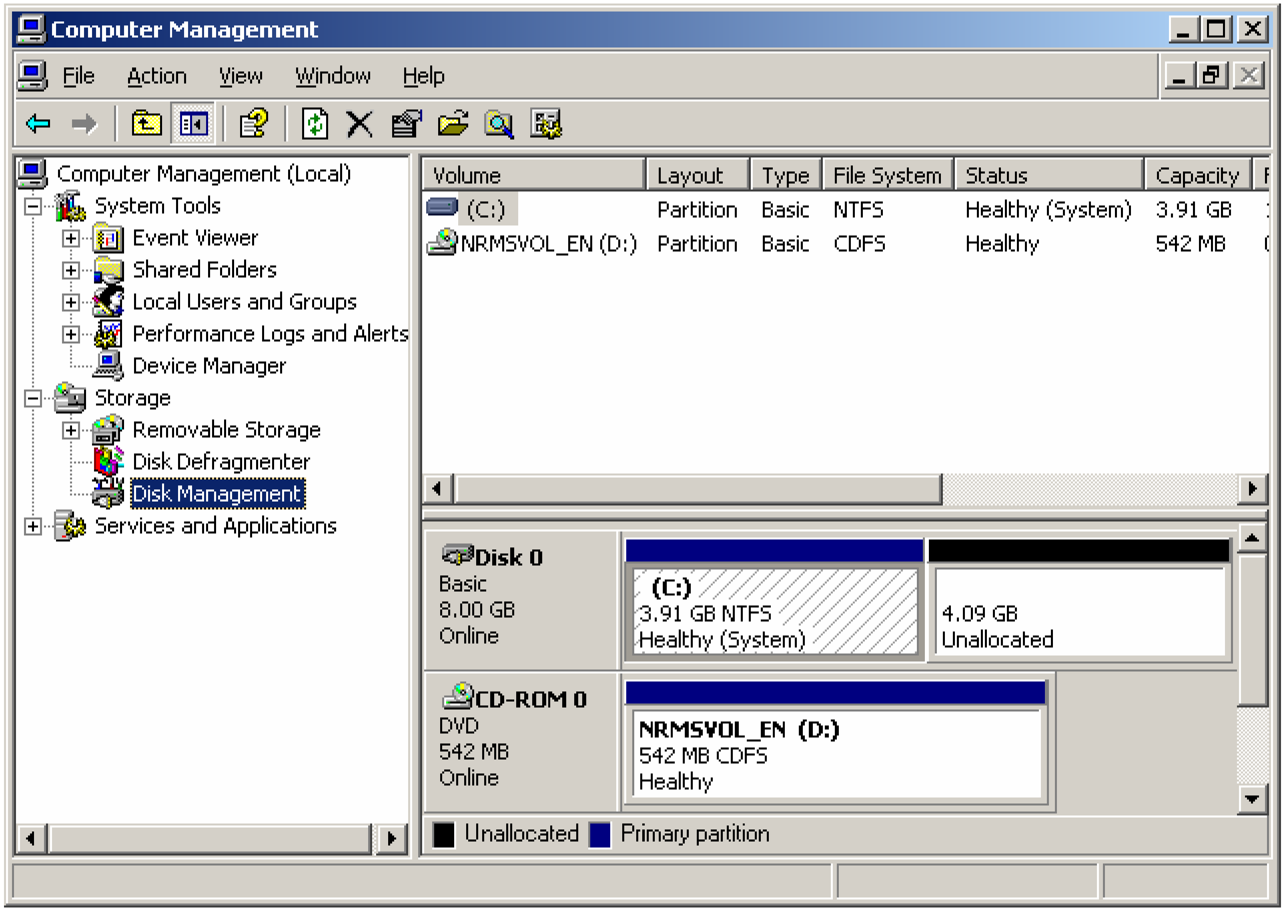
Password authentication can also be offered through a new generic authentication method called keyboard interactive. Check the box below to enable it.

☐ Run password authentication over keyboard interactive

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

Step 8.0 – Media Configuration and Permissions

Step 8.1 – Go to **Start** > **Programs** > **Administrative Tools** > **Computer Management** > **Disk Management**



Volume	Layout	Type	File System	Status	Capacity
(C:)	Partition	Basic	NTFS	Healthy (System)	3.91 GB
NRMSVOL_EN (D:)	Partition	Basic	CDFS	Healthy	542 MB

Disk 0
Basic
8.00 GB
Online

(C:)
3.91 GB NTFS
Healthy (System)

4.09 GB
Unallocated

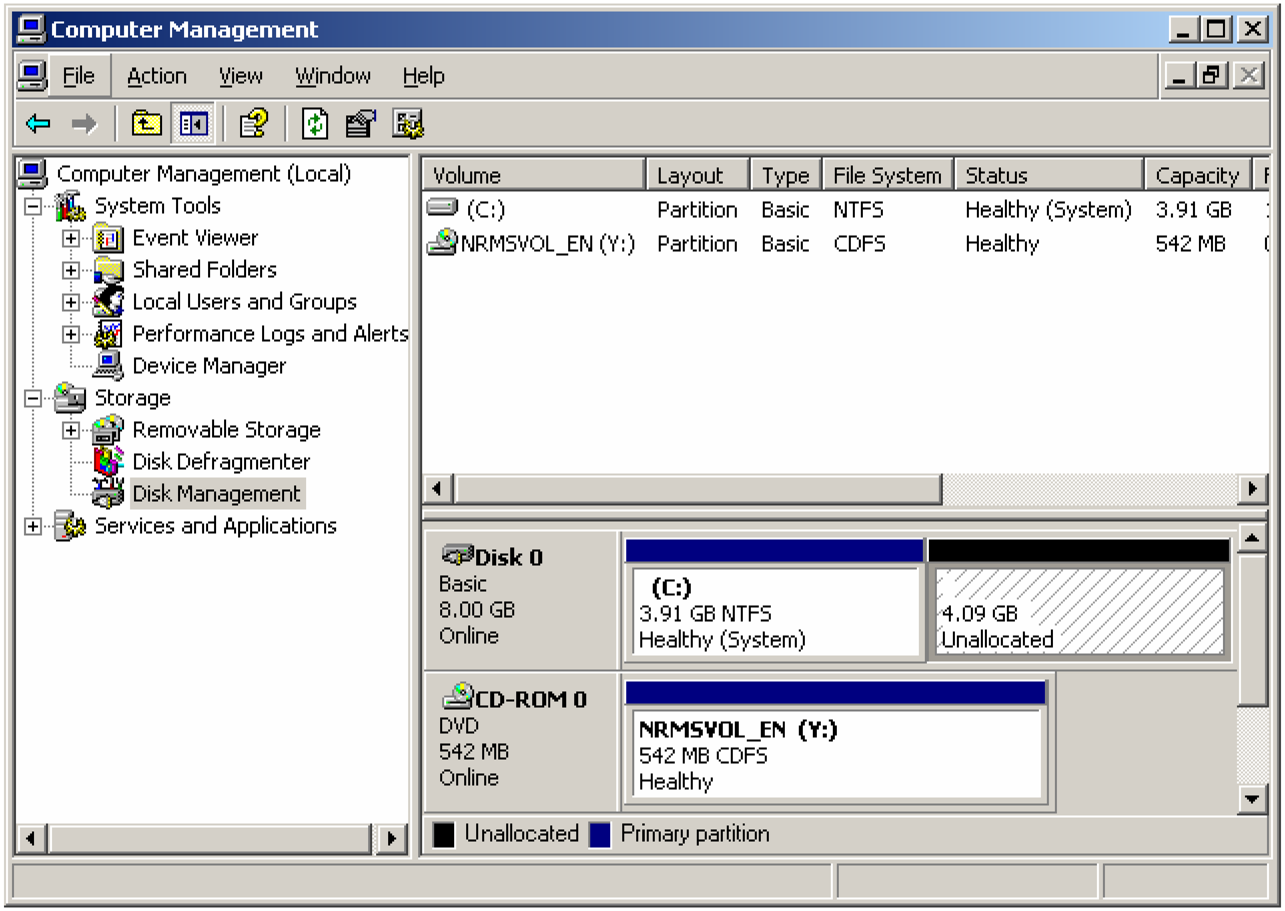
CD-ROM 0
DVD
542 MB
Online

NRMSVOL_EN (D:)
542 MB CDFS
Healthy

■ Unallocated ■ Primary partition

Step 8.3 - 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**.



Volume	Layout	Type	File System	Status	Capacity
(C:)	Partition	Basic	NTFS	Healthy (System)	3.91 GB
NRMSVOL_EN (Y:)	Partition	Basic	CDFS	Healthy	542 MB

Disk 0
Basic
8.00 GB
Online

(C:)
3.91 GB NTFS
Healthy (System)

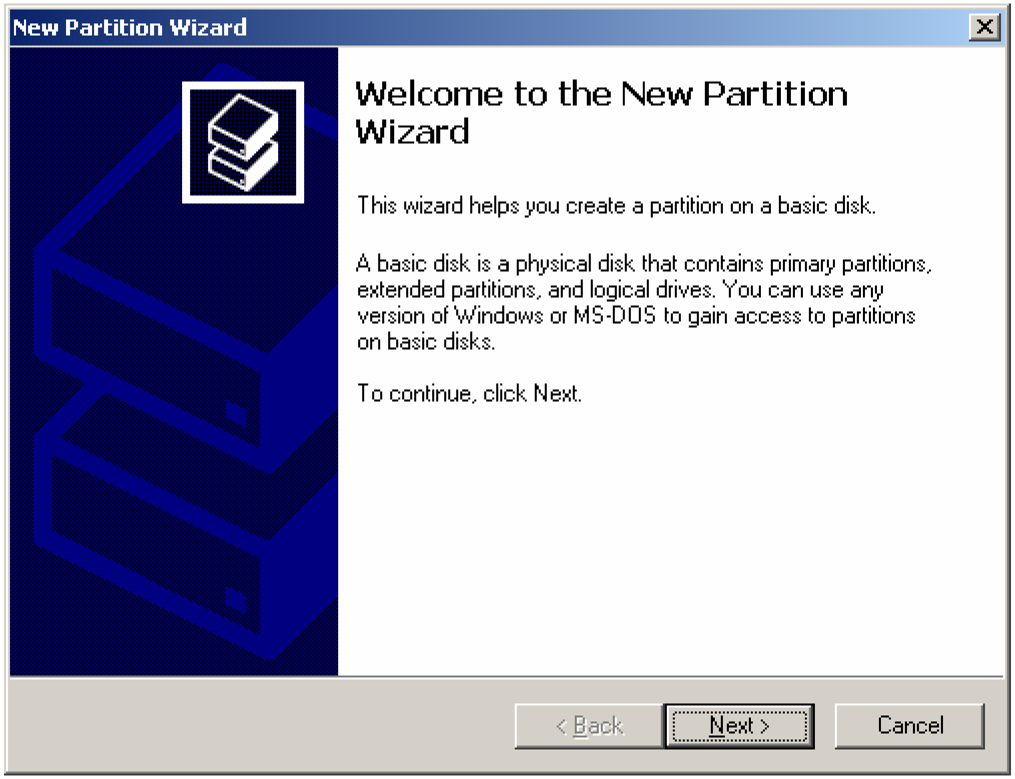
4.09 GB
Unallocated

CD-ROM 0
DVD
542 MB
Online

NRMSVOL_EN (Y:)
542 MB CDFS
Healthy

■ Unallocated ■ Primary partition

This will bring up the New Partition Wizard



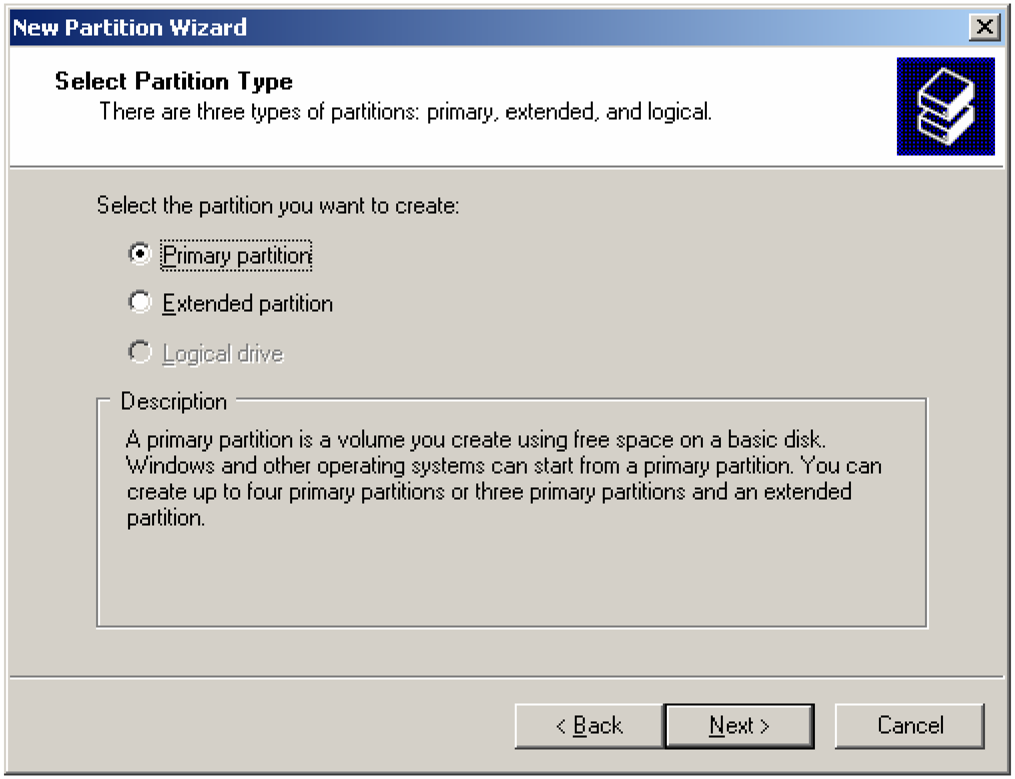
Welcome to the New Partition Wizard

This wizard helps you create a partition on a basic disk.

A basic disk is a physical disk that contains primary partitions, extended partitions, and logical drives. You can use any version of Windows or MS-DOS to gain access to partitions on basic disks.

To continue, click Next.

Step 8.7 – Click **Next** to continue



There are three types of partitions: primary, extended, and logical.

Select the partition you want to create:

● Primary partition

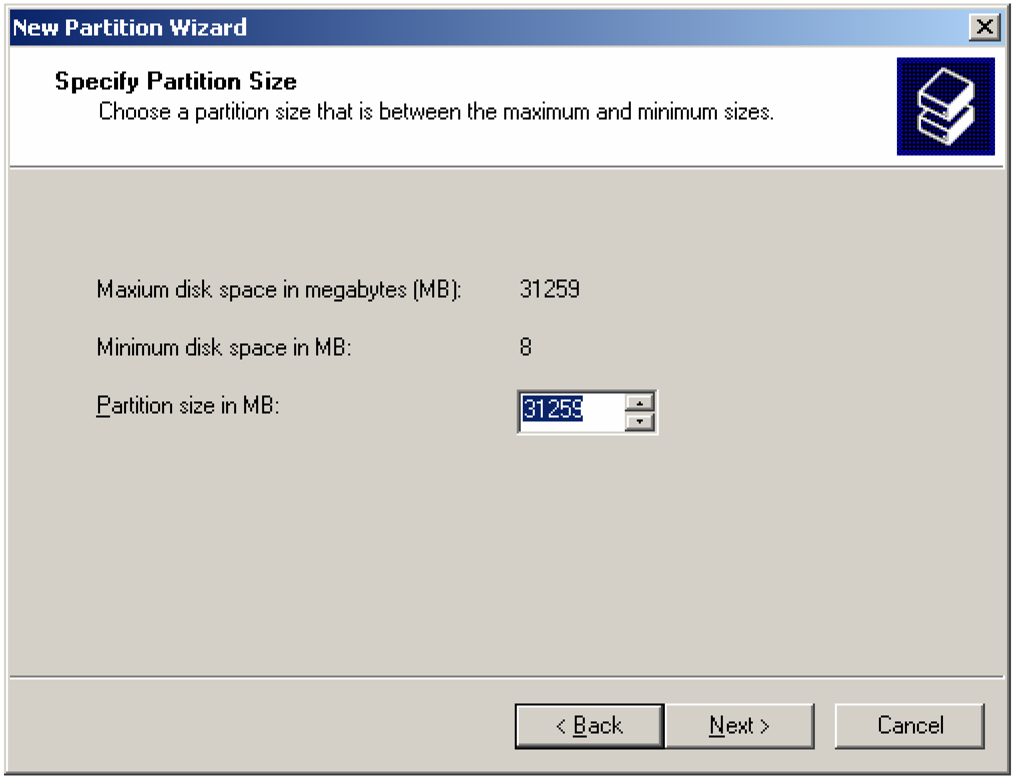
○ Extended partition

○ Logical drive

Description

A primary partition is a volume you create using free space on a basic disk. Windows and other operating systems can start from a primary partition. You can create up to four primary partitions or three primary partitions and an extended partition.

Step 8.8 – Ensure that **Primary partition** is selected and click **Next** to continue.



Specify Partition Size

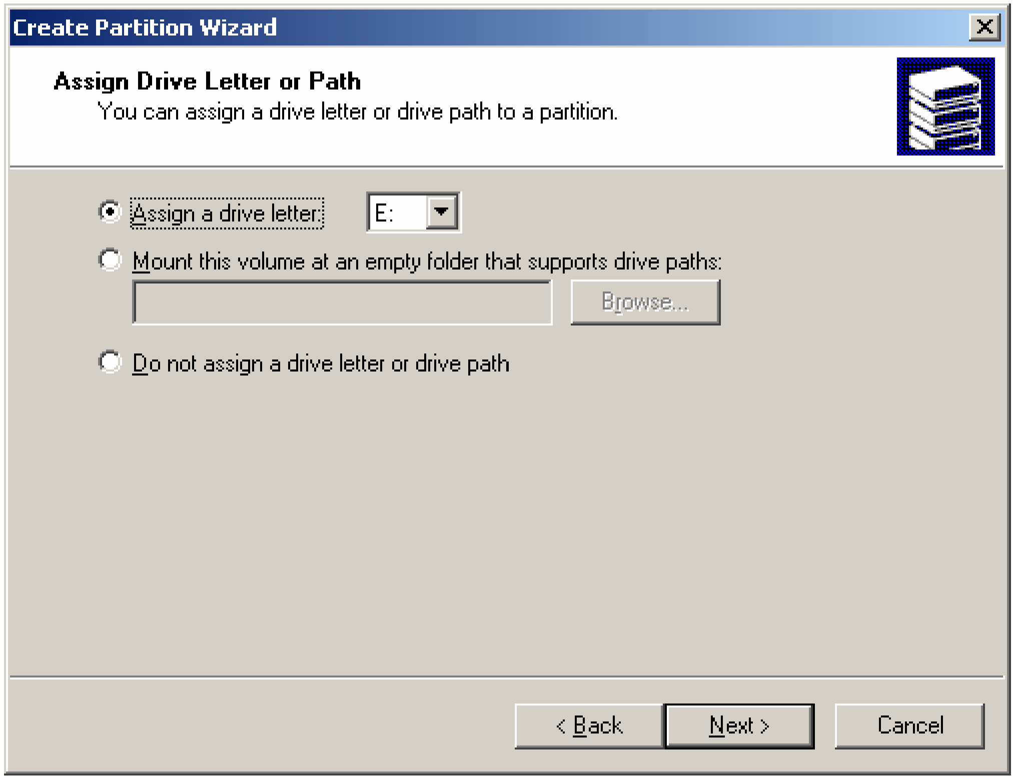
Choose a partition size that is between the maximum and minimum sizes.

Maxium disk space in megabytes (MB): 31259

Minimum disk space in MB: 8

Partition size in MB: 31259

Step 8.9 – Select the size of your partition in MB and click **Next** to continue.



Create Partition Wizard

Assign Drive Letter or Path

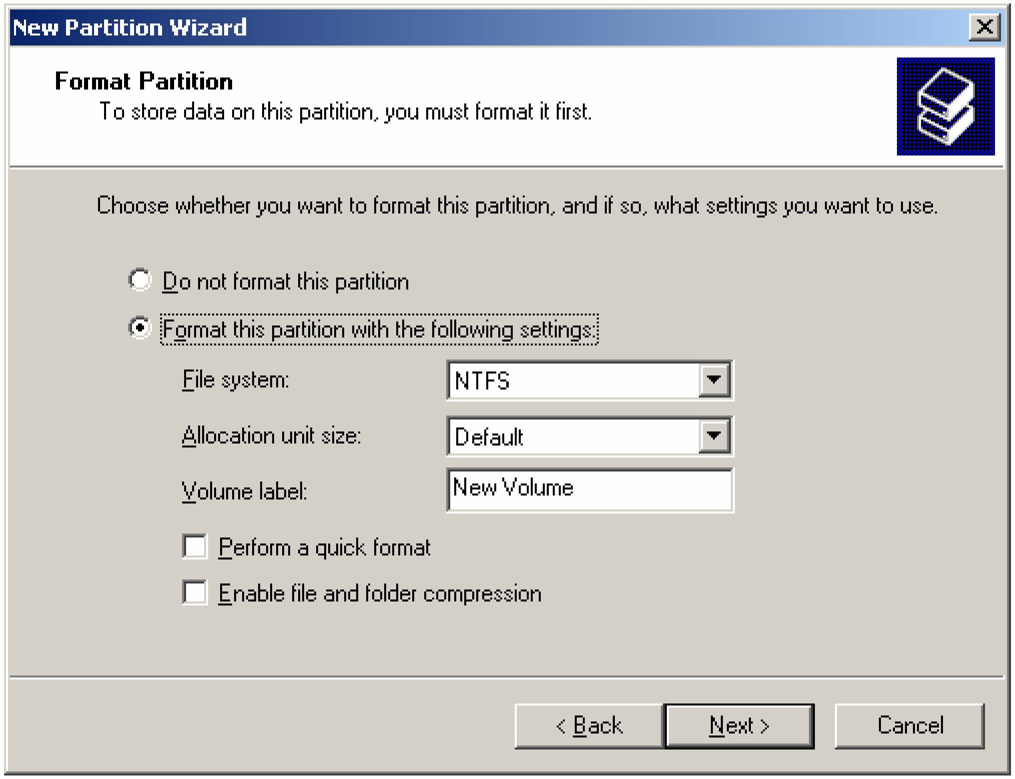
You can assign a drive letter or drive path to a partition.

● Assign a drive letter: E:

○ Mount this volume at an empty folder that supports drive paths:

○ Do not assign a drive letter or drive path

Step 8.10 – Assign it the appropriate drive letter, **E:** and click **Next** to continue.



Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this partition, and if so, what settings you want to use.

○ Do not format this partition

● Format this partition with the following settings:

File system: NTFS

Allocation unit size: Default

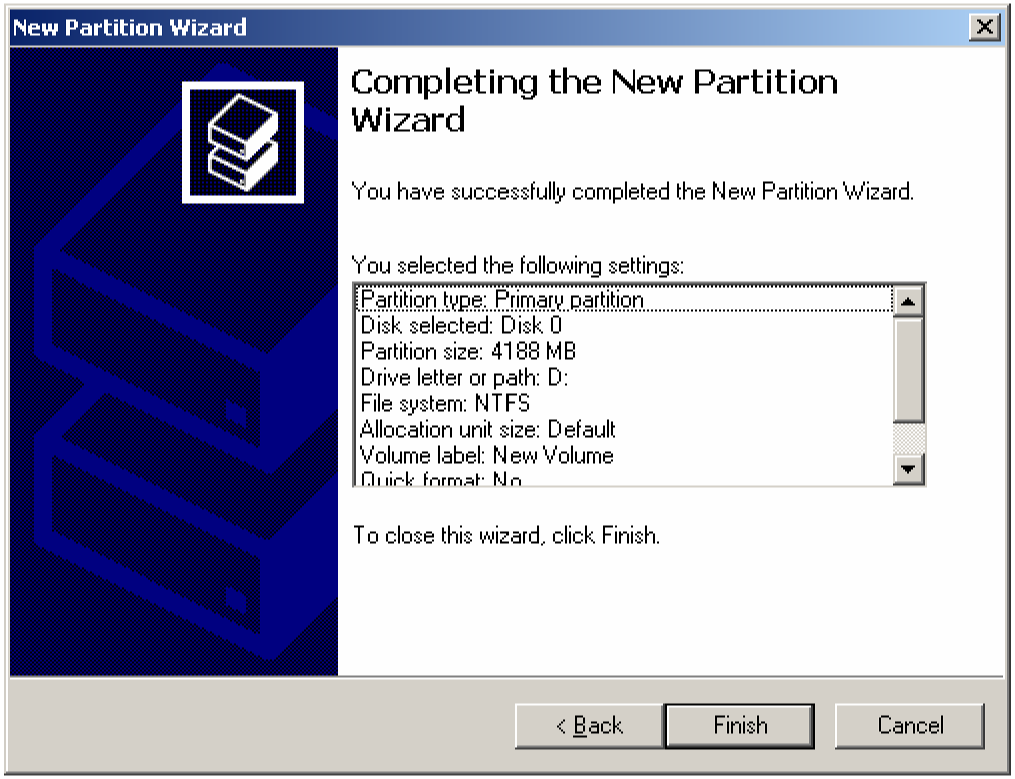
Volume label: New Volume

☐ Perform a quick format

☐ Enable file and folder compression

Step 8.11 – 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.



Completing the New Partition Wizard

You have successfully completed the New Partition Wizard.

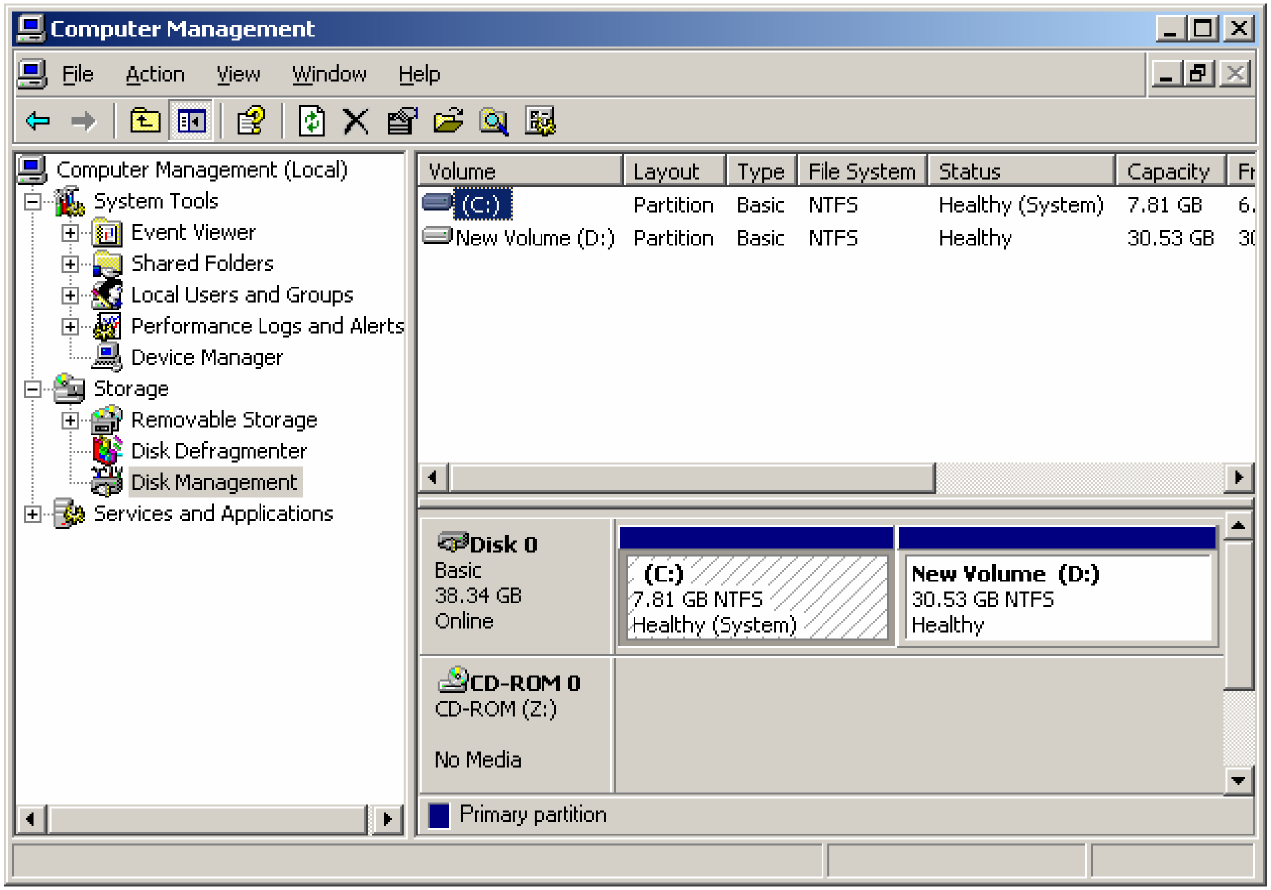
You selected the following settings:

Partition type: Primary partition
Disk selected: Disk 0
Partition size: 4188 MB
Drive letter or path: D:
File system: NTFS
Allocation unit size: Default
Volume label: New Volume
Quick format: No

To close this wizard, click Finish.

Step 8.12 – 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.



Volume	Layout	Type	File System	Status	Capacity	Fr
(C:)	Partition	Basic	NTFS	Healthy (System)	7.81 GB	6.
New Volume (D:)	Partition	Basic	NTFS	Healthy	30.53 GB	3

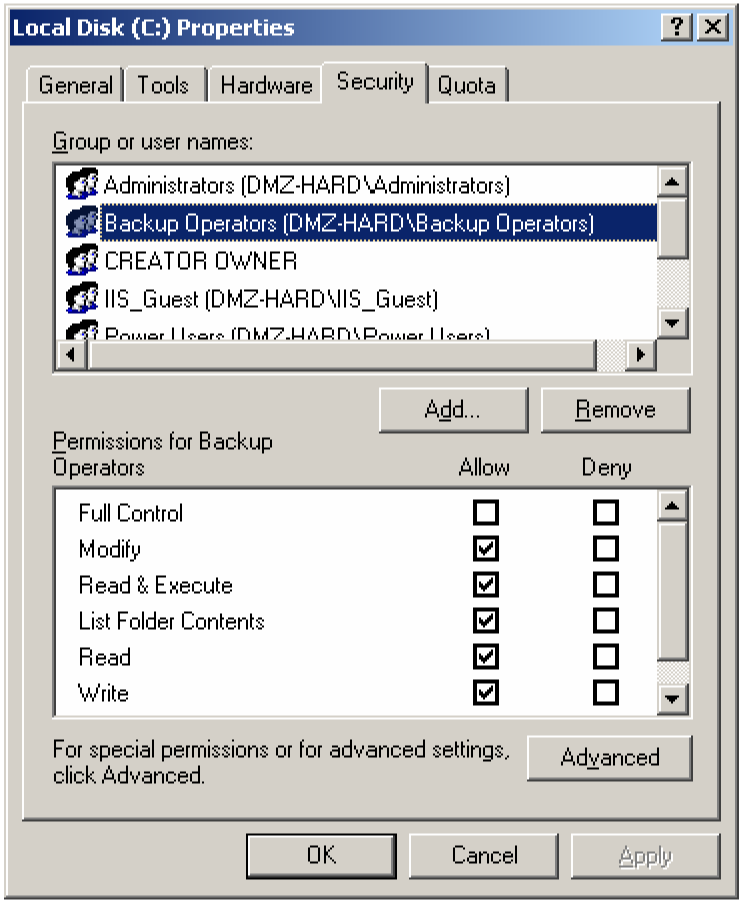
When the formatting is complete, you can close the **Computer Management** window.

Step 8.13 – Double click on the My Computer icon, Right click on the **C:** drive and select **Sharing and Security**

Click on the **Security** Tab

Step 8.14 – Remove the **Everyone** Group

Step 8.15 – Click on **Add** and add the **Backup Operators** Group and give them permissions for **Modify**.



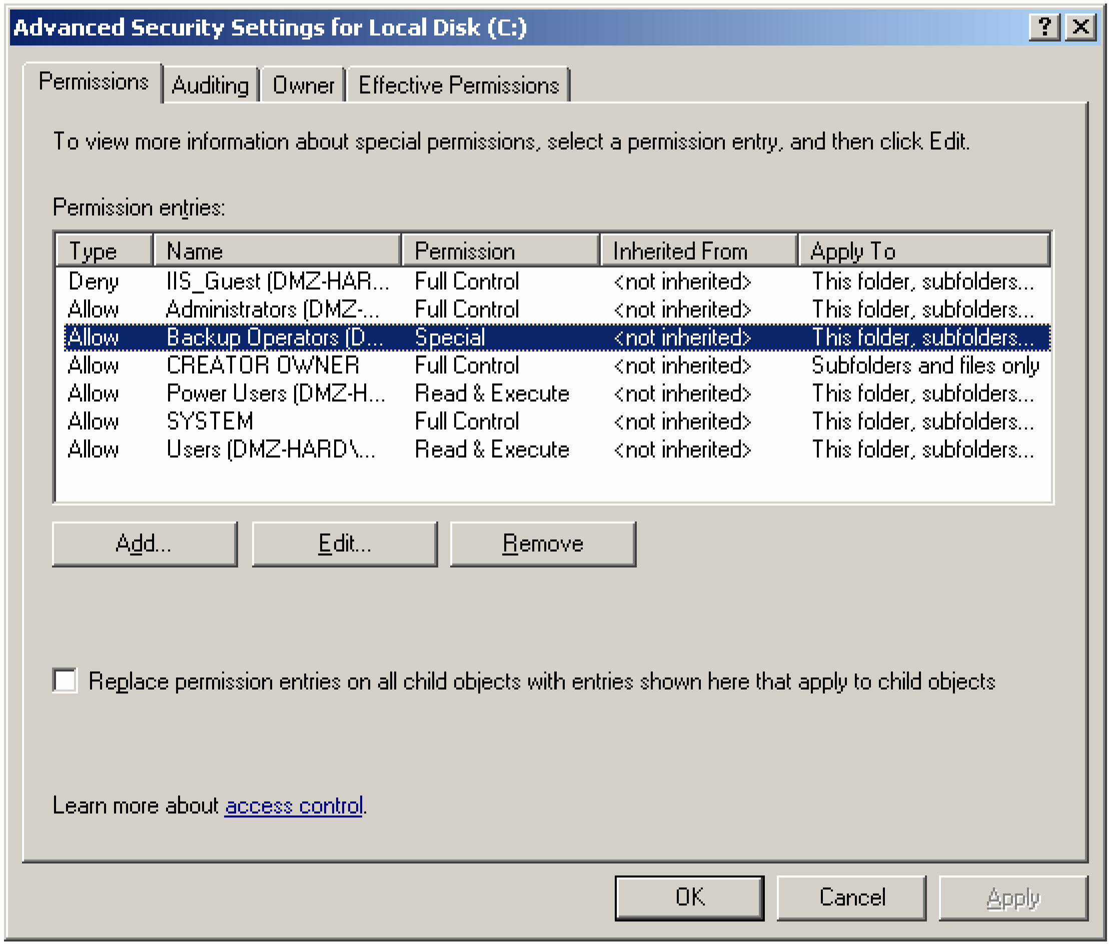
Group or user names:

- Administrators (DMZ-HARD\Administrators)
- Backup Operators (DMZ-HARD\Backup Operators)
- CREATOR OWNER
- IIS_Guest (DMZ-HARD\IIS_Guest)
- Power Users (DMZ-HARD\Power Users)

Permissions for Backup Operators	Allow	Deny
Full Control	☐	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

For special permissions or for advanced settings, click Advanced.

Step 8.16 – Click on the **Advanced** button and highlight the **Backup Operators** group that you just added.



To view more information about special permissions, select a permission entry, and then click Edit.

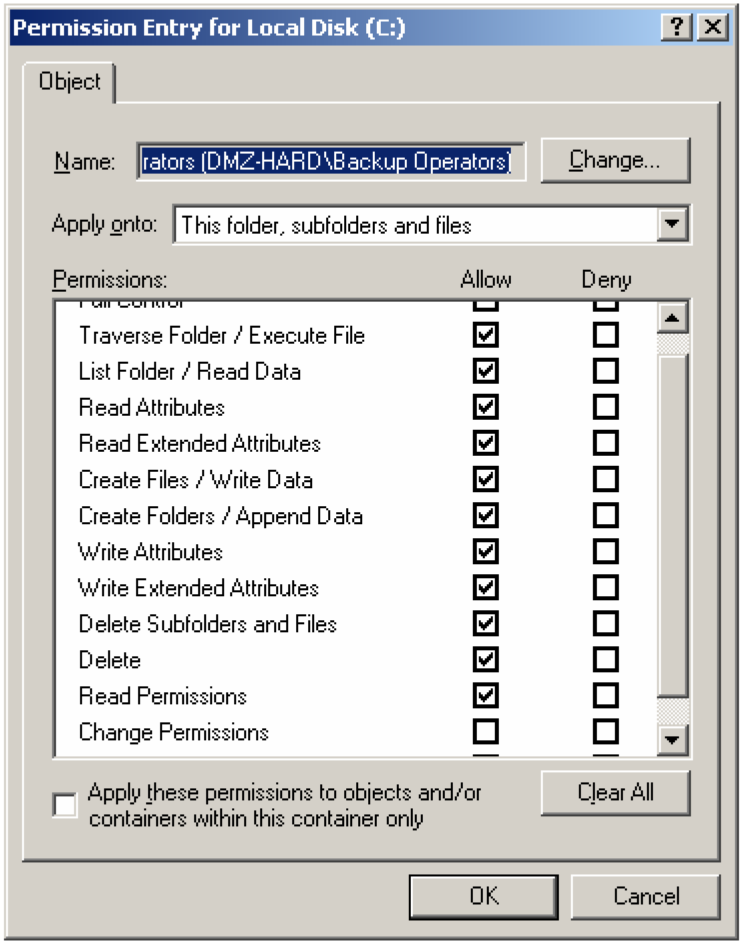
Permission entries:

Type	Name	Permission	Inherited From	Apply To
Deny	IIS_Guest (DMZ-HAR...	Full Control	<not inherited>	This folder, subfolders...
Allow	Administrators (DMZ-...	Full Control	<not inherited>	This folder, subfolders...
Allow	Backup Operators (D...	Special	<not inherited>	This folder, subfolders...
Allow	CREATOR OWNER	Full Control	<not inherited>	Subfolders and files only
Allow	Power Users (DMZ-H...	Read & Execute	<not inherited>	This folder, subfolders...
Allow	SYSTEM	Full Control	<not inherited>	This folder, subfolders...
Allow	Users (DMZ-HARD\...	Read & Execute	<not inherited>	This folder, subfolders...

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

Learn more about access control.

Step 8.17 – Click on the **Edit** button and ensure that the Backup Operators group has permissions for everything **EXCEPT: Full Control**, **Change Permissions** and **Take Control**



Name: rators (DMZ-HARD\Backup Operators)

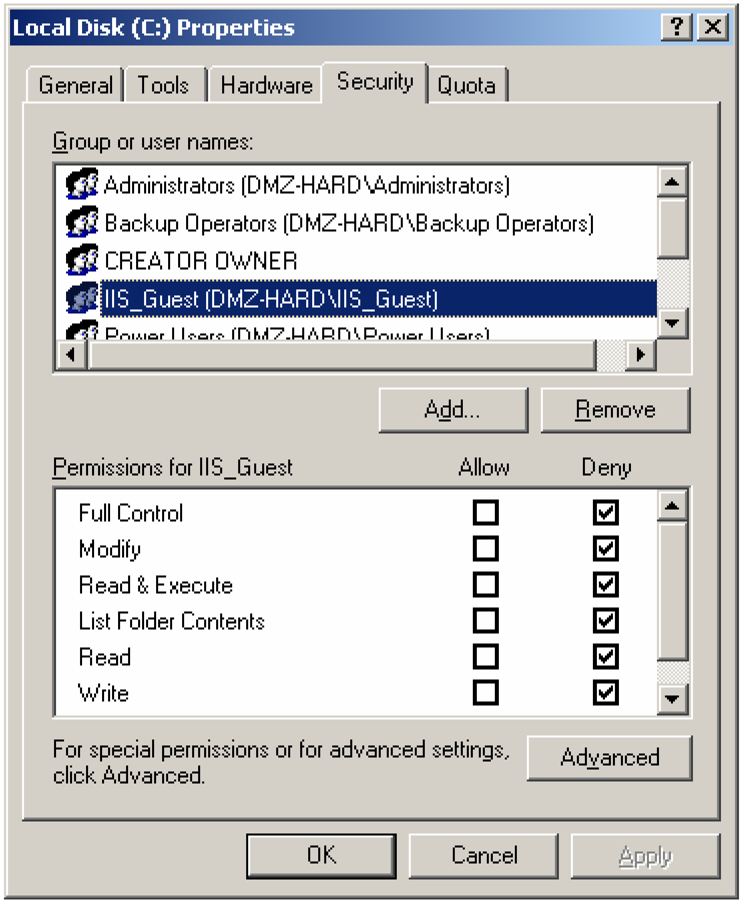
Apply onto: This folder, subfolders and files

Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	☐
List Folder / Read Data	☑	☐
Read Attributes	☑	☐
Read Extended Attributes	☑	☐
Create Files / Write Data	☑	☐
Create Folders / Append Data	☑	☐
Write Attributes	☑	☐
Write Extended Attributes	☑	☐
Delete Subfolders and Files	☑	☐
Delete	☑	☐
Read Permissions	☑	☐
Change Permissions	☐	☐

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

Click **OK** when done.

Step 8.18 – Click on the **Add** button and add the **IIS_Guest** Group.



Group or user names:

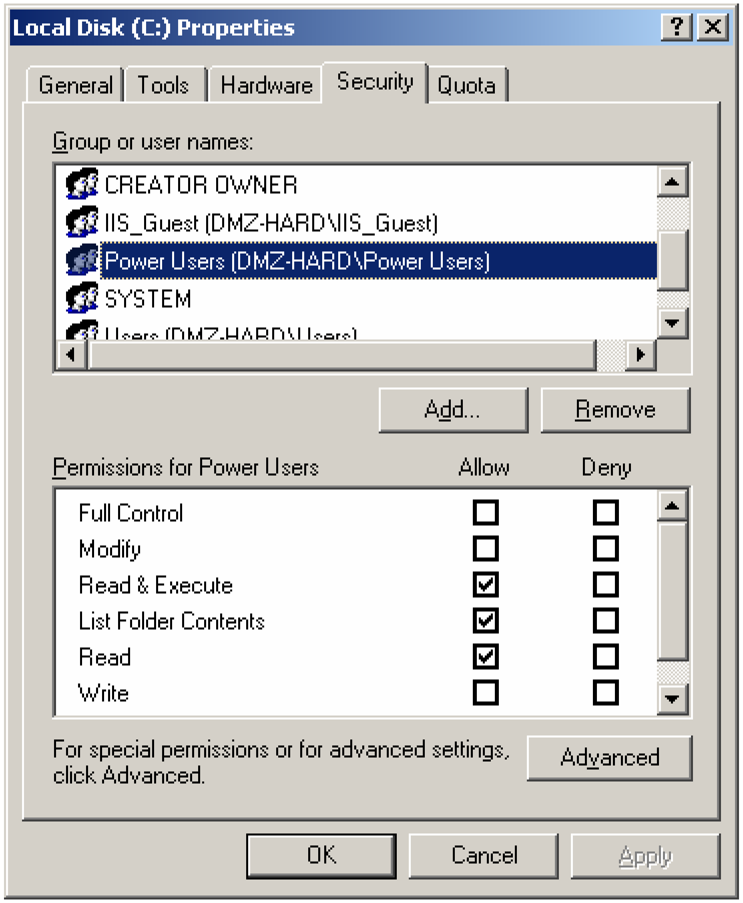
Administrators (DMZ-HARD\Administrators)
Backup Operators (DMZ-HARD\Backup Operators)
CREATOR OWNER
IIS_Guest (DMZ-HARD\IIS_Guest)
Power Users (DMZ-HARD\Power Users)

Permissions for IIS_Guest	Allow	Deny
Full Control	☐	☑
Modify	☐	☑
Read & Execute	☐	☑
List Folder Contents	☐	☑
Read	☐	☑
Write	☐	☑

For special permissions or for advanced settings, click Advanced.

Step 8.19 – Click on the **Deny** checkbox for **Full Control**.

Step 8.20 – Click on the **Add** button and add the **Power Users** Group.



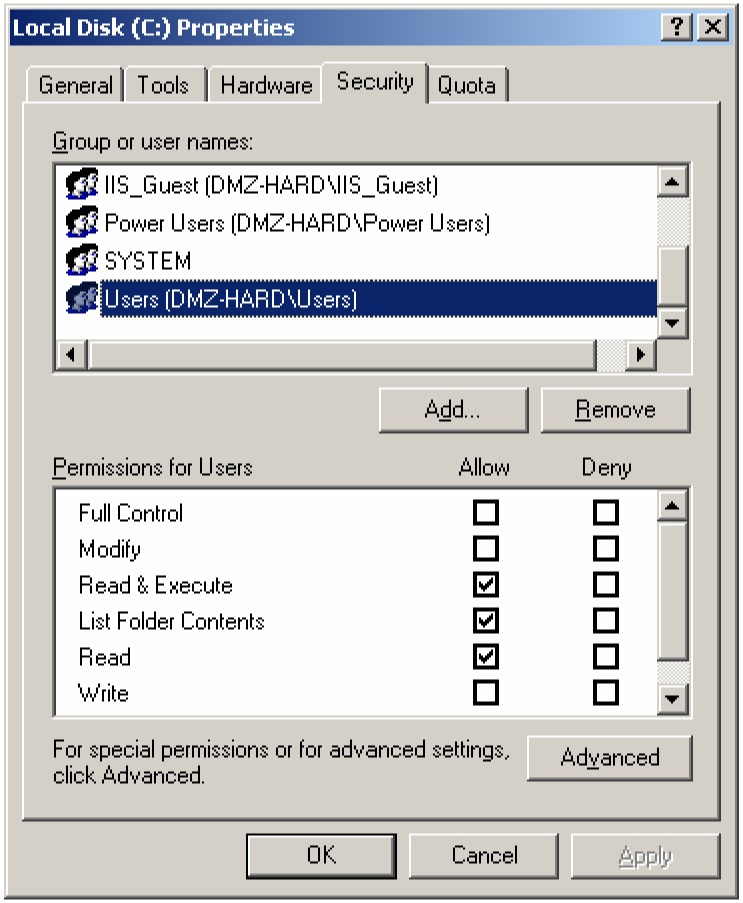
Group or user names:

- CREATOR OWNER
- IIS_Guest (DMZ-HARD\IIS_Guest)
- Power Users (DMZ-HARD\Power Users)
- SYSTEM
- Users (DMZ-HARD\Users)

Permissions for Power Users	Allow	Deny
Full Control	☐	☐
Modify	☐	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☐	☐

For special permissions or for advanced settings, click Advanced.

Step 8.21 – Ensure that the **Users** Group has permissions for **Read & Execute**, **List Folder Contents** and **Read** only.



Group or user names:

- IIS_Guest (DMZ-HARD\IIS_Guest)
- Power Users (DMZ-HARD\Power Users)
- SYSTEM
- Users (DMZ-HARD\Users)

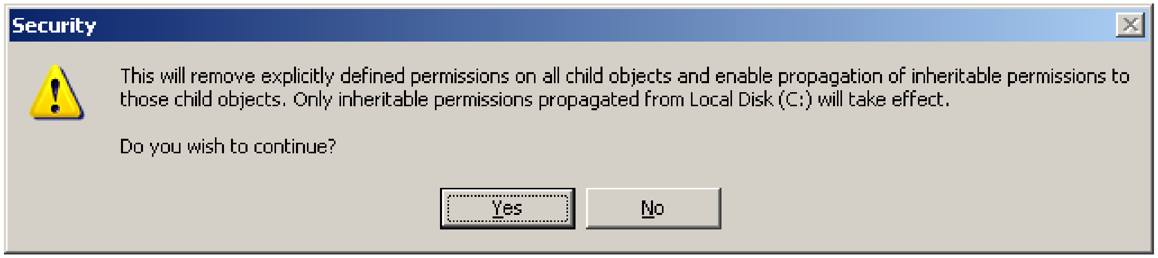
Permissions for Users	Allow	Deny
Full Control	☐	☐
Modify	☐	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☐	☐

For special permissions or for advanced settings, click Advanced.

Step 8.22 – IMPORTANT!! Click the Advanced button and place a check mark in the box labeled **Replace permission entries on all child objects with entries shown here that apply to child objects.**

Step 8.23 – Click **OK** to apply the new permissions.

A security warning should pop up that looks like this:

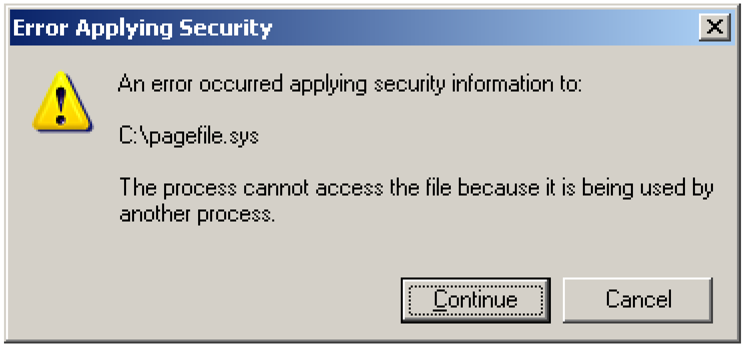


This will remove explicitly defined permissions on all child objects and enable propagation of inheritable permissions to those child objects. Only inheritable permissions propagated from Local Disk (C:) will take effect.

Do you wish to continue?

Step 8.24 – Click **Yes** to continue.

Right before completion, you will receive an Error Warning box:



Error Applying Security

An error occurred applying security information to:

C:\pagefile.sys

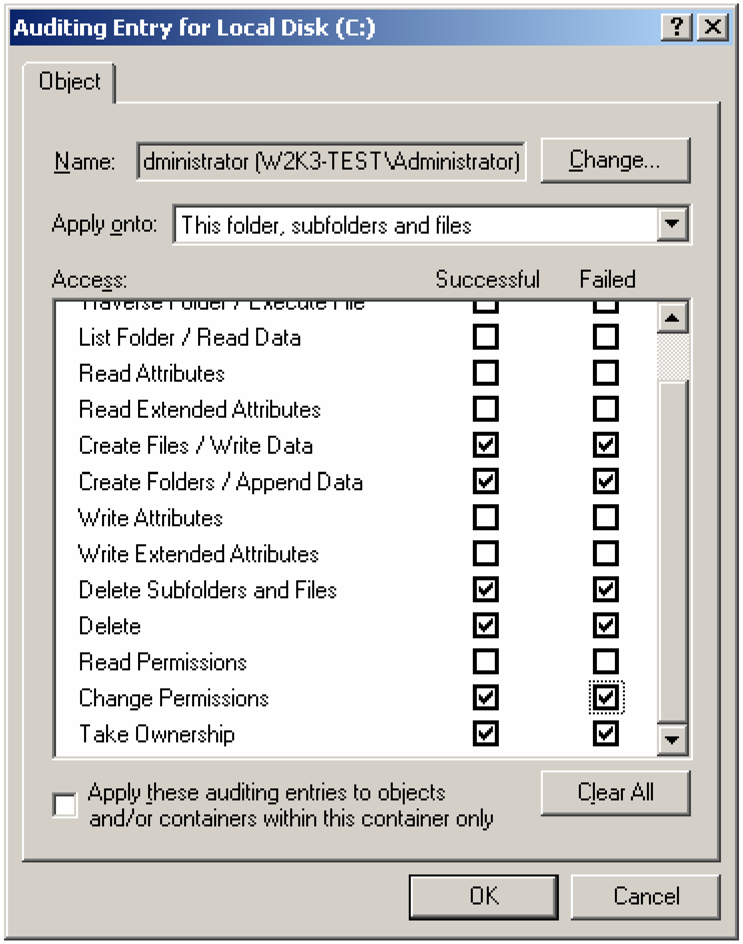
The process cannot access the file because it is being used by another process.

Step 8.25 – Click **Continue** to proceed.

Step 8.26 – Click on the **Advanced** button again and go to the **Auditing** Tab.

Step 8.27 – Click the **Add** button and add the **Administrators Group** and place a checkmark in the boxes for each of the following:

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



Auditing Entry for Local Disk (C:)

Name: dministrator (W2K3-TEST\Administrator)

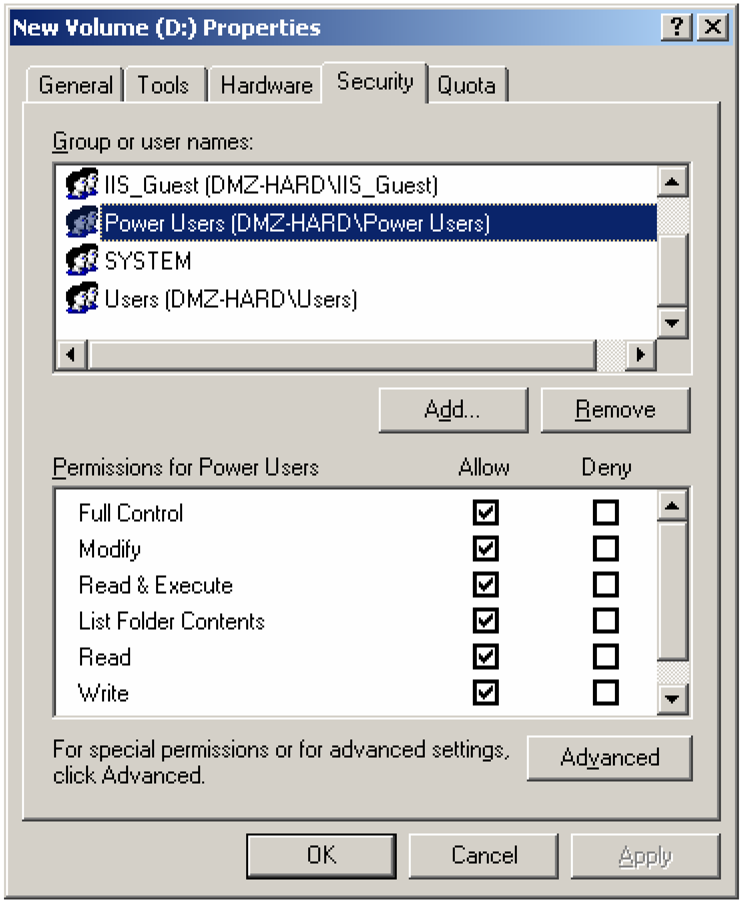
Apply onto: This folder, subfolders and files

Access:	Successful	Failed
List Folder / Read Data	☐	☐
Read Attributes	☐	☐
Read Extended Attributes	☐	☐
Create Files / Write Data	☑	☑
Create Folders / Append Data	☑	☑
Write Attributes	☐	☐
Write Extended Attributes	☐	☐
Delete Subfolders and Files	☑	☑
Delete	☑	☑
Read Permissions	☐	☐
Change Permissions	☑	☑
Take Ownership	☑	☑

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

Step 8.28 – Repeat steps (**8.26 - 8.27**) for the **Power Users** Group and the **Backup Operators** Group.

Step 8.29 – For the **E:\** partition, repeat the above steps (**8.14 - 8.27**) with the exception of the following permissions:



Group or user names:

- IIS_Guest (DMZ-HARD\IIS_Guest)
- Power Users (DMZ-HARD\Power Users)
- SYSTEM
- Users (DMZ-HARD\Users)

Permissions for Power Users	Allow	Deny
Full Control	☑	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

For special permissions or for advanced settings, click Advanced.

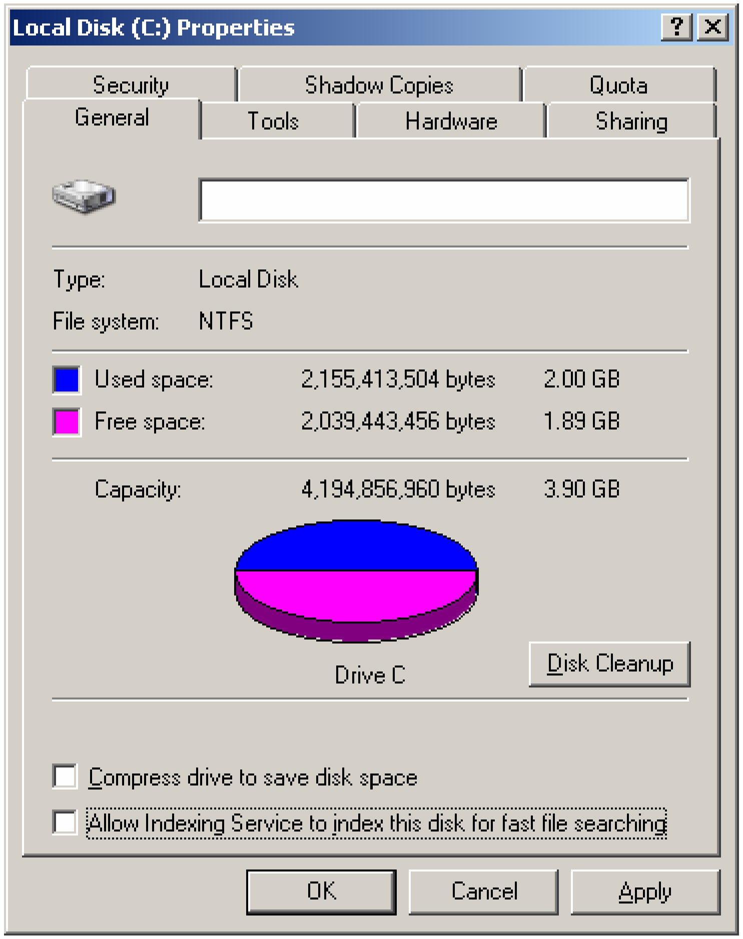
Give the **Power Users** group, full access to this partition.

Step 8.30 – Repeat the above steps (**8.14 – 8.27**) for all additional disk partitions.

Step 8.31 – Click **Apply** then click **OK**

Step 9.0 – Turn off Indexing on all Volumes

Step 9.1 – Under the **General** Tab, uncheck the box marked **Allow Indexing Service to index this disk for fast file searching**



Type: Local Disk

File system: NTFS

🟦	Used space:	2,155,413,504 bytes	2.00 GB
🟪	Free space:	2,039,443,456 bytes	1.89 GB
	Capacity:	4,194,856,960 bytes	3.90 GB

☐ Compress drive to save disk space

☐ Allow Indexing Service to index this disk for fast file searching

Click **OK**

A confirmation box reading **Confirm Attribute Changes** will pop-up.

Step 9.2 – Choose **Apply changes to C:\, subfolders and files.**

Step 9.3 – Repeat this procedure for all other hard drive partitions.

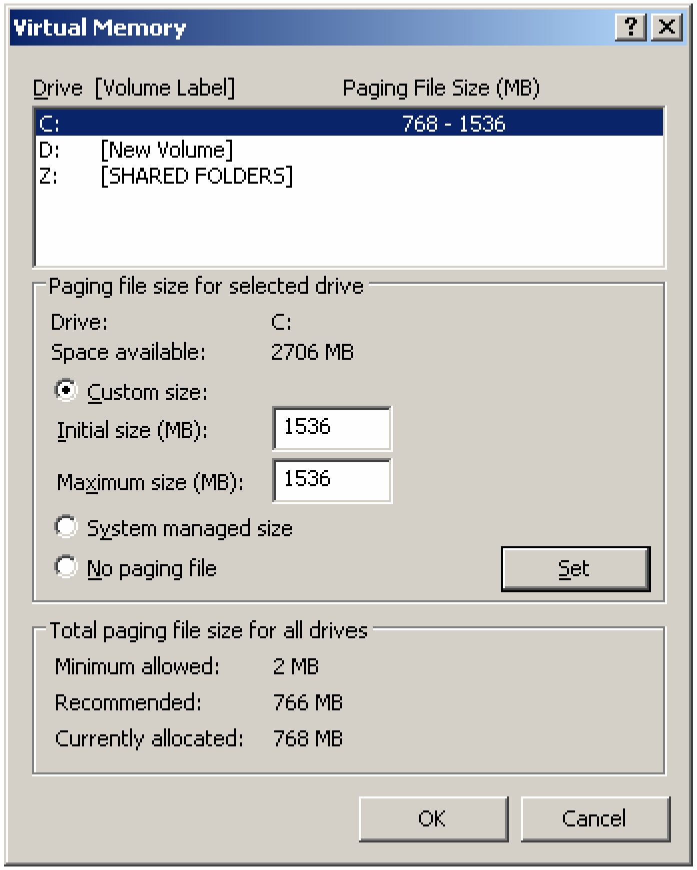
Step 10.0 – Virtual Memory Settings

Step 10.1 – Right mouse click on the **My Computer** icon and choose **Properties** and go to the **Advanced** Tab.

Step 10.2 – Under the **Performance** subsection, choose **Settings** and then click on the **Advanced** Tab.

Step 10.3 – Under the **Virtual Memory** subsection, choose **Change**.

Step 10.4 – 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 (use the Maximum figure as the value).



Virtual Memory

Drive [Volume Label]		Paging File Size (MB)
C:		768 - 1536
D:	[New Volume]	
Z:	[SHARED FOLDERS]	

Paging file size for selected drive

Drive: C:

Space available: 2706 MB

● Custom size:

Initial size (MB): 1536

Maximum size (MB): 1536

○ System managed size

○ No paging file

Total paging file size for all drives

Minimum allowed: 2 MB

Recommended: 766 MB

Currently allocated: 768 MB

Step 10.5 – Click the **Set** button.

Step 10.6 – Repeat these same steps (10.1-10.5) for all other volumes.

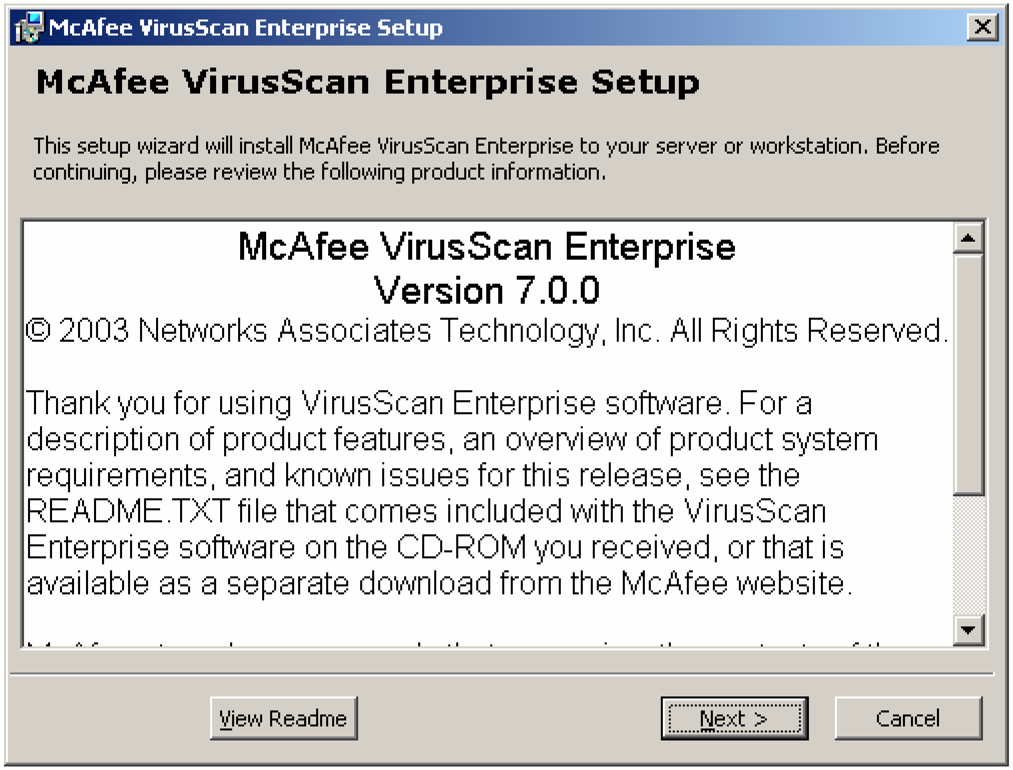
Step 10.7 – Click **OK** to get back to the System Properties window.

Step 11.0 – Installing the Anti-Virus Engine

Step 11.1 – Download a Virus Scan Engine of your choice. We recommend McAfee and this guide details the installation of that.

Step 11.2 – Create a folder and extract the Virus Scan Engine into it.

Step 11.3 – Go to the folder that you extracted the file to and double click on **vse700.msi**



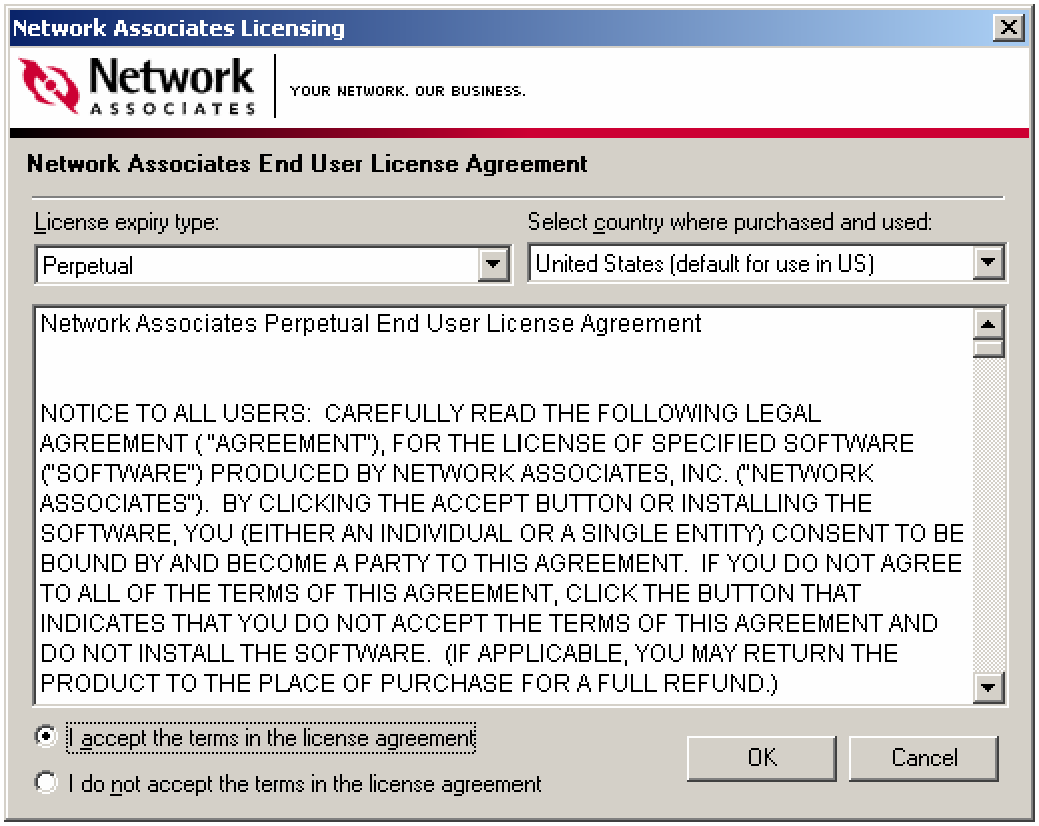
McAfee VirusScan Enterprise Setup

This setup wizard will install McAfee VirusScan Enterprise to your server or workstation. Before continuing, please review the following product information.

McAfee VirusScan Enterprise
Version 7.0.0
© 2003 Networks Associates Technology, Inc. All Rights Reserved.

Thank you for using VirusScan Enterprise software. For a description of product features, an overview of product system requirements, and known issues for this release, see the README.TXT file that comes included with the VirusScan Enterprise software on the CD-ROM you received, or that is available as a separate download from the McAfee website.

Click **Next**



Network Associates End User License Agreement

License expiry type: Perpetual

Select country where purchased and used: United States (default for use in US)

Network Associates Perpetual End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY NETWORK ASSOCIATES, INC. ("NETWORK ASSOCIATES"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

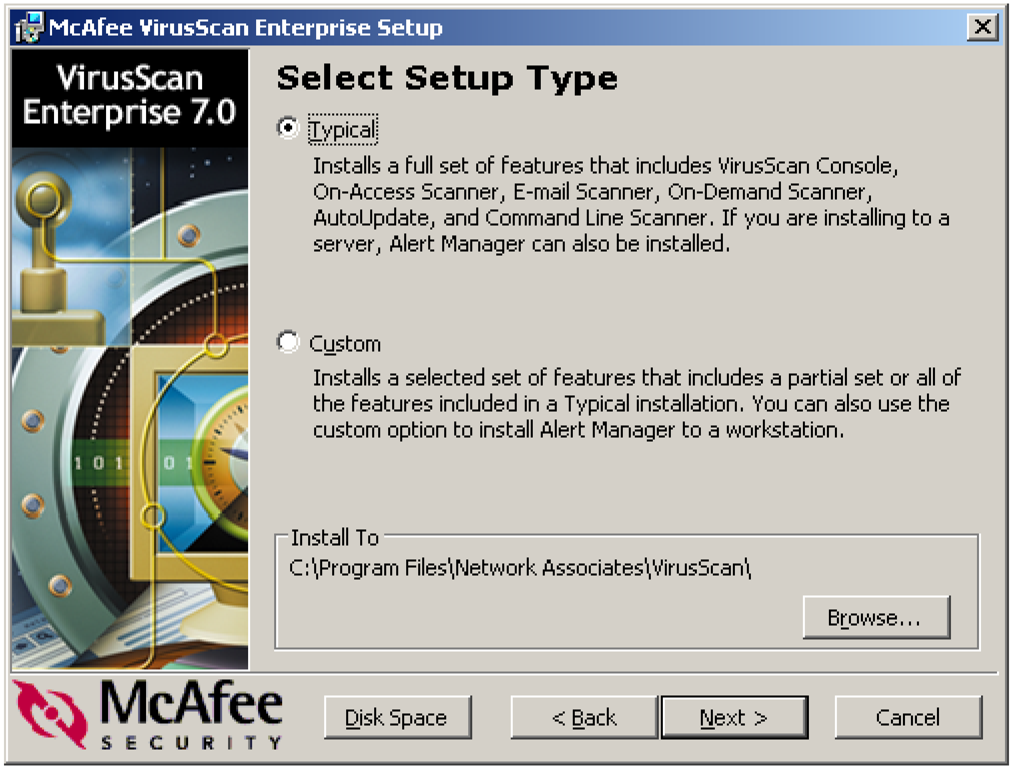
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 11.4 – Change the License expiry type to: **Perpetual**

Step 11.5 – Click on **I accept the terms in the license agreement**

Click **OK**.



● Typical

Installs a full set of features that includes VirusScan Console, On-Access Scanner, E-mail Scanner, On-Demand Scanner, AutoUpdate, and Command Line Scanner. If you are installing to a server, Alert Manager can also be installed.

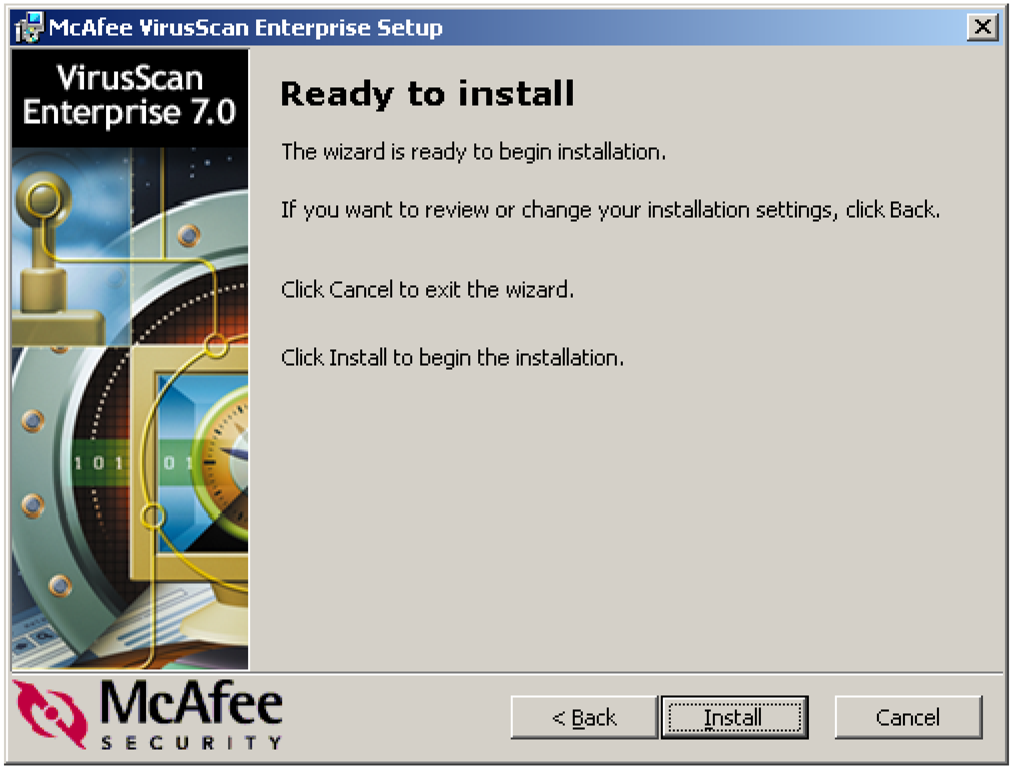
○ Custom

Installs a selected set of features that includes a partial set or all of the features included in a Typical installation. You can also use the custom option to install Alert Manager to a workstation.

Install To

C:\Program Files\Network Associates\VirusScan\

Click **Next**



Ready to install

The wizard is ready to begin installation.

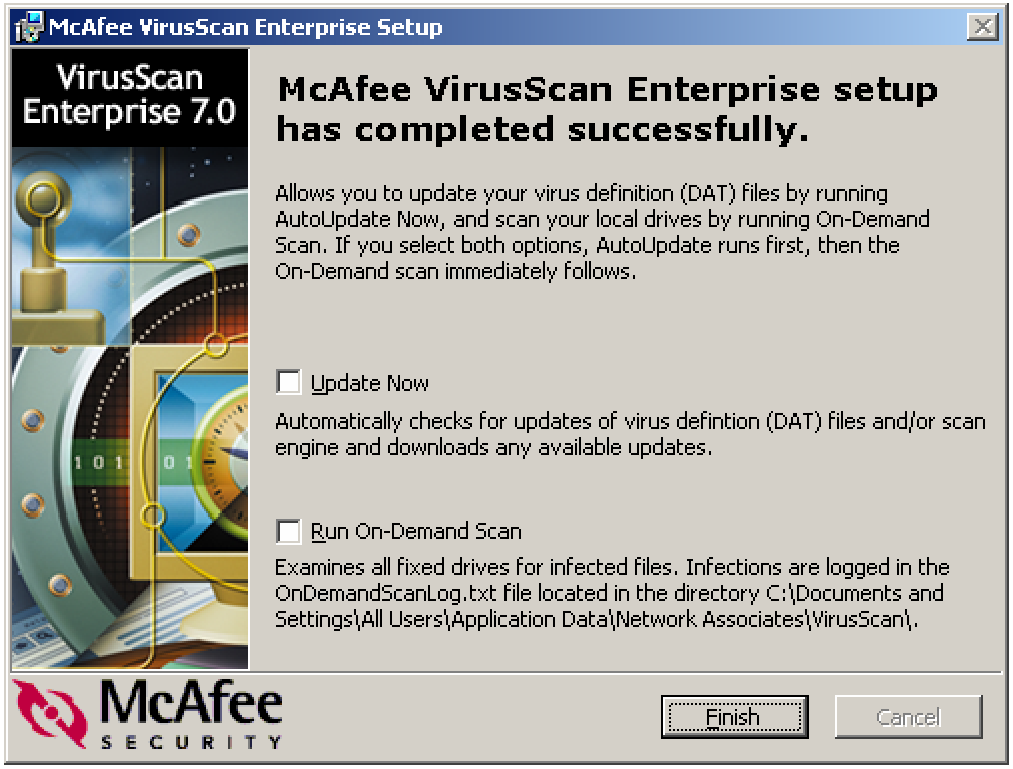
If you want to review or change your installation settings, click Back.

Click Cancel to exit the wizard.

Click Install to begin the installation.

Click **Install**

McAfee will now install the necessary drivers and files.



McAfee VirusScan Enterprise setup has completed successfully.

Allows you to update your virus definition (DAT) files by running AutoUpdate Now, and scan your local drives by running On-Demand Scan. If you select both options, AutoUpdate runs first, then the On-Demand scan immediately follows.

☐ Update Now

Automatically checks for updates of virus defintion (DAT) files and/or scan engine and downloads any available updates.

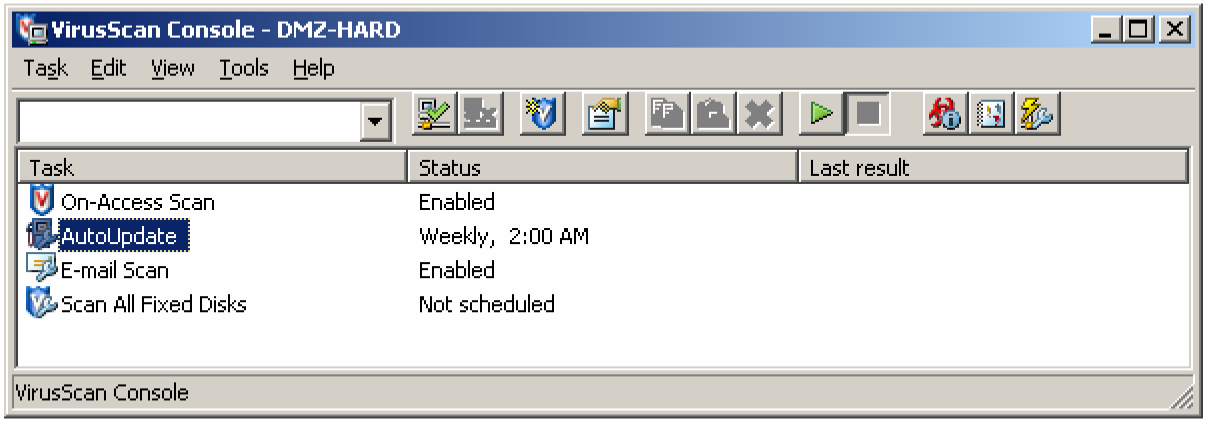
☐ Run On-Demand Scan

Examines all fixed drives for infected files. Infections are logged in the OnDemandScanLog.txt file located in the directory C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan\.

Step 11.6 – Uncheck **Update Now** and **Run On-Demand Scan**

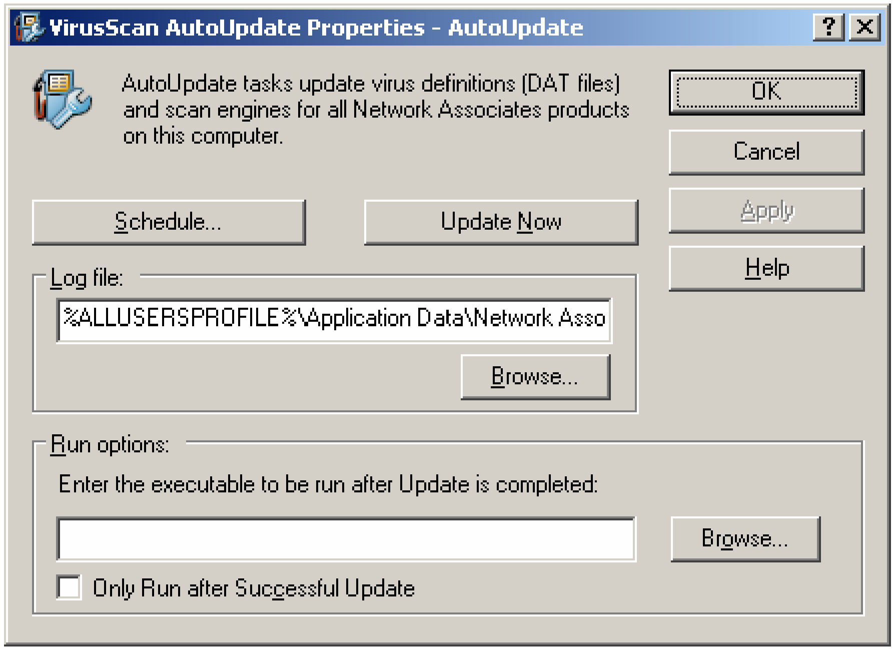
Click **Finish**

Step 11.7 – In the task bar, Right click on the McAfee Antivirus icon and choose **VirusScan Console**



Task	Status	Last result
On-Access Scan	Enabled	
AutoUpdate	Weekly, 2:00 AM	
E-mail Scan	Enabled	
Scan All Fixed Disks	Not scheduled	

Step 11.8 – Right click on **Auto Update** and select **Properties**



VirusScan AutoUpdate Properties - AutoUpdate

AutoUpdate tasks update virus definitions (DAT files) and scan engines for all Network Associates products on this computer.

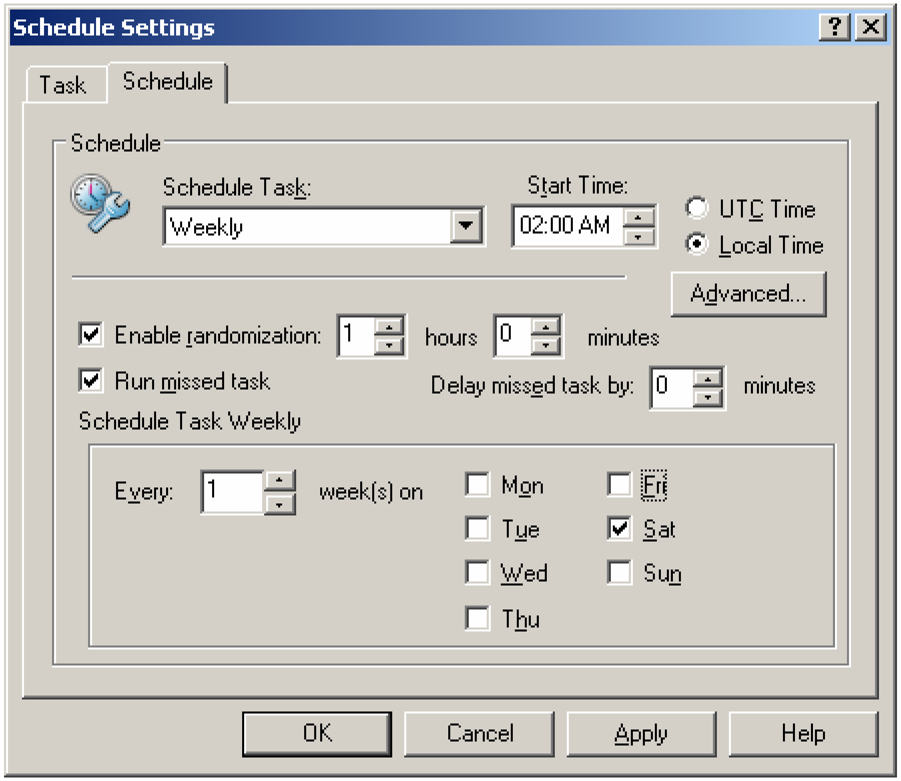
Log file: %ALLUSERSPROFILE%\Application Data\Network Asso

Run options:

Enter the executable to be run after Update is completed:

☐ Only Run after Successful Update

Step 11.9 – Click on the Schedule button



Schedule Task: Weekly

Start Time: 02:00 AM

○ UTC Time

● Local Time

☑ Enable randomization: 1 hours 0 minutes

☑ Run missed task

Delay missed task by: 0 minutes

Schedule Task Weekly

Every: 1 week(s) on

☐ Mon

☐ Tue

☐ Wed

☐ Thu

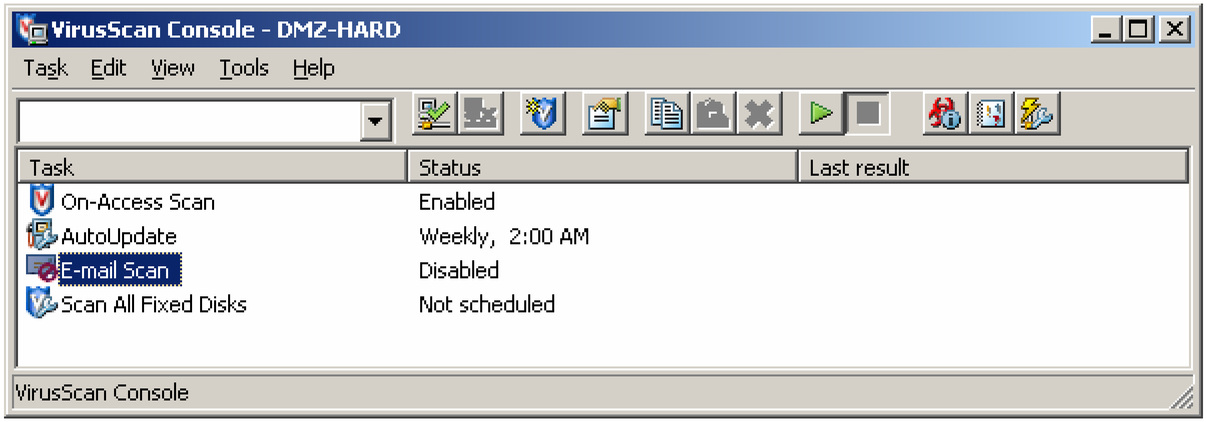
☐ Fri

☑ Sat

☐ Sun

Step 11.10 – Under the **Schedule** Tab you should schedule the Anti-Virus Update according to your needs.

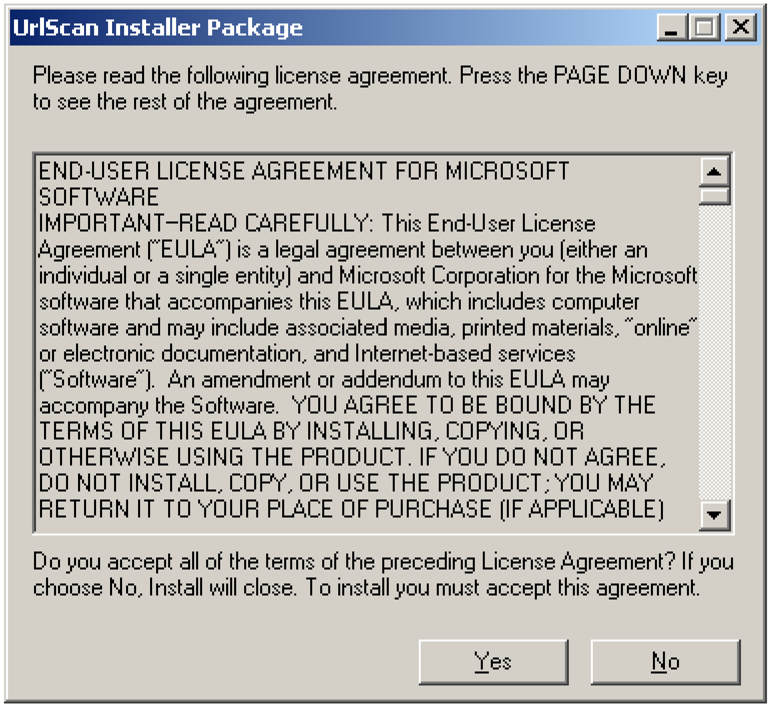
Click **Apply** then **OK**.



Task	Status	Last result
On-Access Scan	Enabled	
AutoUpdate	Weekly, 2:00 AM	
E-mail Scan	Disabled	
Scan All Fixed Disks	Not scheduled	

Step 12.0 - URL Scan Installation

Step 12.1 – Download and Double Click on the URLScan 2.5 executable.



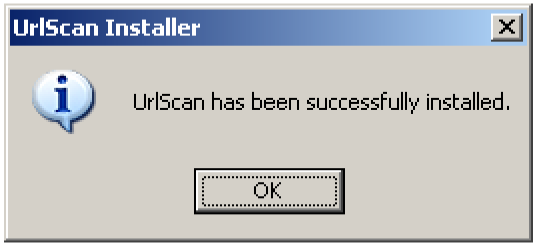
Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.

END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE
IMPORTANT–READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software that accompanies this EULA, which includes computer software and may include associated media, printed materials, "online" or electronic documentation, and Internet-based services ("Software"). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE PRODUCT. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE PRODUCT; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE (IF APPLICABLE)

Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.

Step 12.2 – Click on **Yes** to accept the EULA.

URLScan will install and you will see the screen below when it is finished.



UrlScan has been successfully installed.

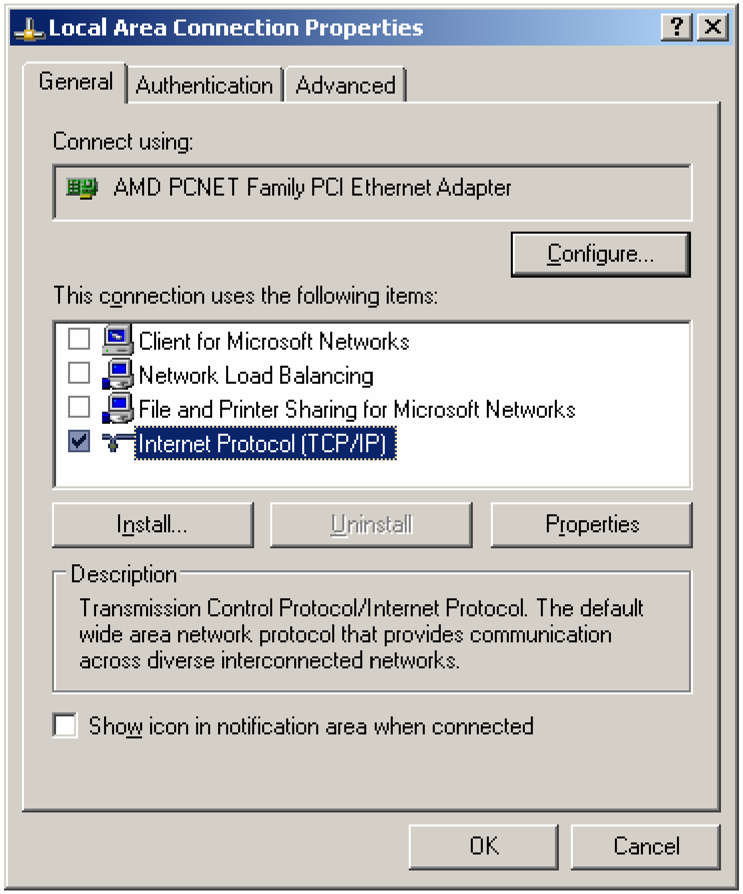
Click on **OK** to finish installation.

Step 13.0 – Disabling Protocols and Setting a Fixed IP for the Server.

Step 13.1 – Right click on **My Network Places** and choose **Properties**.

Step 13.2 – Right click on **Local Area Connection** and choose **Properties**. Choose the appropriate Local Area Connection and right click on it and choose **Properties**.

- Uncheck **Client for Microsoft Networks**
- Uncheck **File and Printer Sharing for Microsoft Networks**



Connect using:

AMD PCNET Family PCI Ethernet Adapter

This connection uses the following items:

☐ Client for Microsoft Networks
☐ Network Load Balancing
☐ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

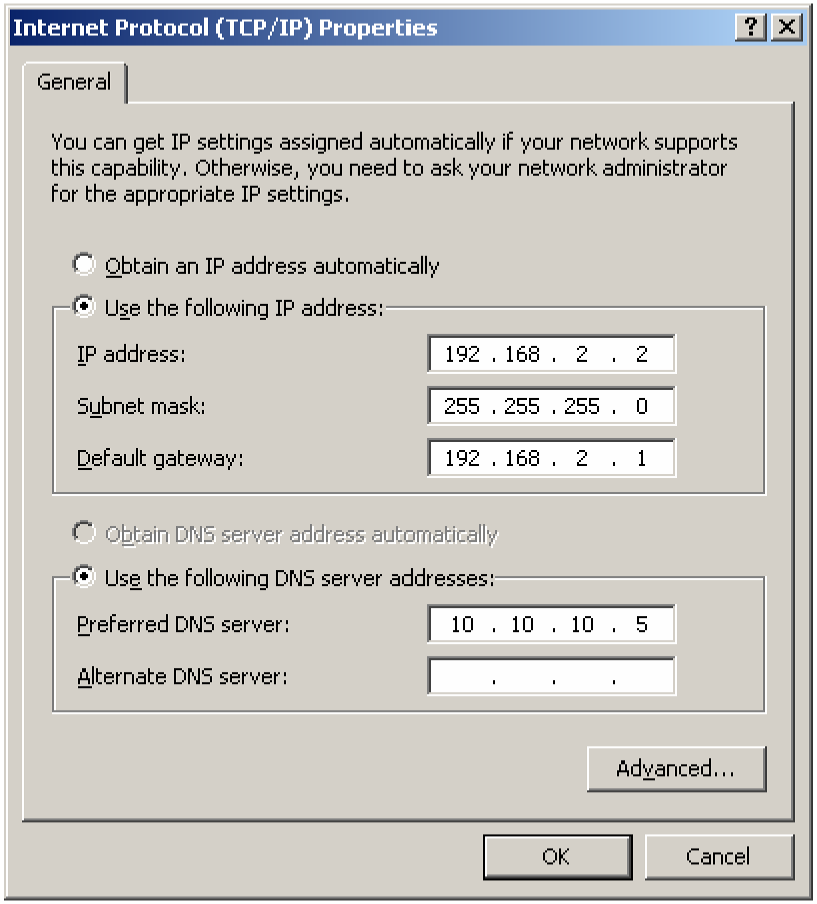
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

Step 13.3 – Select **Internet Protocol (TCP/IP)** and click on the **Properties** button.

Step 13.4 – Choose **Use the Following IP Address** and input your static IP address, Subnet Mask and Default Gateway.

Step 13.5 – Choose **Use the following DNS Server Addresses** and input your DNS Addresses. (**NOTE: The addresses in the below example are for illustration purposes only.**)



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

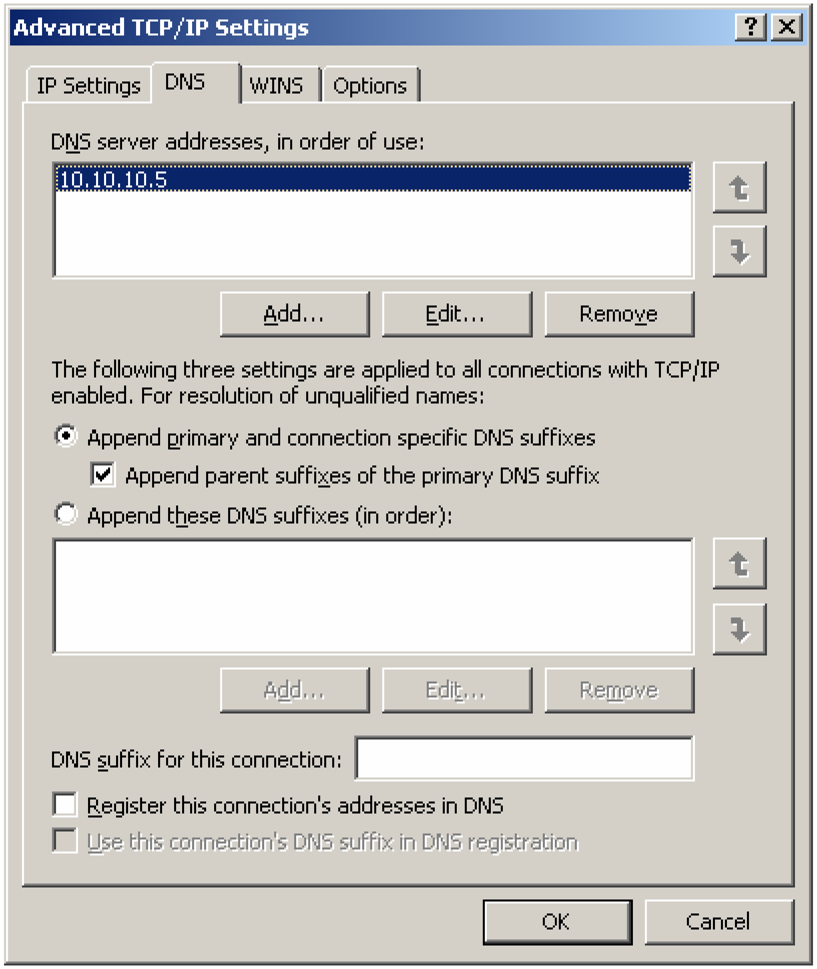
Preferred DNS server: 10 . 10 . 10 . 5

Alternate DNS server: . . .

Step 13.6 – Click on the **Advanced** button.

Under the **DNS** Tab

Step 13.7 – Uncheck **Register this connection's address in DNS.**



DNS server addresses, in order of use:

10.10.10.5

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection:

☐ Register this connection's addresses in DNS

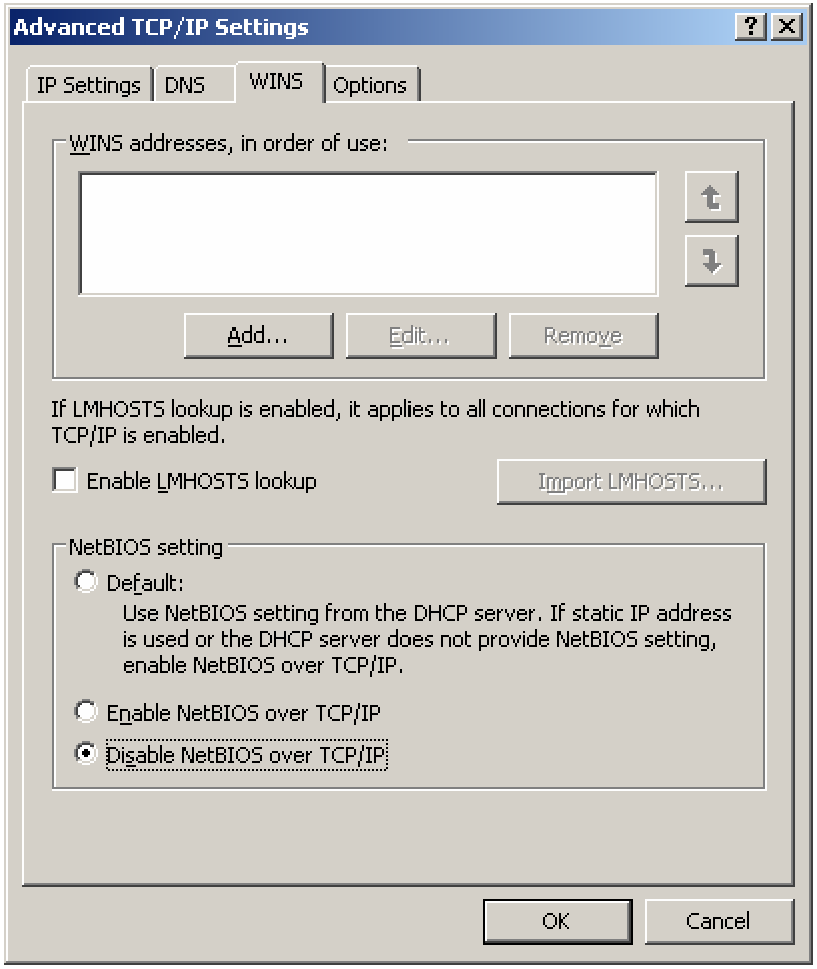
☐ Use this connection's DNS suffix in DNS registration

Under the **WINS** Tab

Step 13.8 – Remove any WINS entries if they exist.

Step 13.9 – Uncheck **Enable LMHOSTS** lookup

Step 13.10 – Choose **Disable NetBIOS over TCP/IP**



WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☐ Enable LMHOSTS lookup

NetBIOS setting

○ Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

Under the **Options** Tab

Step 13.11 – Choose **TCP/IP Filtering** and click on the **Properties** button

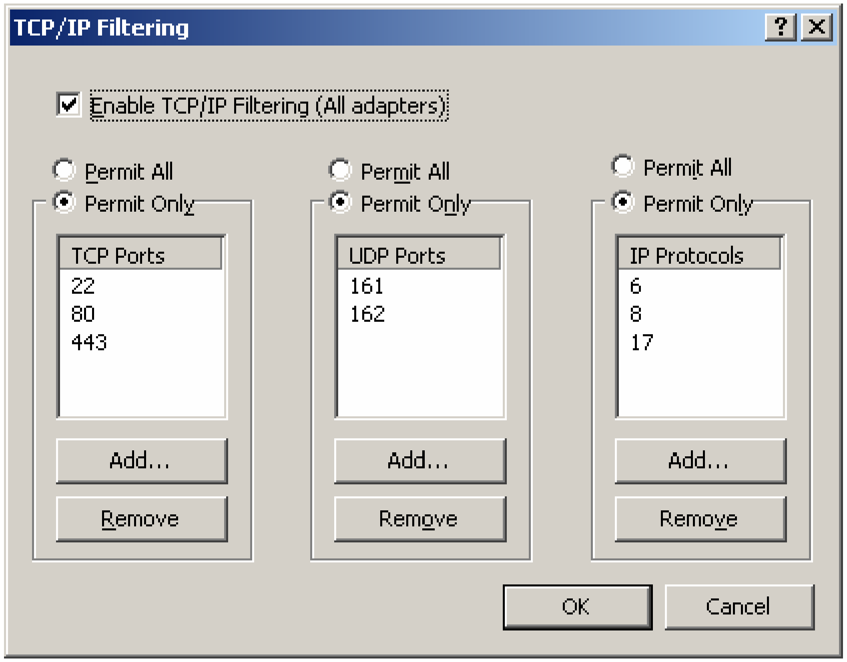
Step 13.12 – Click on **Enable TCP/IP Filtering (All adapters)**

Step 13.13 – Change the Permit All radio buttons to **Permit Only**

Step 13.14 – 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


TCP/IP Filtering

☑ Enable TCP/IP Filtering (All adapters)

○ Permit All
● Permit Only

TCP Ports
22
80
443

○ Permit All
● Permit Only

UDP Ports
161
162

○ Permit All
● Permit Only

IP Protocols
6
8
17

Click **OK** to apply the filters.

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

Click **OK** to finalize all configurations.

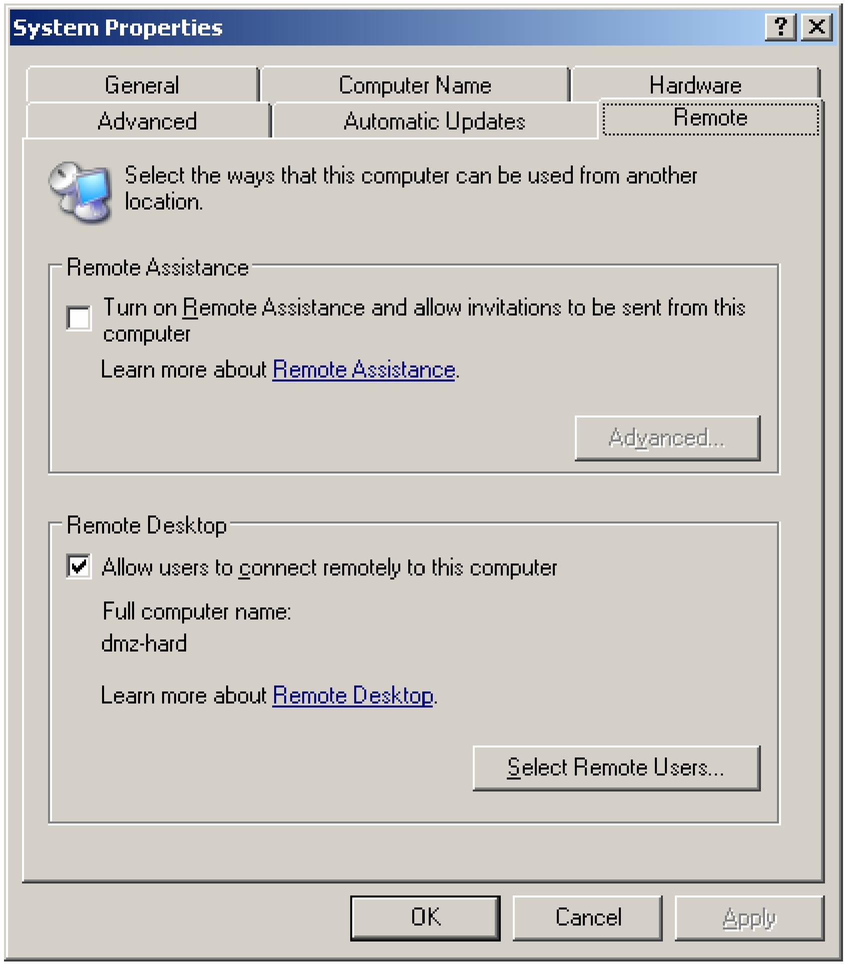
Click **Close** to close the Local Area Connection Properties.

Step 13.15 – Select **Yes** when prompted to reboot.

Step 14.0 – Turn on Remote Control

Step 14.1 – Right Click on **My Computer > Properties > Remote**

Step 14.2 – Under the Remote Desktop subsection, place a checkmark in the box.



Select the ways that this computer can be used from another location.

Remote Assistance

☐ Turn on Remote Assistance and allow invitations to be sent from this computer

Learn more about Remote Assistance.

Remote Desktop

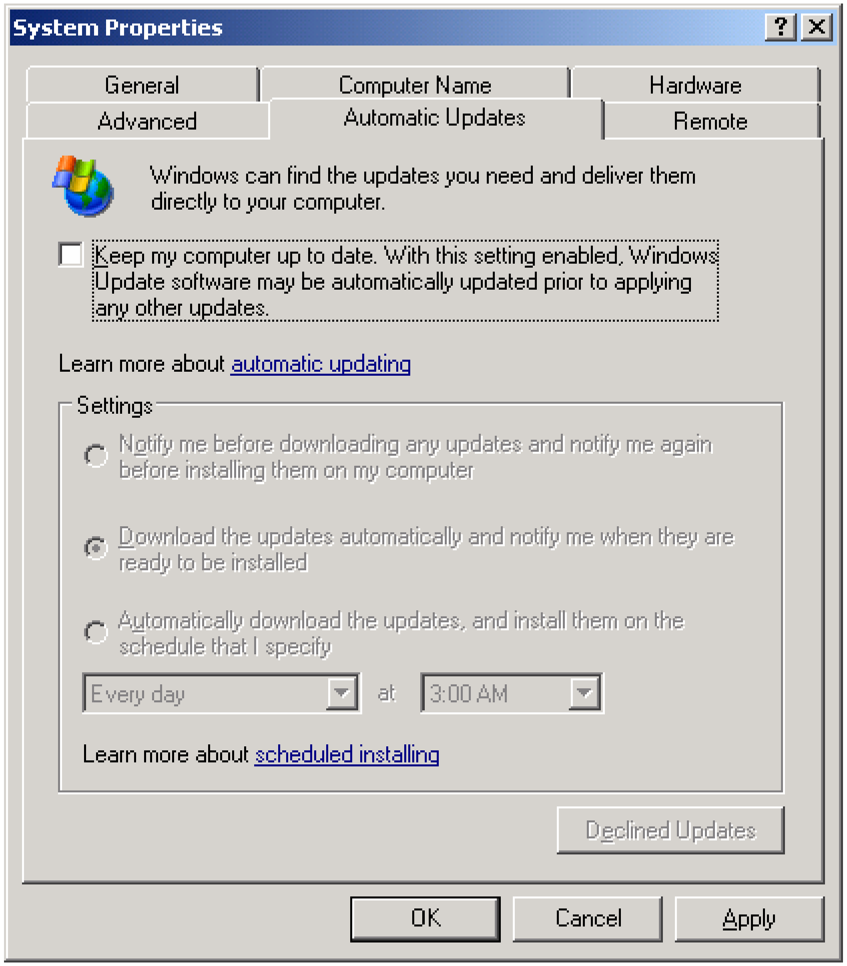
☑ Allow users to connect remotely to this computer

Full computer name:
dmz-hard

Learn more about Remote Desktop.

Step 15.0 – Turn off Automatic Upgrades

Step 15.1 – Right Click on **My Computer > Properties > Automatic Updates**



Windows can find the updates you need and deliver them directly to your computer.

☐ Keep my computer up to date. With this setting enabled, Windows Update software may be automatically updated prior to applying any other updates.

Learn more about automatic updating

○ Notify me before downloading any updates and notify me again before installing them on my computer

● Download the updates automatically and notify me when they are ready to be installed

○ Automatically download the updates, and install them on the schedule that I specify

Every day at 3:00 AM

Learn more about scheduled installing

Step 15.2 – Uncheck the **Keep my computer up to date** box.

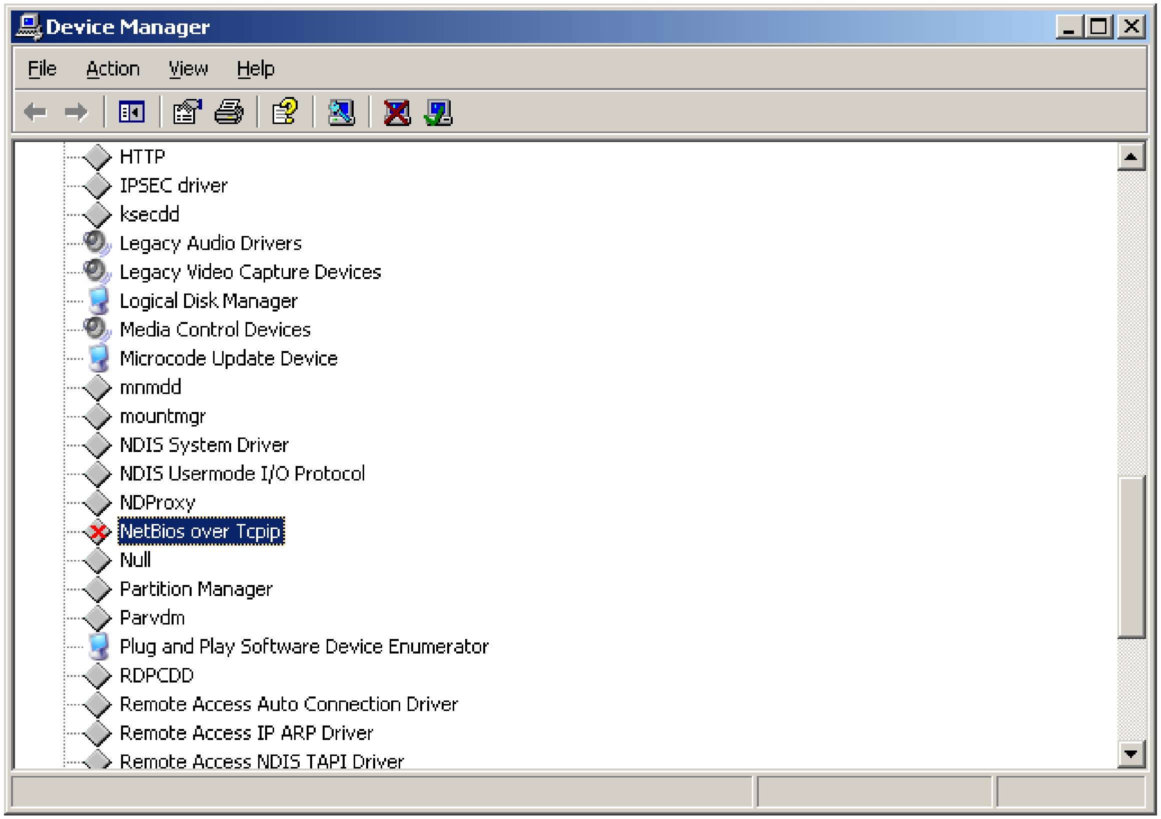
Step 16.0 - Disable NetBIOS over TCP/IP

Step 16.1 – Click on **Hardware** Tab **> Device Manager** box.

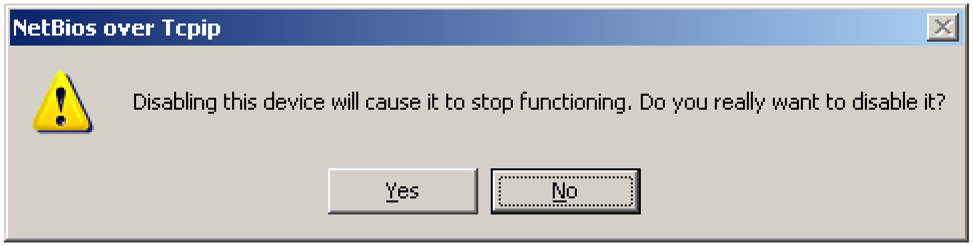
Step 16.2 – Click on **View > Show Hidden Devices**

Step 16.3 – Click on **View > Devices by Connection**

Step 16.4 – Right click on **NetBios over Tcpip** > **Properties > Disable**

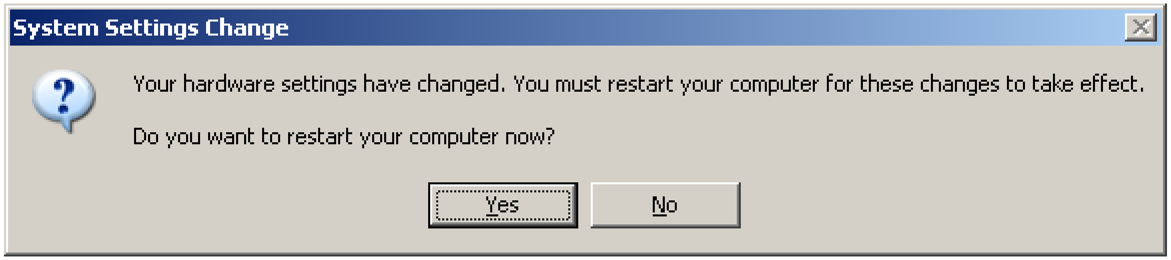


A pop up window should open that looks like this:



Disabling this device will cause it to stop functioning. Do you really want to disable it?

Choose **Yes**



Your hardware settings have changed. You must restart your computer for these changes to take effect.

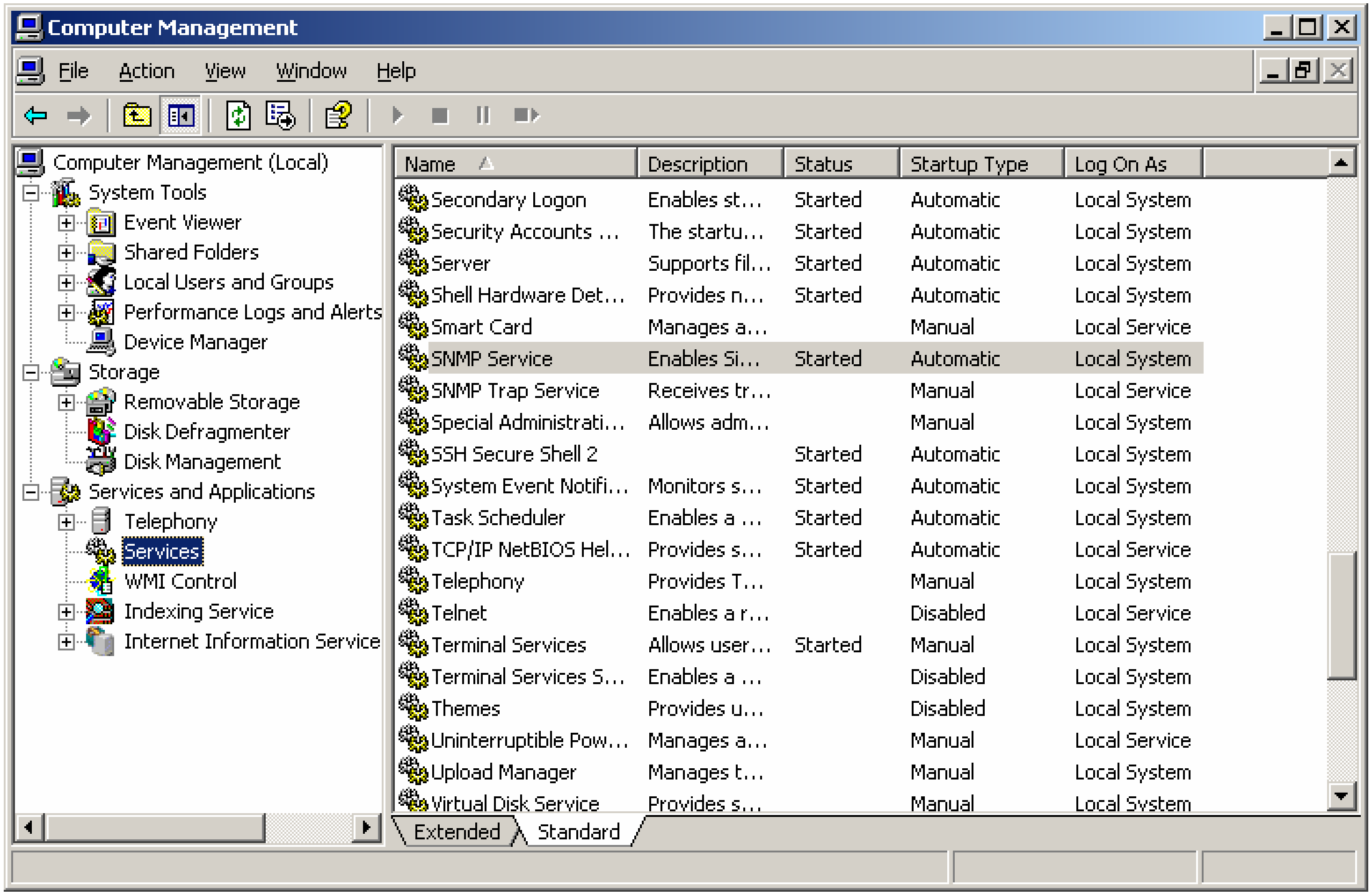
Do you want to restart your computer now?

Choose **Yes** when prompted to reboot.

Step 17.0 - SNMP Community String

Step 17.1 – Right Click on **My Computer** > **Manage**

Step 17.2 – Under **Services and Applications**, select **Services**



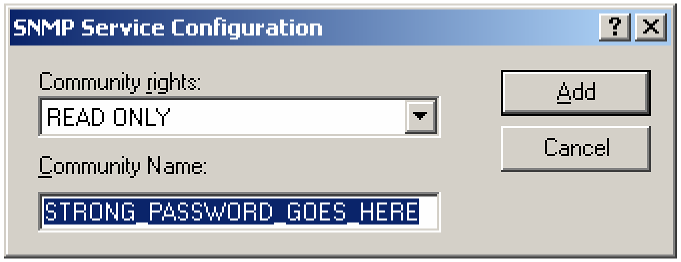
Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables st...	Started	Automatic	Local System
Security Accounts ...	The startu...	Started	Automatic	Local System
Server	Supports fil...	Started	Automatic	Local System
Shell Hardware Det...	Provides n...	Started	Automatic	Local System
Smart Card	Manages a...		Manual	Local Service
SNMP Service	Enables Si...	Started	Automatic	Local System
SNMP Trap Service	Receives tr...		Manual	Local Service
Special Administrati...	Allows adm...		Manual	Local System
SSH Secure Shell 2		Started	Automatic	Local System
System Event Notifi...	Monitors s...	Started	Automatic	Local System
Task Scheduler	Enables a ...	Started	Automatic	Local System
TCP/IP NetBIOS Hel...	Provides s...	Started	Automatic	Local Service
Telephony	Provides T...		Manual	Local System
Telnet	Enables a r...		Disabled	Local Service
Terminal Services	Allows user...	Started	Manual	Local System
Terminal Services S...	Enables a ...		Disabled	Local System
Themes	Provides u...		Disabled	Local System
Uninterruptible Pow...	Manages a...		Manual	Local Service
Upload Manager	Manages t...		Manual	Local System
Virtual Disk Service	Provides s...		Manual	Local System

Step 17.3 – Scroll Down and right click on **SNMP Service** and select **Properties**

Under the **Security** Tab

Step 17.4 – Ensure that **Send authentication trap** is selected.

Step 17.5 – Click **Add**



Community rights: READ ONLY

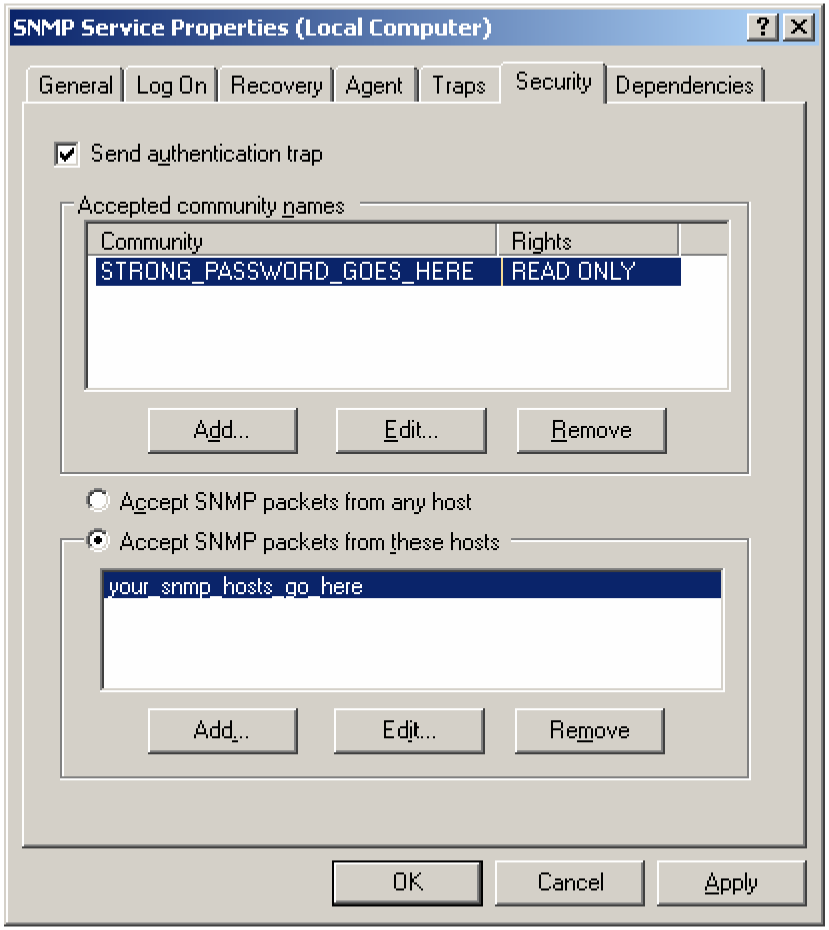
Community Name: STRONG_PASSWORD_GOES_HERE

Step 17.6 – Select **READ ONLY** for Community Rights

Step 17.7 – 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 17.8 – Choose **Accept SNMP packets from these hosts**.

Step 17.9 – Click **Add** and add the addresses from your SNMP network



☑ Send authentication trap

Accepted community names

Community	Rights
STRONG_PASSWORD_GOES_HERE	READ ONLY

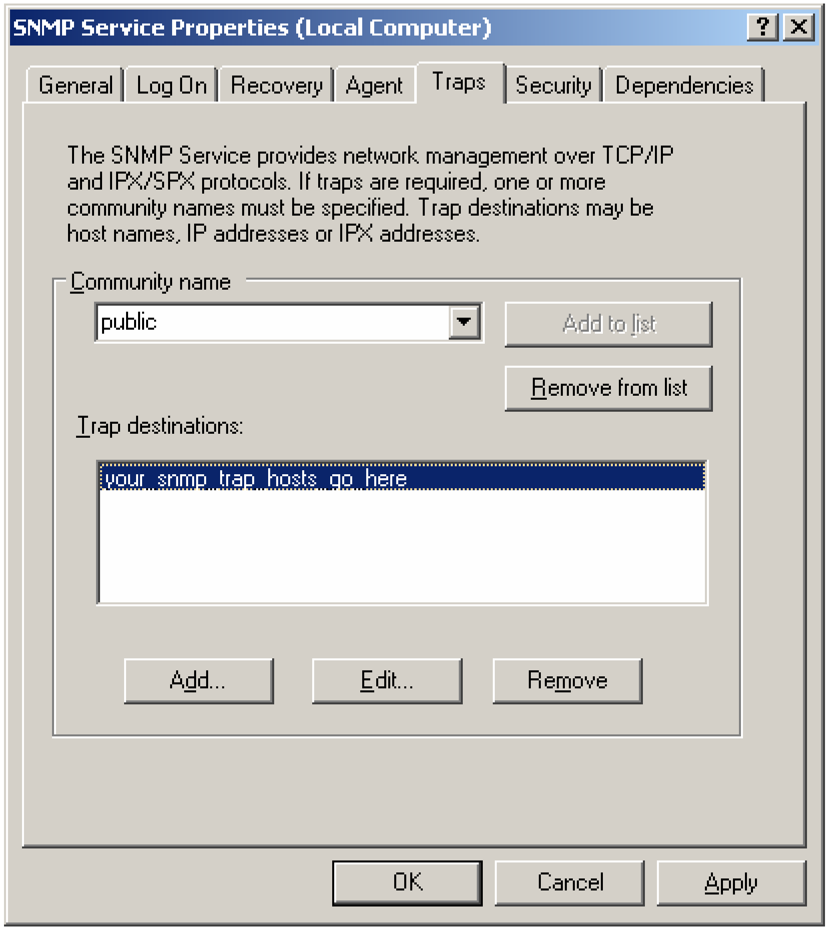
○ Accept SNMP packets from any host

● Accept SNMP packets from these hosts

your_snmp_hosts_go_here

Step 17.10 – Click on the **Traps** Tab and in the Community Name white-space, type: **public**

Step 17.11 – Click on the **Add** button and add the addresses of your trap destinations



The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.

Community name: public

Trap destinations: your_snmp_trap_hosts_go_here

Step 17.12 – Click **Apply** then click **OK** to exit.

Step 17.13 – Close the Computer Management window.

Step 18.0 – Setup the IPSec Policy

Step 18.1 – Download the IPSec Policy File.

Step 18.2 – 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 6.0 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
ICMP	ICMP	ANY	ANY	ANY	ME	ALLOW	YES
All Other Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

Step 18.3 – You can copy and paste the lines from the file into a command shell window to install the policy.

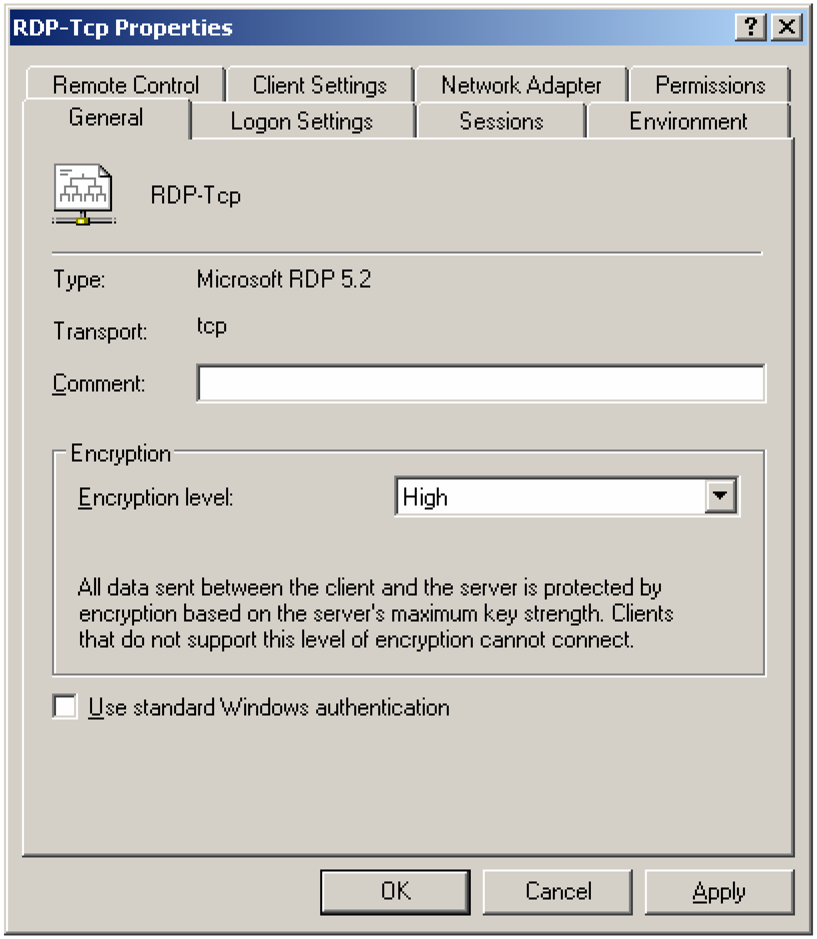
Step 19.0 - Configure Terminal Services

Step 19.1 – Go to **Start > Programs > Administrative Tools > Terminal Services Configuration (TSC).**

Step 19.2 – Over in the right panel, right mouse click on **RDP-Tcp** and choose **Properties**.

Under the General Tab:

Step 19.3 – Change the Encryption Level to **High**.



Type: Microsoft RDP 5.2

Transport: tcp

Comment:

Encryption level: High

All data sent between the client and the server is protected by encryption based on the server's maximum key strength. Clients that do not support this level of encryption cannot connect.

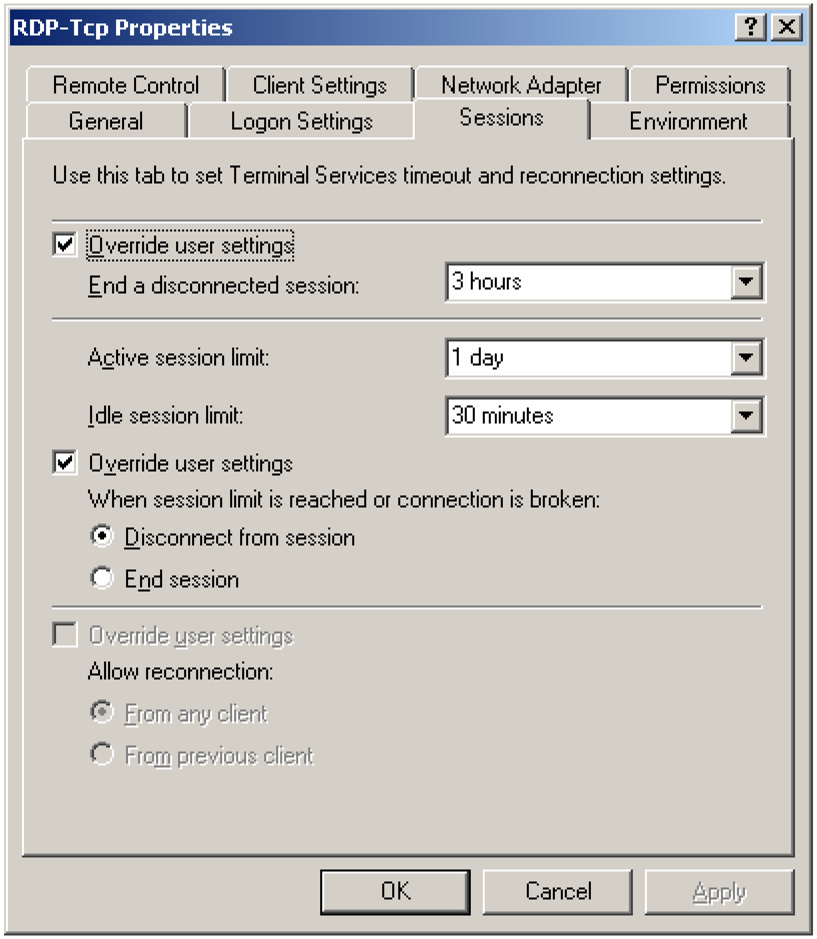
☐ Use standard Windows authentication

Under the **Sessions** Tab

Step 19.4 – Check the first **Override User Settings**, then choose:

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

Step 19.5 – Check the second **Override User Settings** and choose: **Disconnect from Session.**



Use this tab to set Terminal Services timeout and reconnection settings.

☑ Override user settings

End a disconnected session: 3 hours

Active session limit: 1 day

Idle session limit: 30 minutes

☑ Override user settings

When session limit is reached or connection is broken:

● Disconnect from session

○ End session

☐ Override user settings

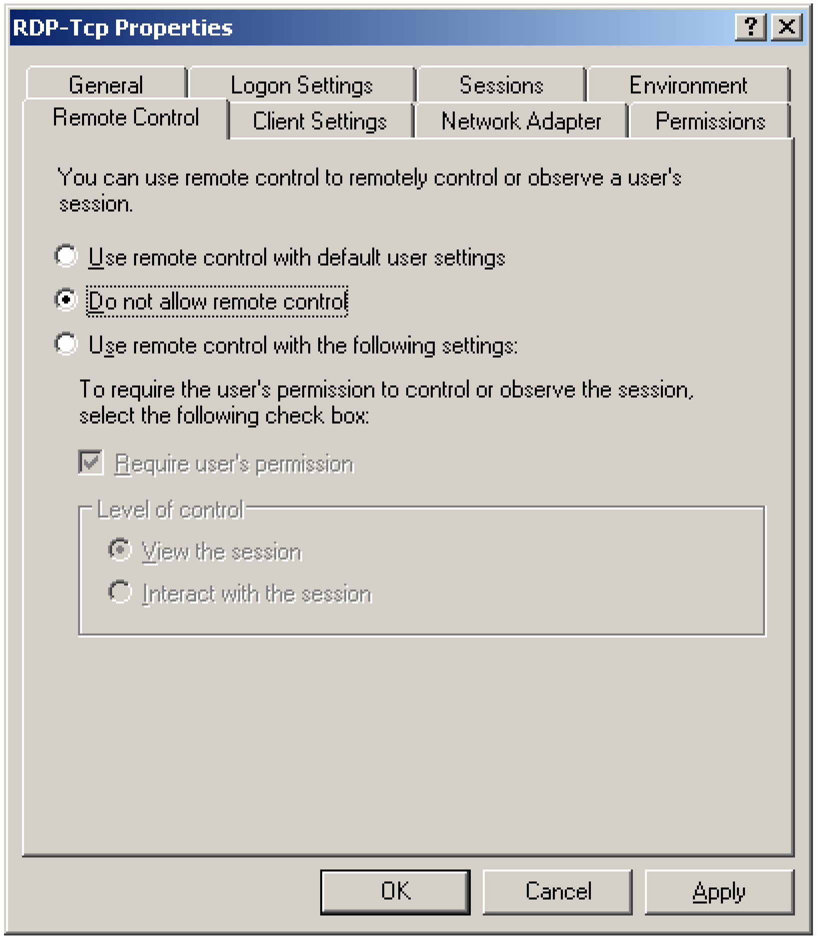
Allow reconnection:

● From any client

○ From previous client

Under the **Remote Control** Tab

Step 19.6 – Choose **Do not allow remote control**



You can use remote control to remotely control or observe a user's session.

○ Use remote control with default user settings
● Do not allow remote control
○ Use remote control with the following settings:

To require the user's permission to control or observe the session, select the following check box:

☑ Require user's permission

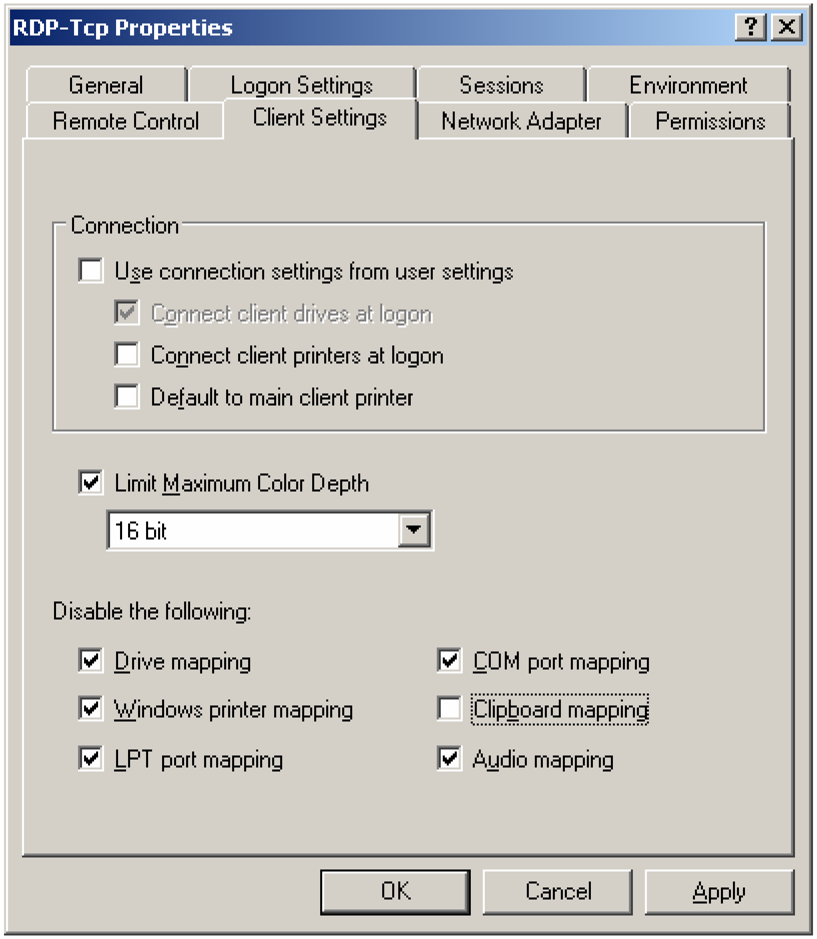
Level of control
● View the session
○ Interact with the session

Under the Client Settings Tab:

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

Under the Disable subsection:

Step 19.7 – Check all boxes except **Clipboard Mapping**.



Connection

☐ Use connection settings from user settings

☑ Connect client drives at logon

☐ Connect client printers at logon

☐ Default to main client printer

☑ Limit Maximum Color Depth

16 bit

Disable the following:

☑ Drive mapping

☑ Windows printer mapping

☑ LPT port mapping

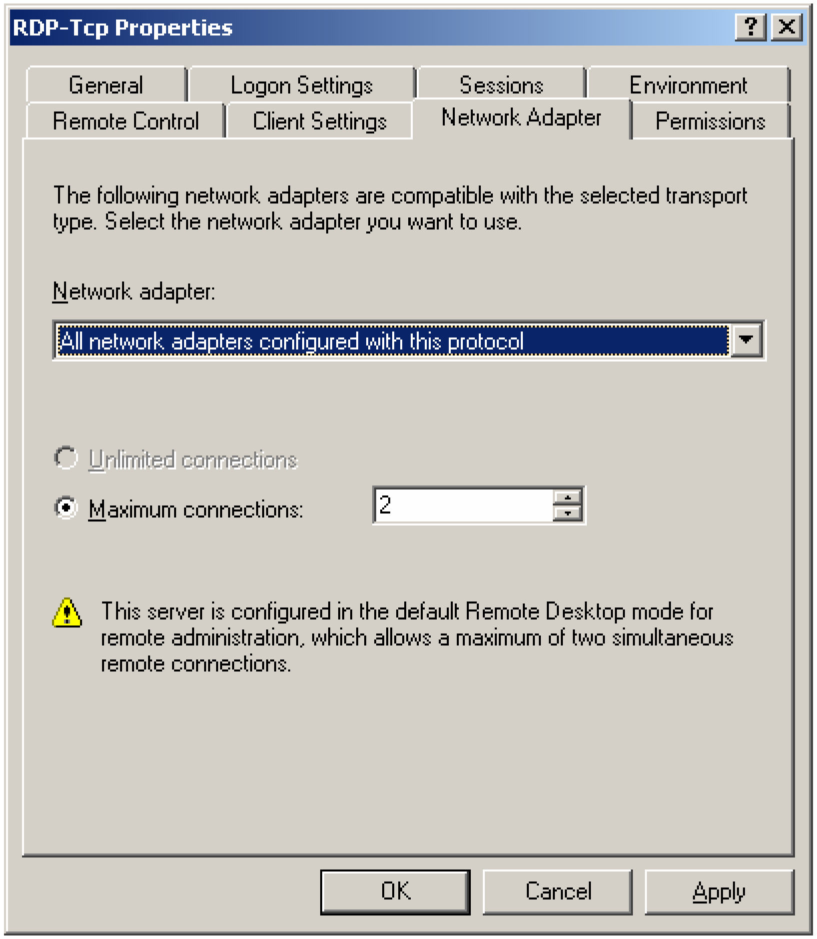
☑ COM port mapping

☐ Clipboard mapping

☑ Audio mapping

Under the Network Adapter Tab:

Step 19.8 – Click on the **Maximum Connections** radio button and ensure the number is set to 2.



The following network adapters are compatible with the selected transport type. Select the network adapter you want to use.

Network adapter: All network adapters configured with this protocol

○ Unlimited connections

● Maximum connections: 2

This server is configured in the default Remote Desktop mode for remote administration, which allows a maximum of two simultaneous remote connections.

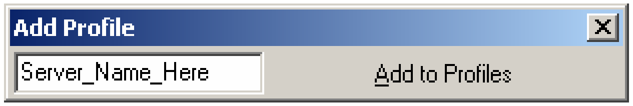
Step 19.9 – Click **Apply** and then close the window.

Step 20.0 - Set up Terminal Services to run over SSH

Step 20.1 – Open the SSH Secure Shell Client

Step 20.2 – Select the folder named **Profiles** > **Add Profile**

Step 20.3 – Give the Profile a Name and then click the **Add to Profiles** button.



Server_Name_Here

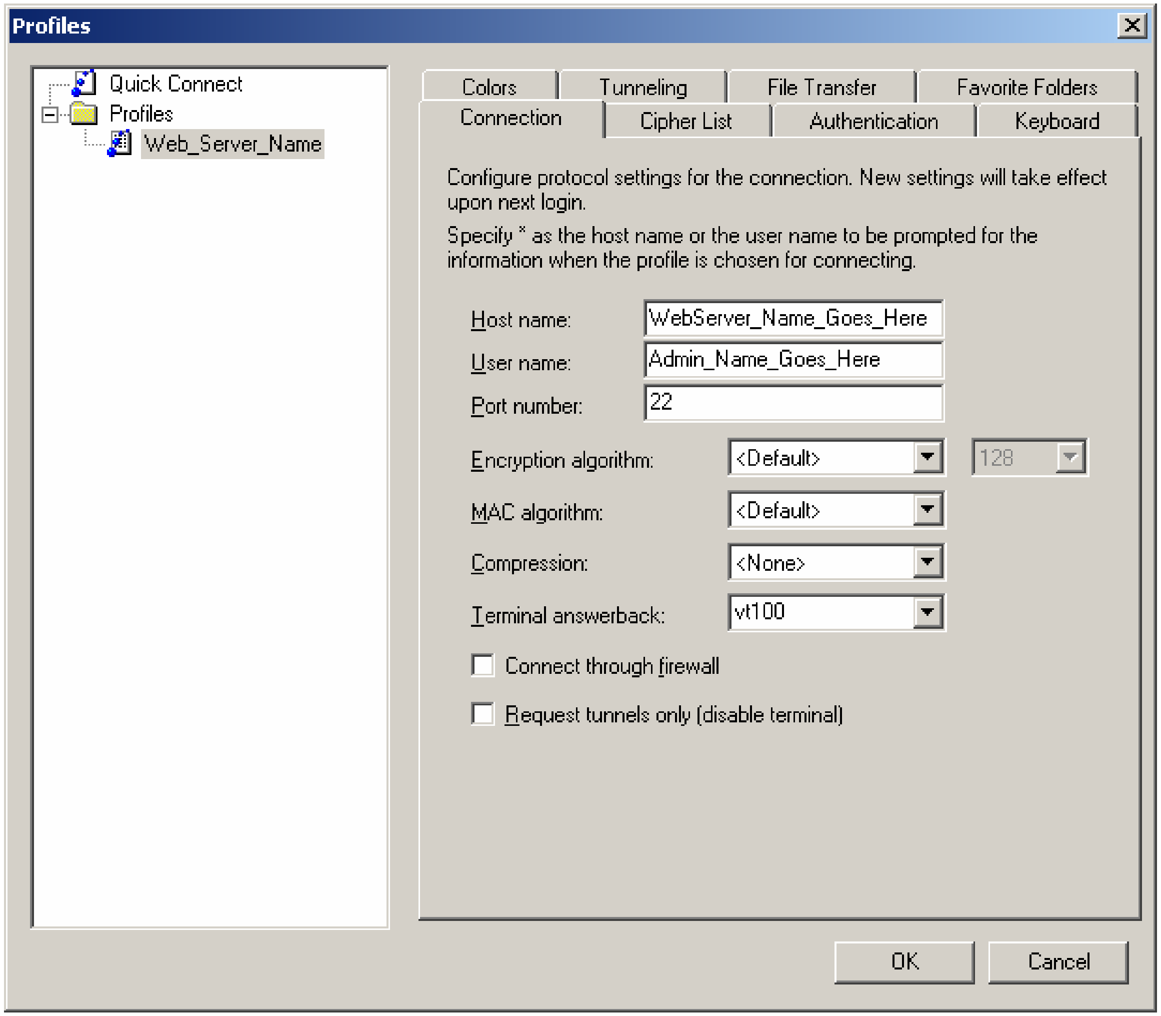
Step 20.4 – Select **Profiles** folder again and select **Edit Profile**.

Step 20.5 - 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 23.2**



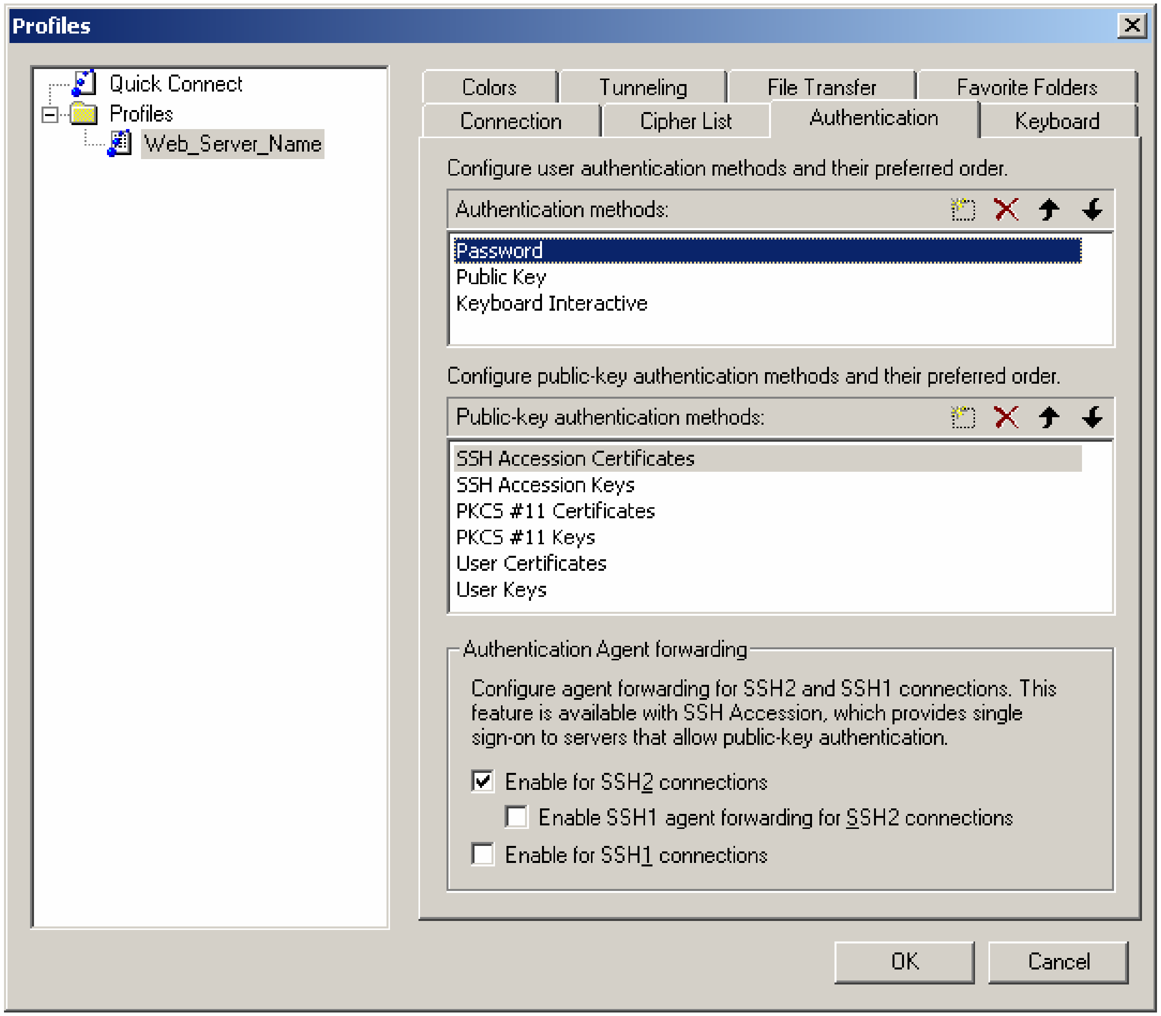
Configure protocol settings for the connection. New settings will take effect upon next login.

Specify * as the host name or the user name to be prompted for the information when the profile is chosen for connecting.

Host name: WebServer_Name_Goes_Here
User name: Admin_Name_Goes_Here
Port number: 22
Encryption algorithm: <Default> 128
MAC algorithm: <Default>
Compression: <None>
Terminal answerback: vt100
☐ Connect through firewall
☐ Request tunnels only (disable terminal)

Under the Authentication Tab:

Step 20.6 – Under **Authentication methods**, choose **Password**. Move Password to the TOP of the list using the black arrows.



Configure user authentication methods and their preferred order.

Authentication methods:

- Password
- Public Key
- Keyboard Interactive

Configure public-key authentication methods and their preferred order.

Public-key authentication methods:

- SSH Accession Certificates
- SSH Accession Keys
- PKCS #11 Certificates
- PKCS #11 Keys
- User Certificates
- User Keys

Authentication Agent forwarding

Configure agent forwarding for SSH2 and SSH1 connections. This feature is available with SSH Accession, which provides single sign-on to servers that allow public-key authentication.

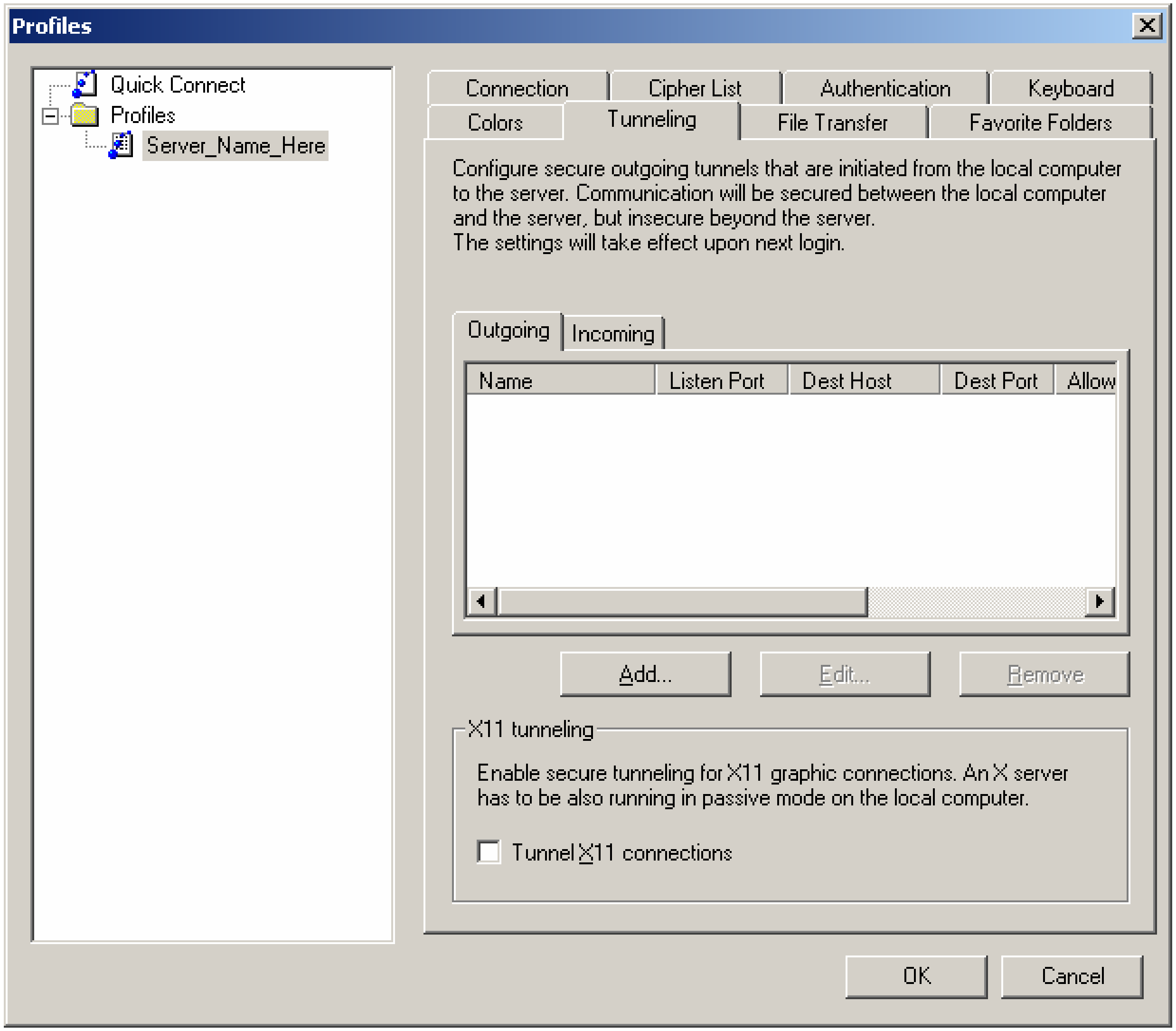
☑ Enable for SSH2 connections

  ☐ Enable SSH1 agent forwarding for SSH2 connections

☐ Enable for SSH1 connections

Under the Tunneling Tab:

Step 20.7 – Ensure that the **Outgoing** frame is selected and click on the **Add** button.



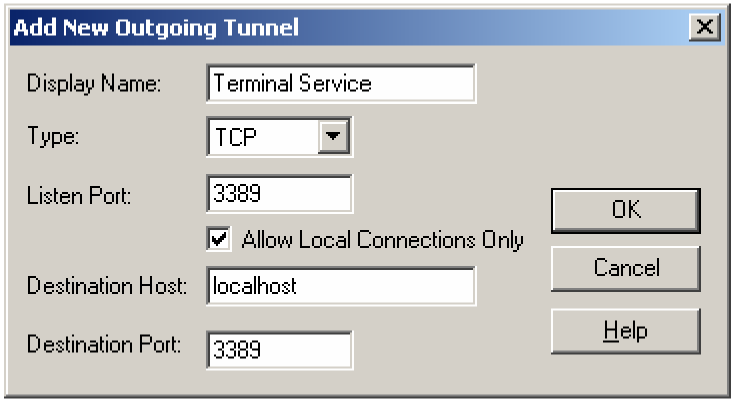
Configure secure outgoing tunnels that are initiated from the local computer to the server. Communication will be secured between the local computer and the server, but insecure beyond the server.
The settings will take effect upon next login.

Enable secure tunneling for X11 graphic connections. An X server has to be also running in passive mode on the local computer.

☐ Tunnel X11 connections

Step 20.8 - When the **Add New Outgoing Tunnel** prompt comes up fill in the following information:

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



Add New Outgoing Tunnel

Display Name: Terminal Service

Type: TCP

Listen Port: 3389

☑ Allow Local Connections Only

Destination Host: localhost

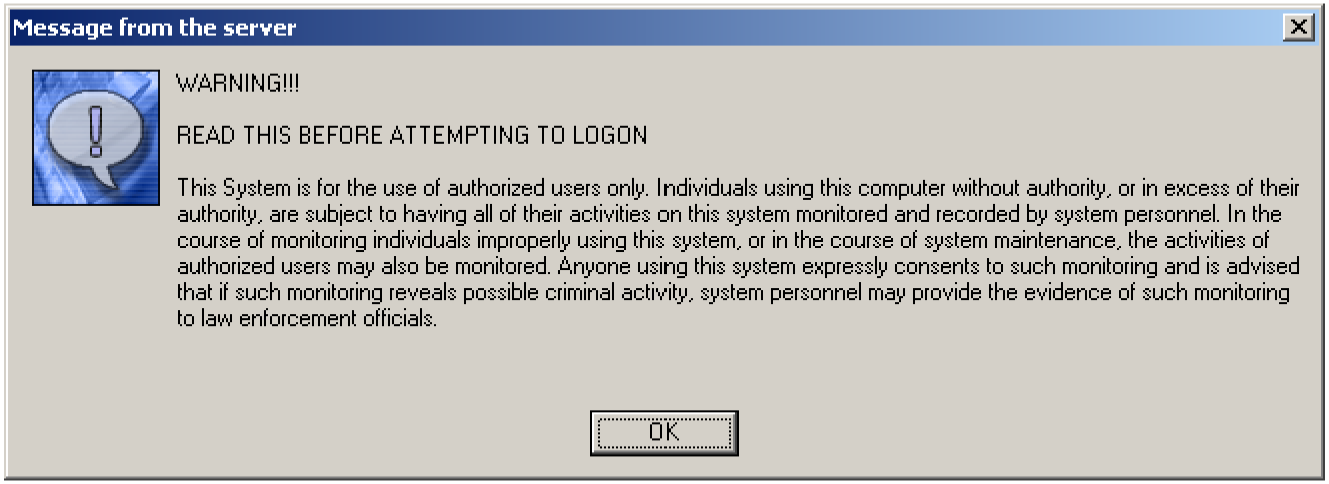
Destination Port: 3389

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

Step 20.9 – 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.



Message from the server

WARNING!!!

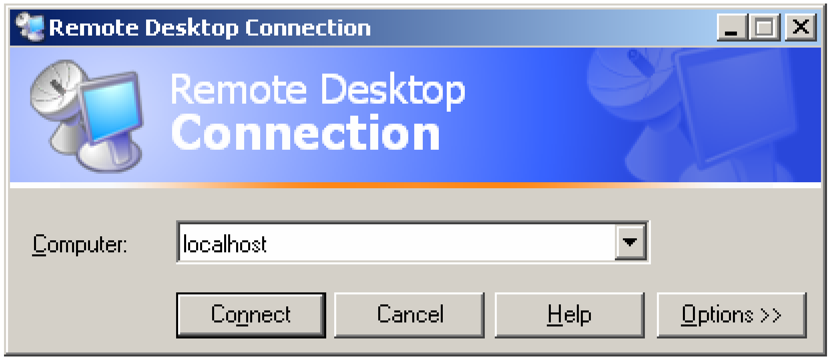
READ THIS BEFORE ATTEMPTING TO LOGON

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.

The Password prompt box will pop up.

Step 20.10 – Enter the correct password and click **OK** to continue.

Step 20.11 – After you have successfully authenticated and logged in, open your Terminal Services Client and connect to **Localhost**.



Computer: localhost

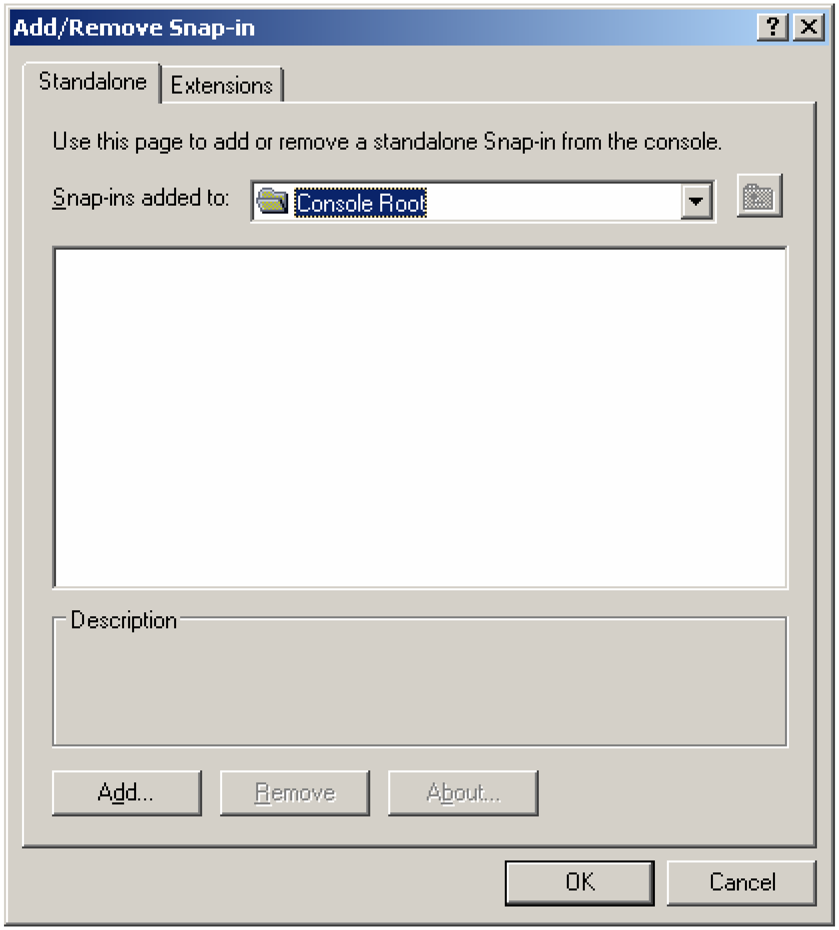
You will now be running Terminal Services over one of the most security-scrutinized protocols ever. This is the **only** InfoSec approved remote management for MS 2003 Servers in the DMZ.

Step 21.0 - Applying the High Security Web Server .inf file

Step 21.1 – Download the www-w2k3-dmz.inf file to your desktop.

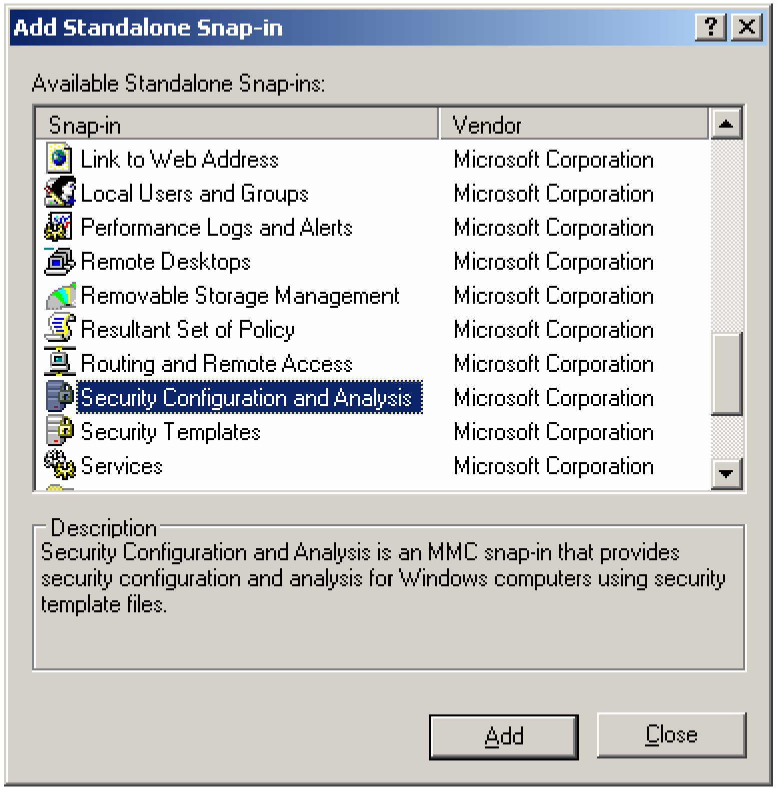
Step 21.2 – Go to **Start > Run > MMC**

Step 21.3 – Click on **File > Add/Remove Snap In**



Use this page to add or remove a standalone Snap-in from the console.

Step 21.4 – Click on the **Add** button and scroll down to **Security Configuration and Analysis**


Add Standalone Snap-in

Available Standalone Snap-ins:

Snap-in	Vendor
Link to Web Address	Microsoft Corporation
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Remote Desktops	Microsoft Corporation
Removable Storage Management	Microsoft Corporation
Resultant Set of Policy	Microsoft Corporation
Routing and Remote Access	Microsoft Corporation
Security Configuration and Analysis	Microsoft Corporation
Security Templates	Microsoft Corporation
Services	Microsoft Corporation

Description

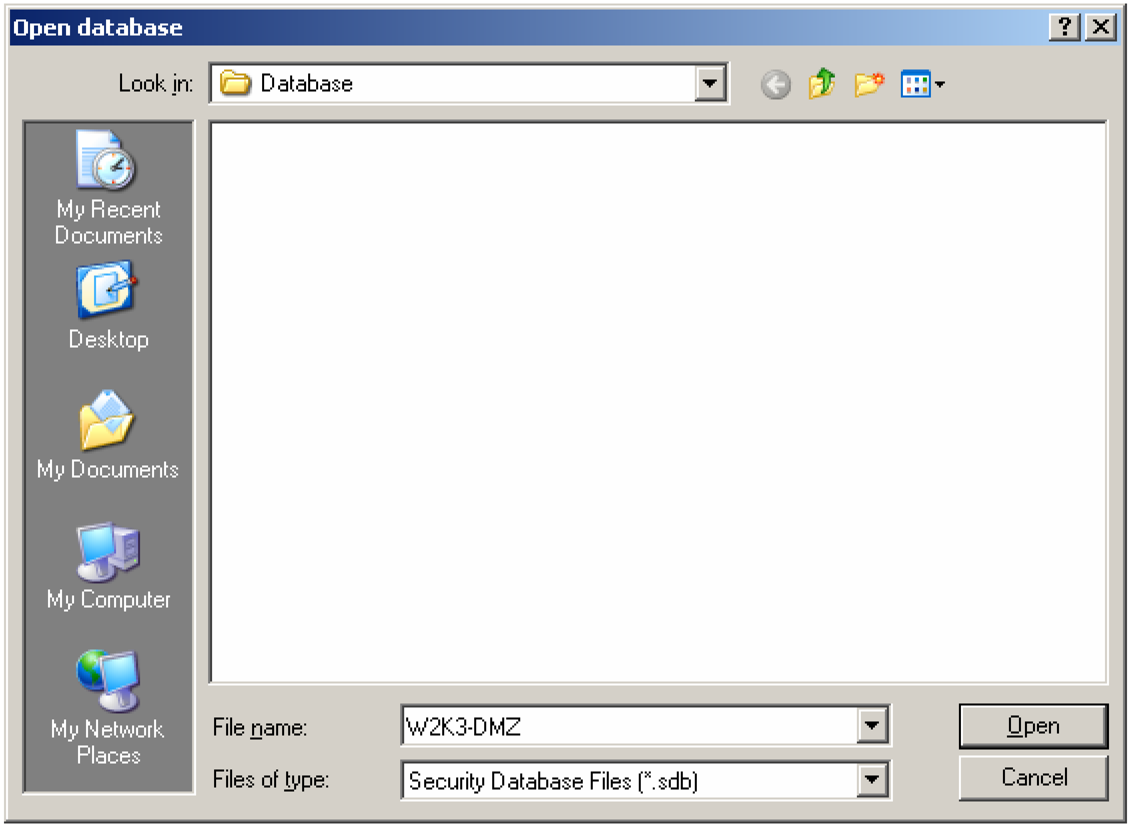
Security Configuration and Analysis is an MMC snap-in that provides security configuration and analysis for Windows computers using security template files.

Step 21.5 – Click the **Add** button then Click the **Close** button

Step 21.6 – Click the **OK** button on the **Add/Remove Snap In** window to continue.

Step 21.7 – In the Left Pane, right click on **Security Configuration and Analysis** and choose **Open Database**

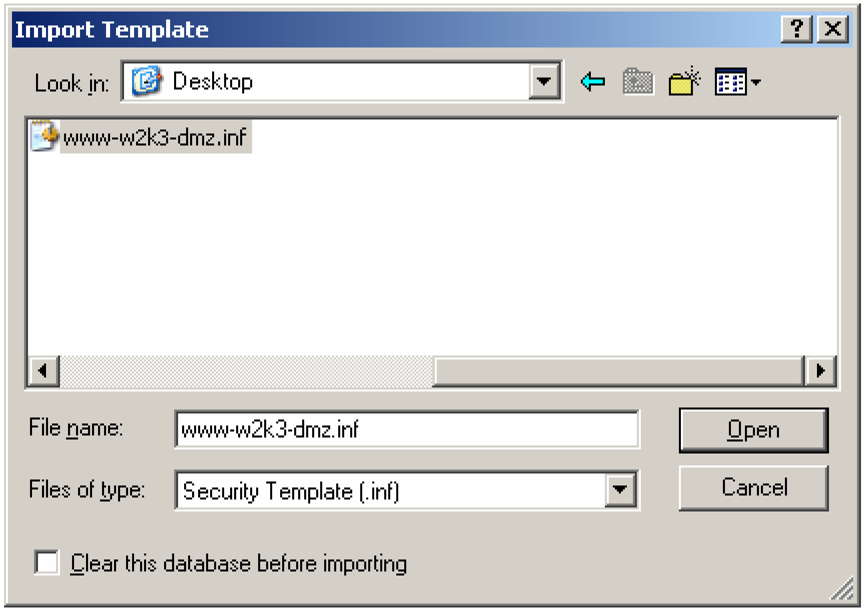
Step 21.8 – Navigate to the C:\WINDOWS\security\Database directory and give your database a name in the form **LOCALSERVER_SECPOL_LGPO** and click **Open**



File name: W2K3-DMZ

Files of type: Security Database Files (*.sdb)

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



Look in: Desktop

www-w2k3-dmz.inf

File name: www-w2k3-dmz.inf

Files of type: Security Template (.inf)

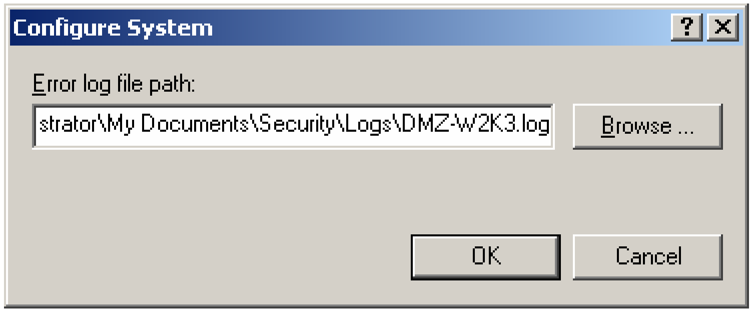
☐ Clear this database before importing

Step 21.9 – Navigate to your Desktop and type in the name of the .inf file that you previously downloaded.

Step 21.10 – Click **Open** to continue.

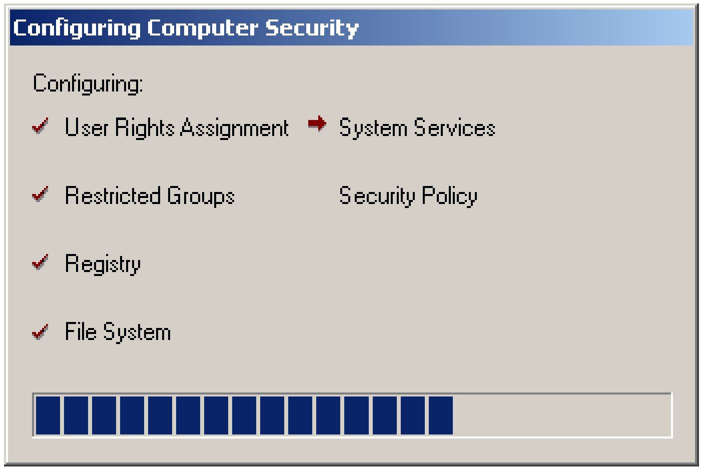
Step 21.11 – Right click on **Security Configuration and Analysis** and choose **Configure computer now**.

Step 21.12 – This will pop up a box asking where you wish to write the log file. You can choose the default and click ok.



Error log file path: strator\My Documents\Security\Logs\DMZ-W2K3.log

The computer will now apply the INF file



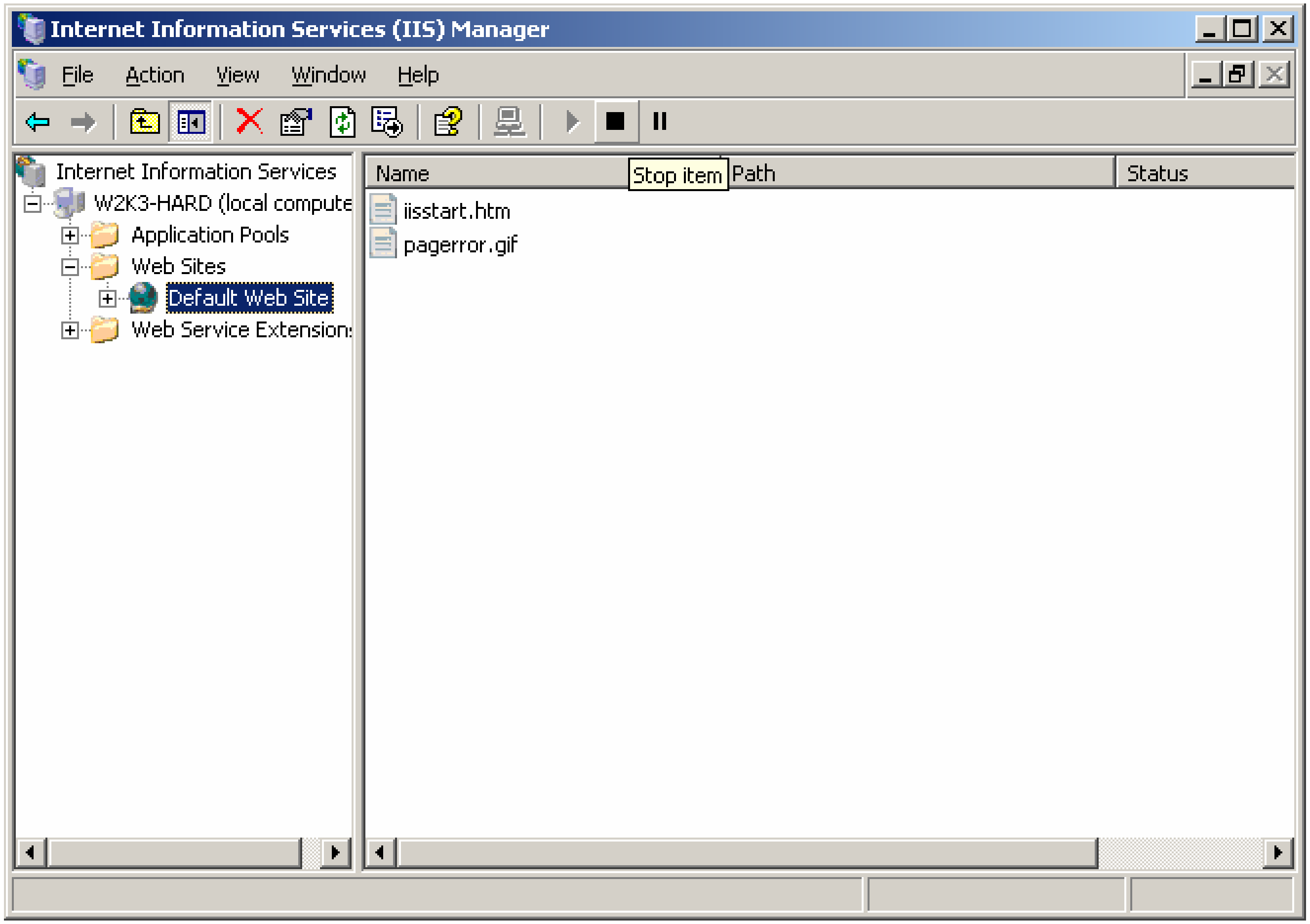
Step 21.13 – When the configuration is done, you can close the Console1 window.

The .inf file will make the following changes. (add changes link here)

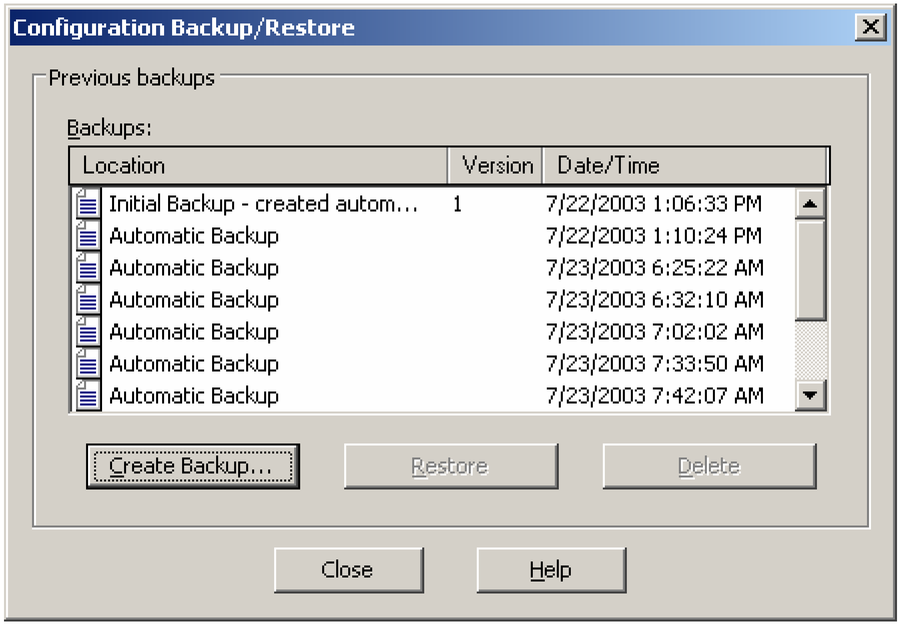
Step 22.0 – IIS 6.0 Configuration

Step 22.1 – Go to **Start > Programs > Administrative Tools > Internet Information Service (IIS) Manager**.

Step 22.2 – Choose the **Default Web Site** and **Stop** it by clicking on the black square on the taskbar.

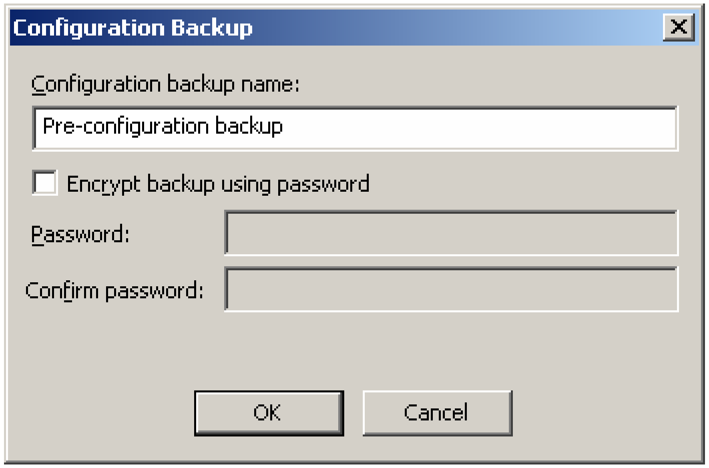


Step 22.3 – Right click on the PC Icon above and choose **All Tasks > Backup/Restore Configuration**.



Location	Version	Date/Time
Initial Backup - created autom...	1	7/22/2003 1:06:33 PM
Automatic Backup		7/22/2003 1:10:24 PM
Automatic Backup		7/23/2003 6:25:22 AM
Automatic Backup		7/23/2003 6:32:10 AM
Automatic Backup		7/23/2003 7:02:02 AM
Automatic Backup		7/23/2003 7:33:50 AM
Automatic Backup		7/23/2003 7:42:07 AM

Step 22.4 – Select **Create Backup**, name your backup file and click **OK** to complete the task.



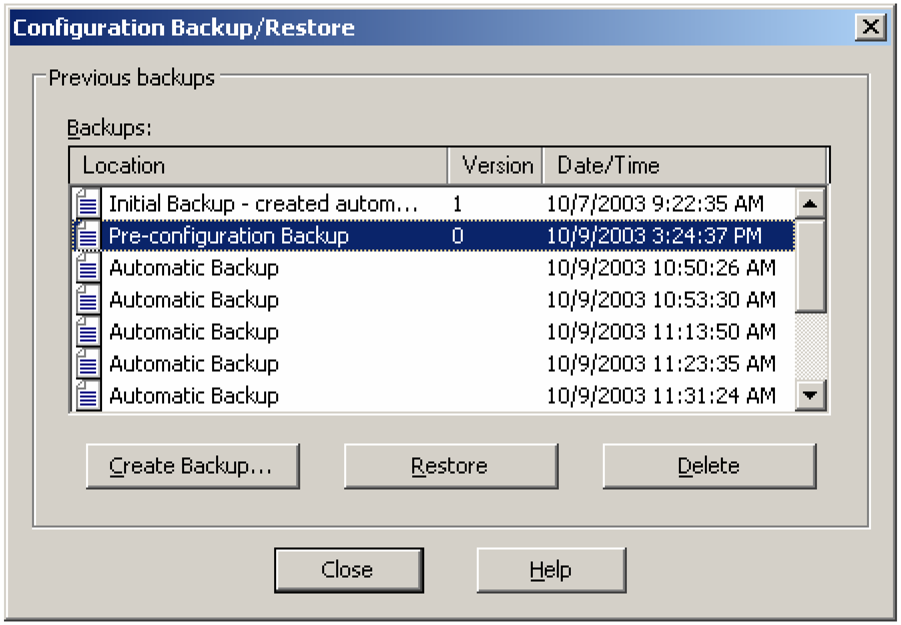
Configuration backup name: Pre-configuration backup

☐ Encrypt backup using password

Password:

Confirm password:

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

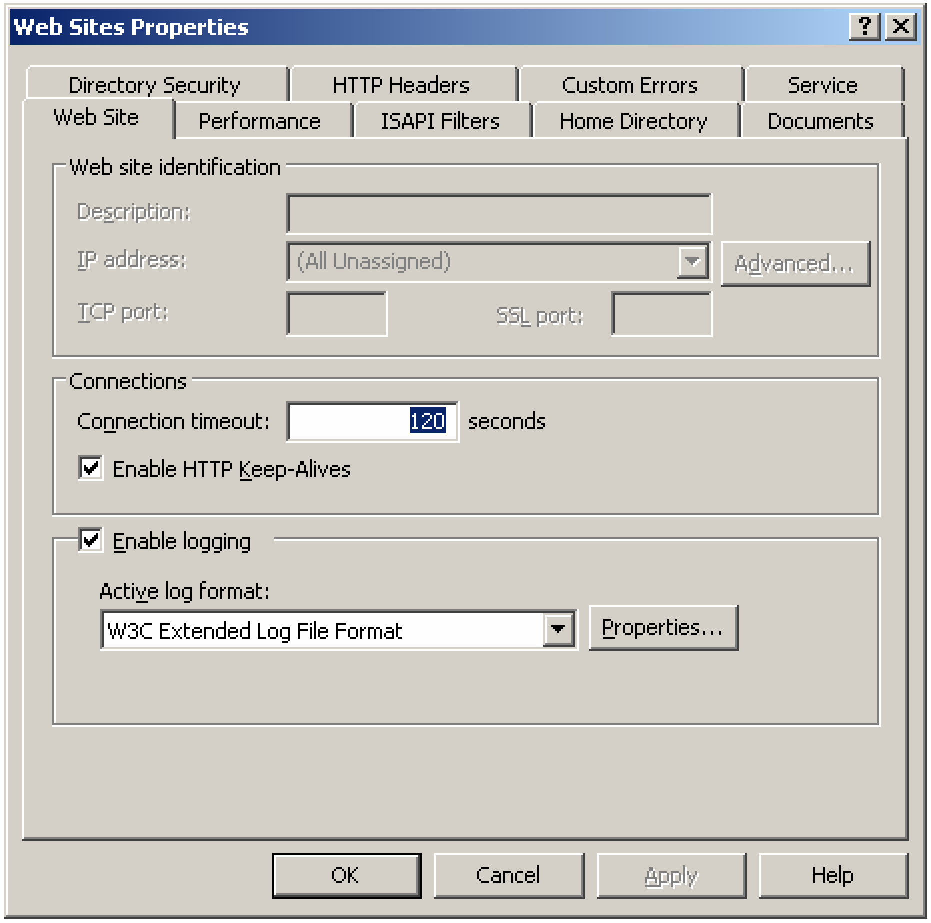


Location	Version	Date/Time
Initial Backup - created autom...	1	10/7/2003 9:22:35 AM
Pre-configuration Backup	0	10/9/2003 3:24:37 PM
Automatic Backup		10/9/2003 10:50:26 AM
Automatic Backup		10/9/2003 10:53:30 AM
Automatic Backup		10/9/2003 11:13:50 AM
Automatic Backup		10/9/2003 11:23:35 AM
Automatic Backup		10/9/2003 11:31:24 AM

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

Step 22.5 – Editing the Master Properties for Web Sites

Right click on the Folder labeled **Web Sites** and choose **Properties**.



IP address: (All Unassigned)

TCP port:

Connection timeout: 120 seconds

☑ Enable HTTP Keep-Alives

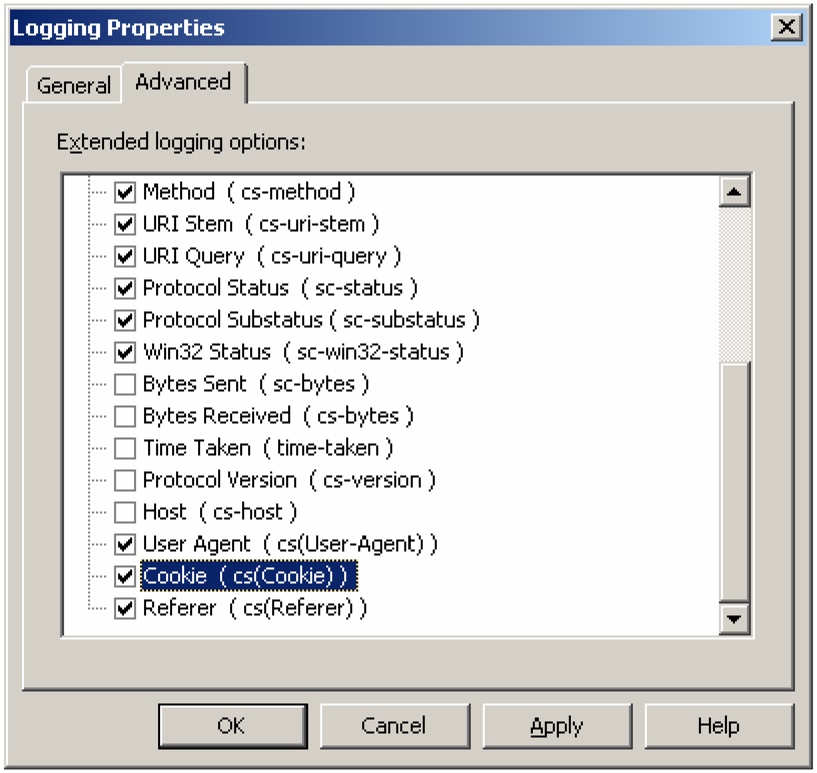
☑ Enable logging

Active log format: W3C Extended Log File Format

Step 22.6 – Choose **Web Site > Enable Logging > Properties**:

Step 22.7 – Under **New Log Schedule**, select the radio button labeled **When file size reaches:** and change the value to **50**.

Step 22.8 – Click on the **Advanced Tab**, scroll to the bottom of the list and add checks for **Cookie** and **Referer**.



Extended logging options:

- ☑ Method (cs-method)
- ☑ URI Stem (cs-uri-stem)
- ☑ URI Query (cs-uri-query)
- ☑ Protocol Status (sc-status)
- ☑ Protocol Substatus (sc-substatus)
- ☑ Win32 Status (sc-win32-status)
- ☐ Bytes Sent (sc-bytes)
- ☐ Bytes Received (cs-bytes)
- ☐ Time Taken (time-taken)
- ☐ Protocol Version (cs-version)
- ☐ Host (cs-host)
- ☑ User Agent (cs(User-Agent))
- ☑ Cookie (cs(Cookie))
- ☑ Referer (cs(Referer))

Click **OK**

Under the **Home Directory** Tab

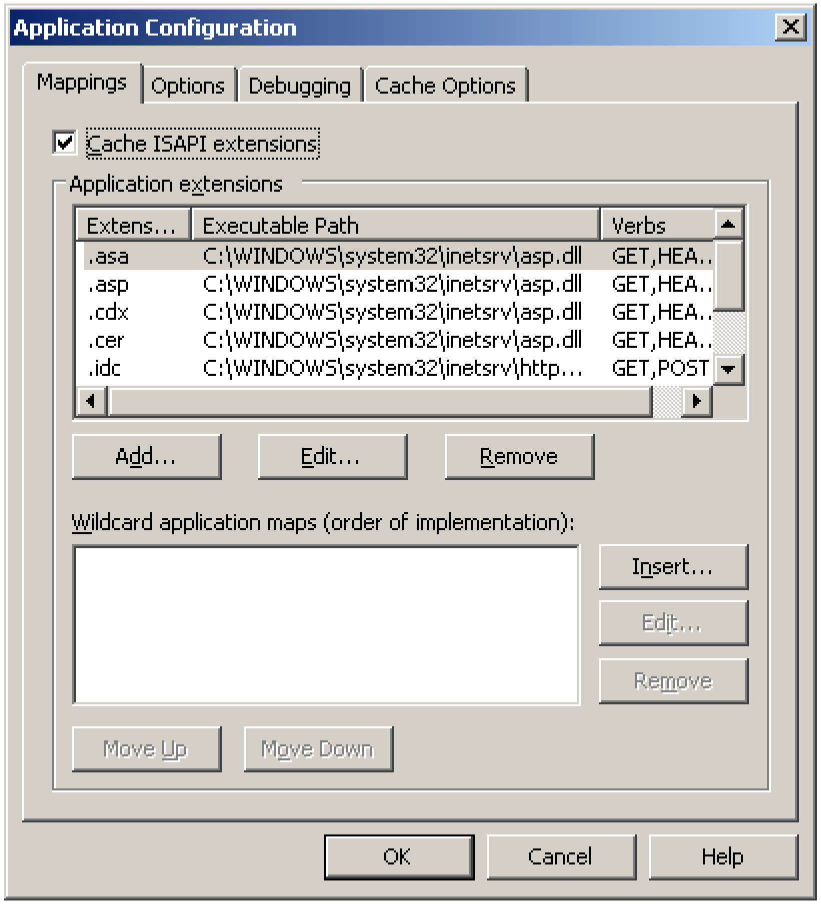
Step 22.9 – Under the **Application Settings** subsection, choose **Configuration**.

Step 22.10 - Remove all Application Extensions, as referenced below:

NOTE: Remove them all and add back in as needed!

Extension	Filetype
.asa	ASP Files to declare objects with session or application scope
.asp	Active Server Pages
.cdx	Scripts to create Channel Definition files
.cer	Scripts for digital certificates
.idc	Internet Database Connection
.shtm	Server Side Includes

.shtml	Server Side Includes
.stm	Server Side Includes



☑ Cache ISAPI extensions

Application extensions

Extens...	Executable Path	Verbs
.asa	C:\WINDOWS\system32\inetsrv\asp.dll	GET,HEA...
.asp	C:\WINDOWS\system32\inetsrv\asp.dll	GET,HEA...
.cdx	C:\WINDOWS\system32\inetsrv\asp.dll	GET,HEA...
.cer	C:\WINDOWS\system32\inetsrv\asp.dll	GET,HEA...
.idc	C:\WINDOWS\system32\inetsrv\http...	GET,POST

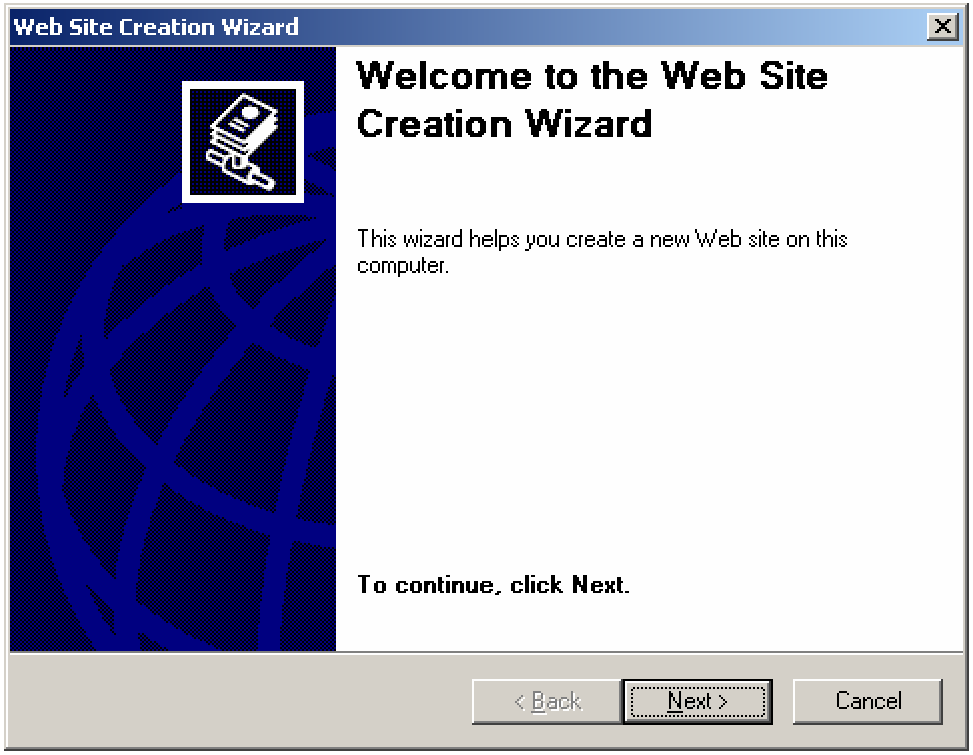
Wildcard application maps (order of implementation):

Step 22.11 – For any extensions that are re-added, consider limiting the HTTP verbs the extension will accept. Instead of using all the verbs (DELETE, GET, HEAD, POST and TRACE), use only GET for Static Web Pages and POST if you have forms on your site. This is in accordance with the least privilege principal.

Step 22.12 – Click **OK** to get out of edit mode.

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

Step 22.13 – Highlight the **Web Sites** Folder**,** right mouse click and select **New** > **Web Site.**



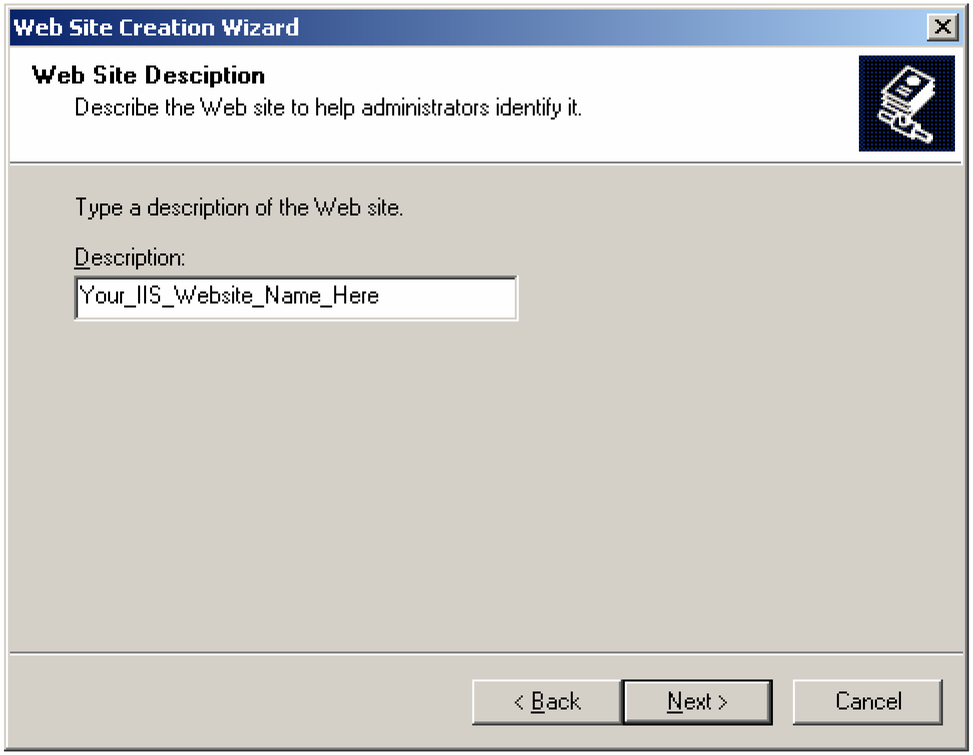
Welcome to the Web Site Creation Wizard

This wizard helps you create a new Web site on this computer.

To continue, click Next.

Click **Next** to continue

Step 22.14 - Give your Web Site a Description



Web Site Desciption

Describe the Web site to help administrators identify it.

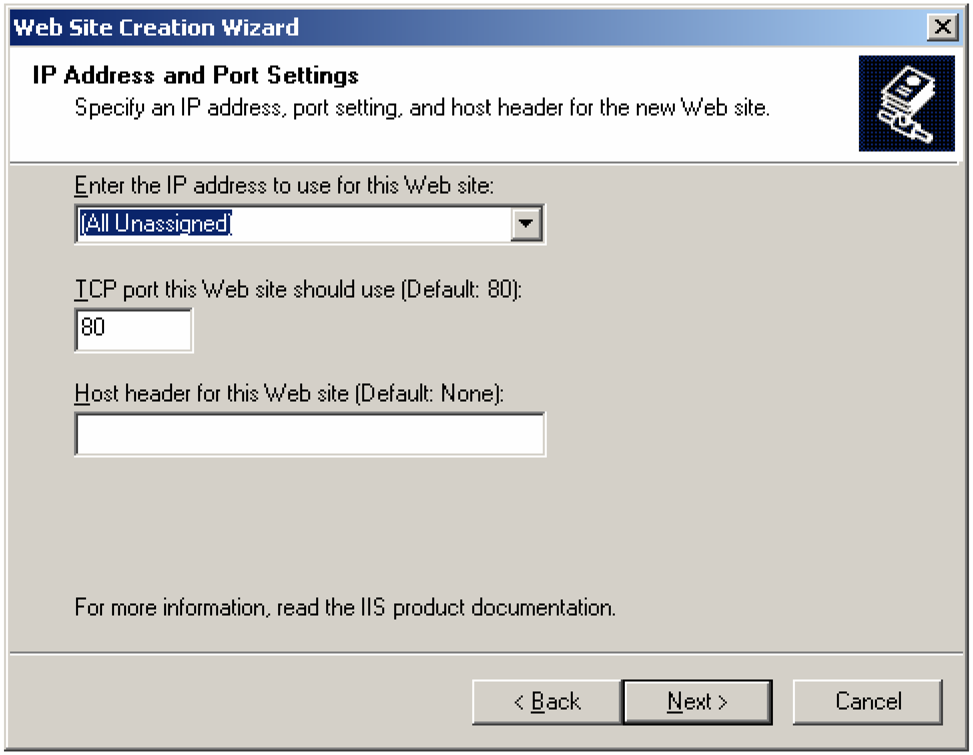
Type a description of the Web site.

Description:

Your_IIS_Website_Name_Here

Click **Next** to continue

Step 22.15 – Add the **IP address** and **Port Number** (the defaults are usually appropriate).



IP Address and Port Settings

Specify an IP address, port setting, and host header for the new Web site.

Enter the IP address to use for this Web site: (All Unassigned)

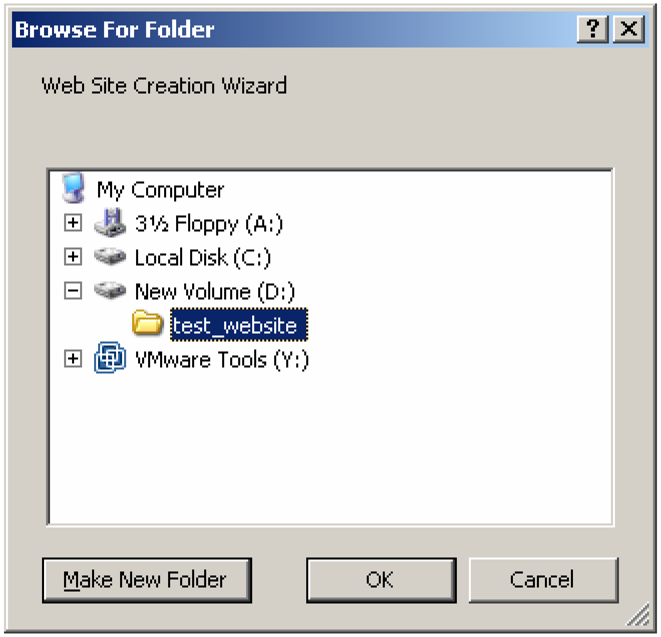
TCP port this Web site should use (Default: 80): 80

Host header for this Web site (Default: None):

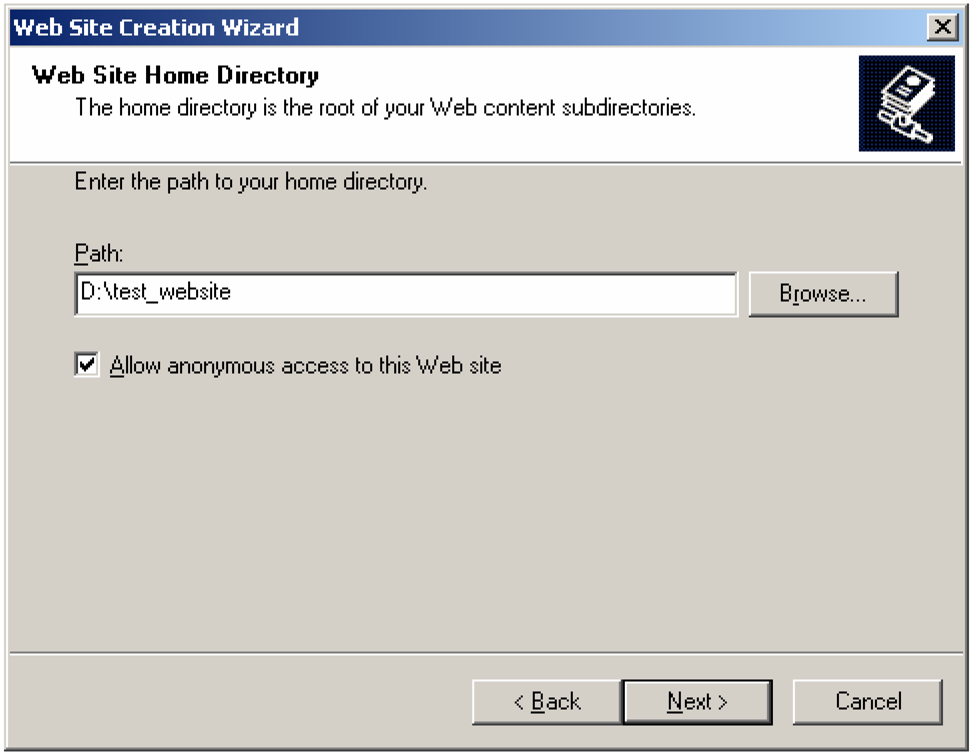
For more information, read the IIS product documentation.

Click **Next** to continue

Step 22.16 – 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**.



Step 22.17 – Click **OK** to select the newly created directory.



Web Site Creation Wizard

Web Site Home Directory

The home directory is the root of your Web content subdirectories.

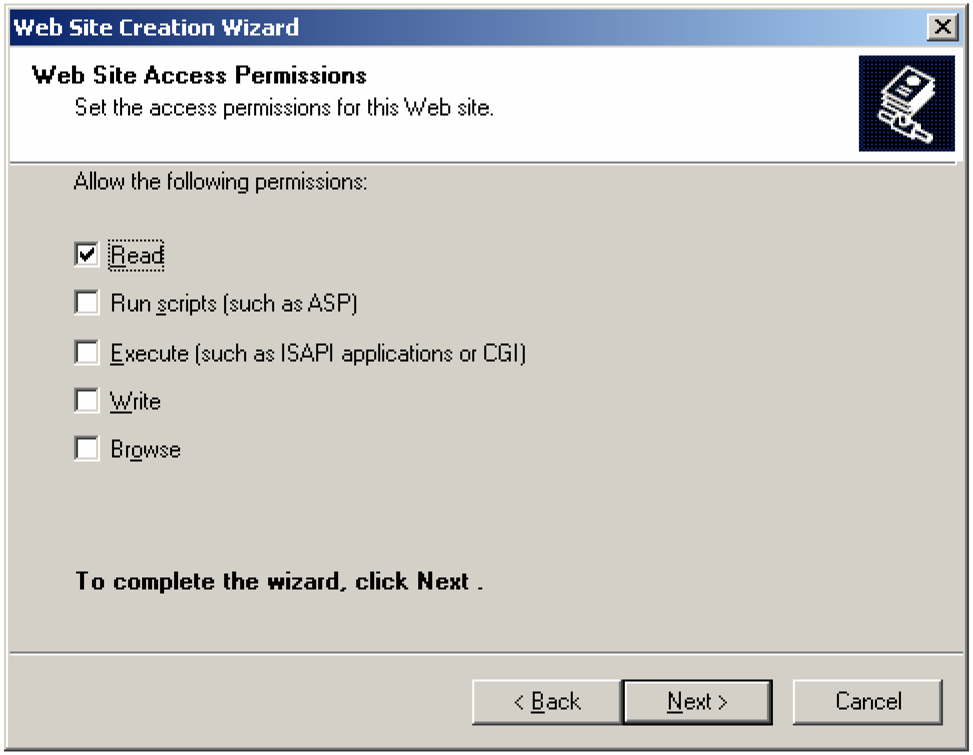
Enter the path to your home directory.

Path: D:\test_website

☑ Allow anonymous access to this Web site

Click **Next** to continue

Step 22.18 – Choose the minimum set of permissions here for your web site by un-checking the **Run scripts (such as ASP)** box.



Web Site Access Permissions

Set the access permissions for this Web site.

Allow the following permissions:

☑ Read

☐ Run scripts (such as ASP)

☐ Execute (such as ISAPI applications or CGI)

☐ Write

☐ Browse

To complete the wizard, click Next .

Click **Next** to continue

Step 22.19 – Click **Finish** to complete the Web Site Creation Wizard

Step 22.20 – (**Optional**) Microsoft recommends configuring a separate directory for each file type so that you can easily set ACLs. Best Practice:

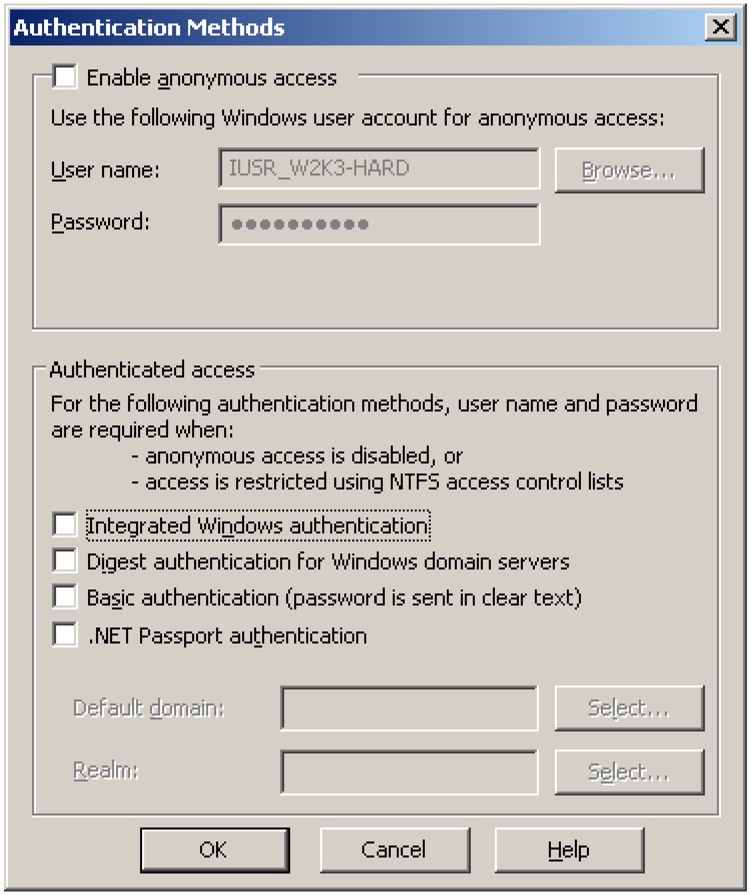
This is a good idea if you have the ability to do so. For example, if your website base directory was E:\test_website then you would setup your web site such as:

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)

Step 22.21 – 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.

Step 22.22 – Right click on the **Default Web Site**. Select **Properties** > **Directory Security** > **Authentication and Access Control** > **Edit**

Step 22.23 – **Uncheck** all the boxes.



☐ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_W2K3-HARD

Password: ●●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

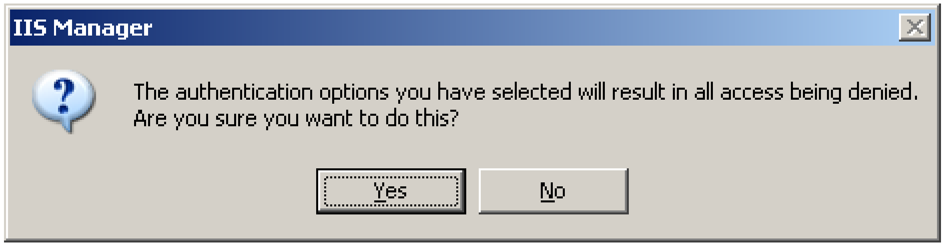
☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

You will get a warning screen as shown:



The authentication options you have selected will result in all access being denied. Are you sure you want to do this?

Step 22.24 – Select **Yes**

Step 22.25 – Click **OK** to complete the task.

Step 22.26 – Check for and remove all IIS Sample directories

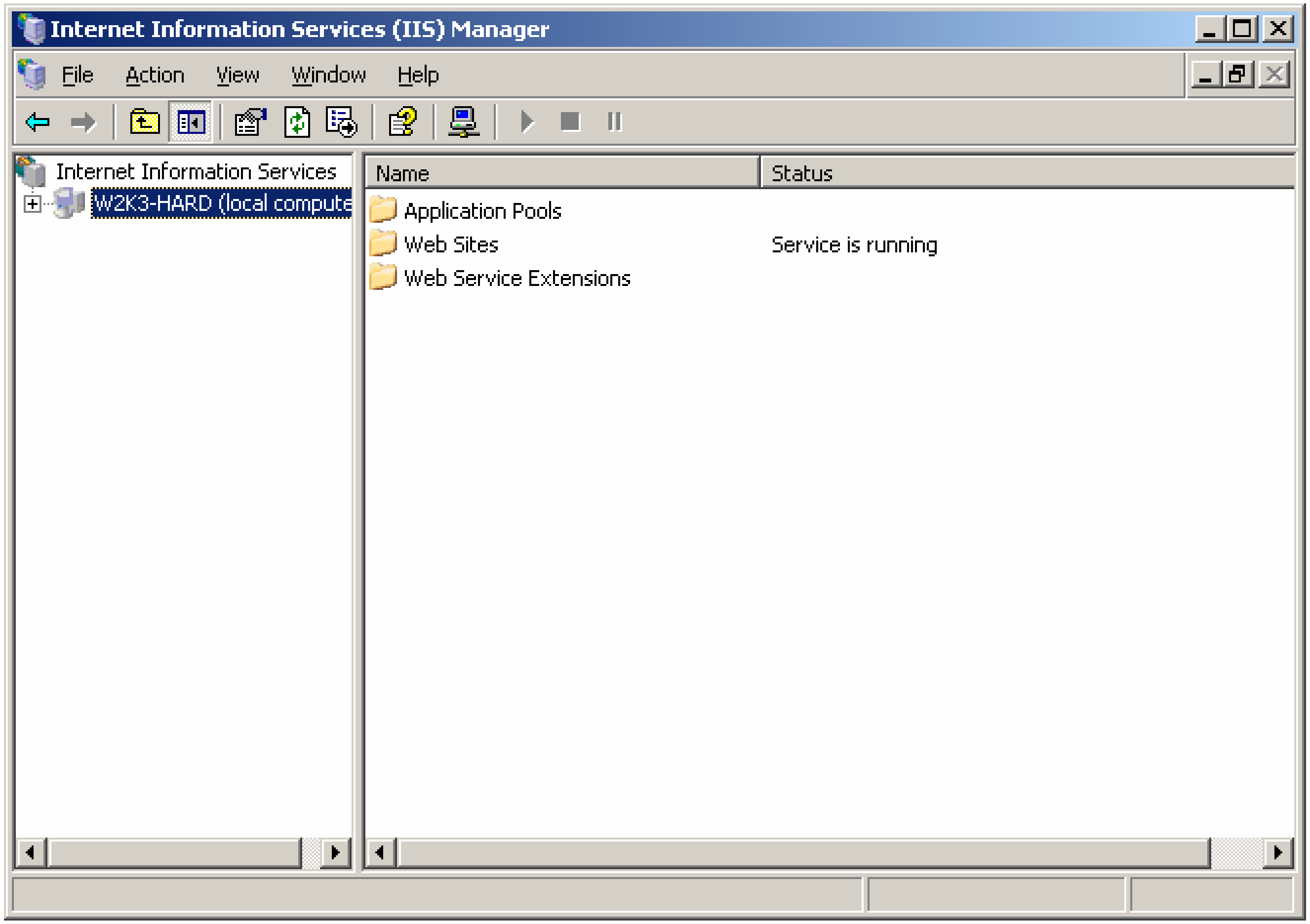
Admin Scripts	C:\InetPub\AdminScripts
IIS Help	C:\Windows\help\iisHelp
IIS admpwd	C:\Windows\System32\inetsrv\iisadmpwd

Remove Internet Printing

Step 22.27 – Delete the printer's virtual directory at C:\Windows\web\printers

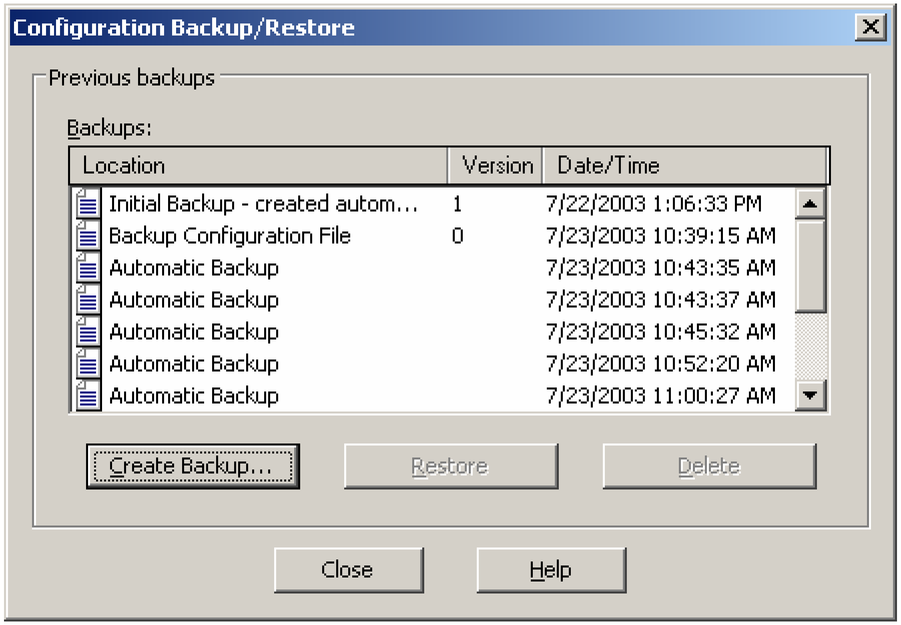
Back up the Metabase again

Step 22.28 – Go to **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**


Internet Information Services (IIS) Manager
File
Action
View
Window
Help
Internet Information Services
W2K3-HARD (local compute
Name
Status

Name	Status
Application Pools	
Web Sites	Service is running
Web Service Extensions	

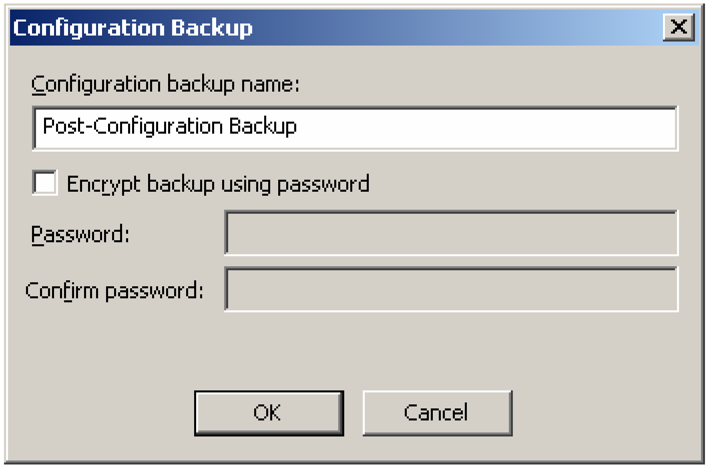
Step 22.29 – Right click on the computer name, select **All Tasks > Backup/Restore Configuration**



Backups:

Location	Version	Date/Time
Initial Backup - created autom...	1	7/22/2003 1:06:33 PM
Backup Configuration File	0	7/23/2003 10:39:15 AM
Automatic Backup		7/23/2003 10:43:35 AM
Automatic Backup		7/23/2003 10:43:37 AM
Automatic Backup		7/23/2003 10:45:32 AM
Automatic Backup		7/23/2003 10:52:20 AM
Automatic Backup		7/23/2003 11:00:27 AM

Step 22.30 – Select **Create Backup**



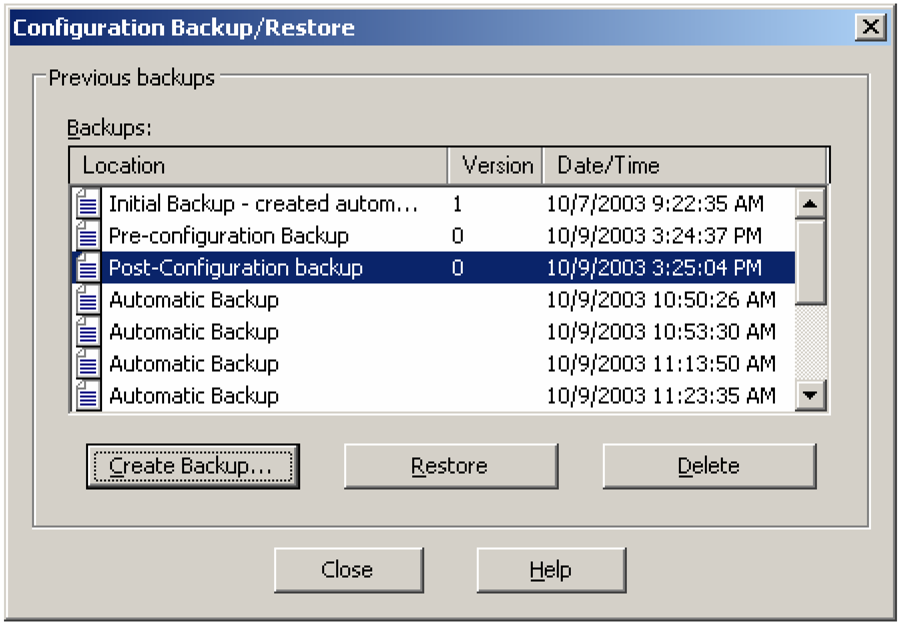
Configuration backup name: Post-Configuration Backup

☐ Encrypt backup using password

Password:

Confirm password:

Step 22.31 – Name your backup file and click **OK** to continue.



Configuration Backup/Restore

Previous backups

Backups:

Location	Version	Date/Time
Initial Backup - created autom...	1	10/7/2003 9:22:35 AM
Pre-configuration Backup	0	10/9/2003 3:24:37 PM
Post-Configuration backup	0	10/9/2003 3:25:04 PM
Automatic Backup		10/9/2003 10:50:26 AM
Automatic Backup		10/9/2003 10:53:30 AM
Automatic Backup		10/9/2003 11:13:50 AM
Automatic Backup		10/9/2003 11:23:35 AM

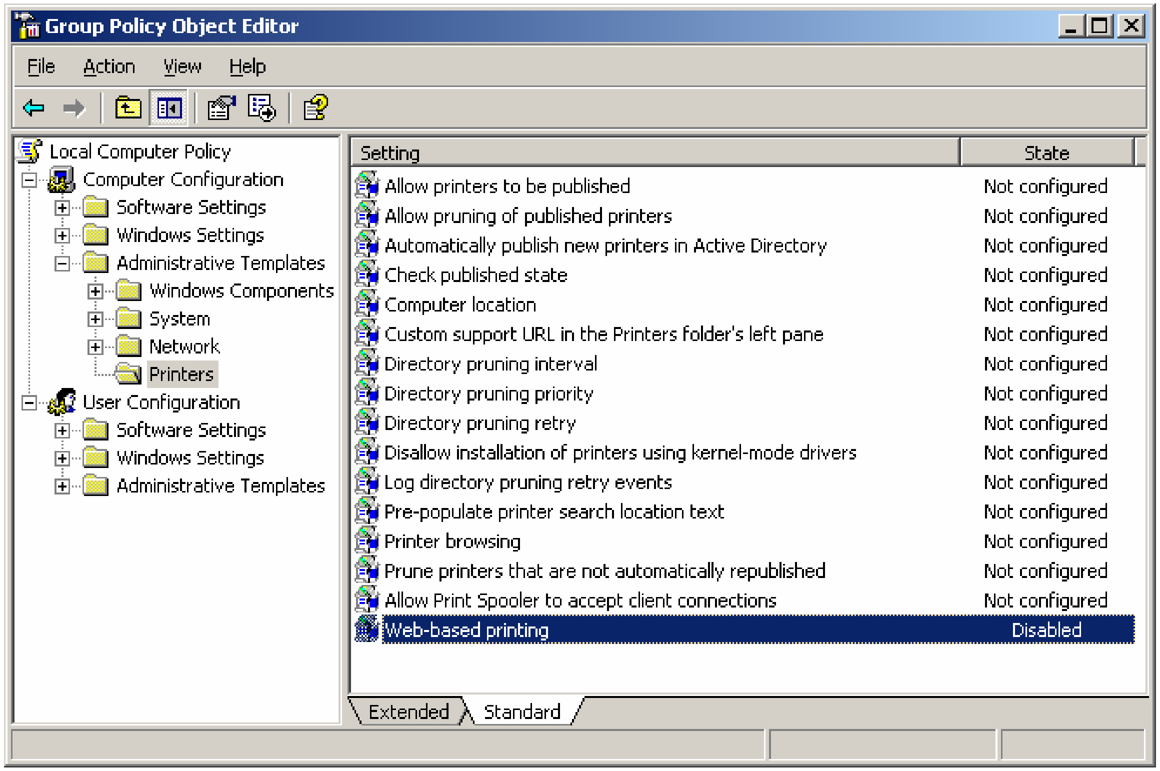
You should see your original backup file and your backup after the configuration steps above.

Step 22.32 – Click **Close** to complete the task.

Step 22.33 – Start > **Run** > **gpedit.msc**

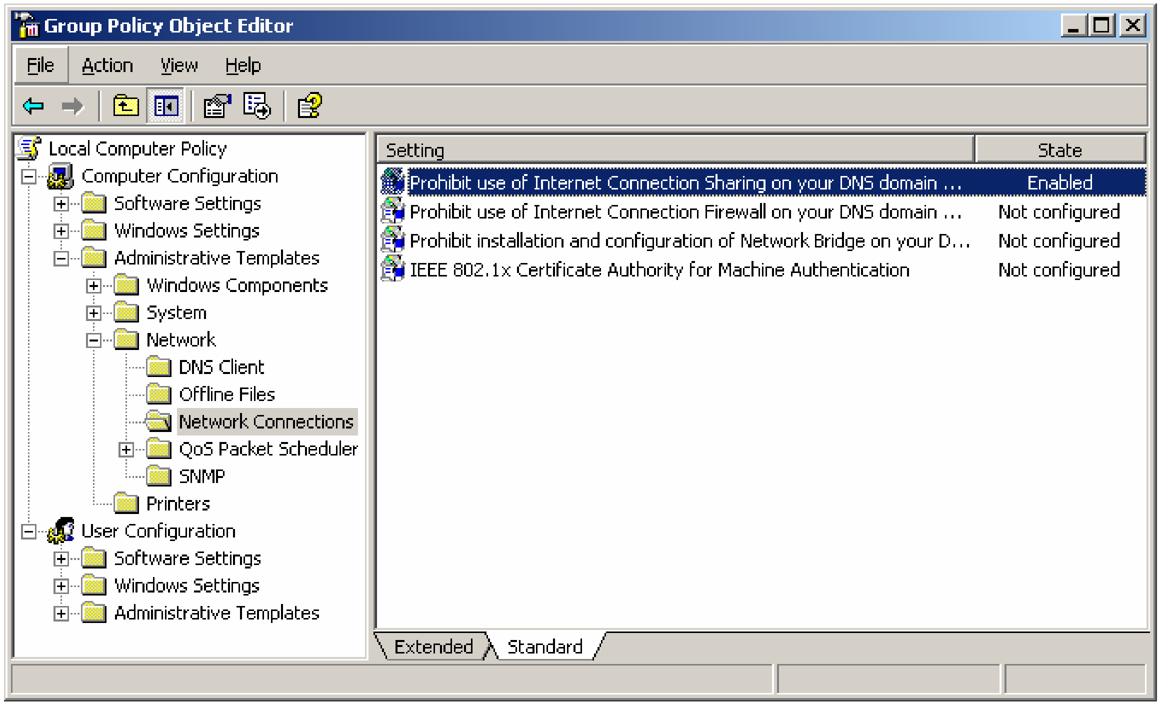
Under **Computer Configuration > Administrative Templates > Printers**

Step 22.34 – Change **Web Based Printing** to disabled.



Setting	State
Allow printers to be published	Not configured
Allow pruning of published printers	Not configured
Automatically publish new printers in Active Directory	Not configured
Check published state	Not configured
Computer location	Not configured
Custom support URL in the Printers folder's left pane	Not configured
Directory pruning interval	Not configured
Directory pruning priority	Not configured
Directory pruning retry	Not configured
Disallow installation of printers using kernel-mode drivers	Not configured
Log directory pruning retry events	Not configured
Pre-populate printer search location text	Not configured
Printer browsing	Not configured
Prune printers that are not automatically republished	Not configured
Allow Print Spooler to accept client connections	Not configured
Web-based printing	Disabled

Step 22.35 – Under the **Network > Network Configurations** folder, change the value for **Prohibit use of Internet Connection Sharing on your DNS Domain Network** to enabled by right clicking and choosing **Enable**.



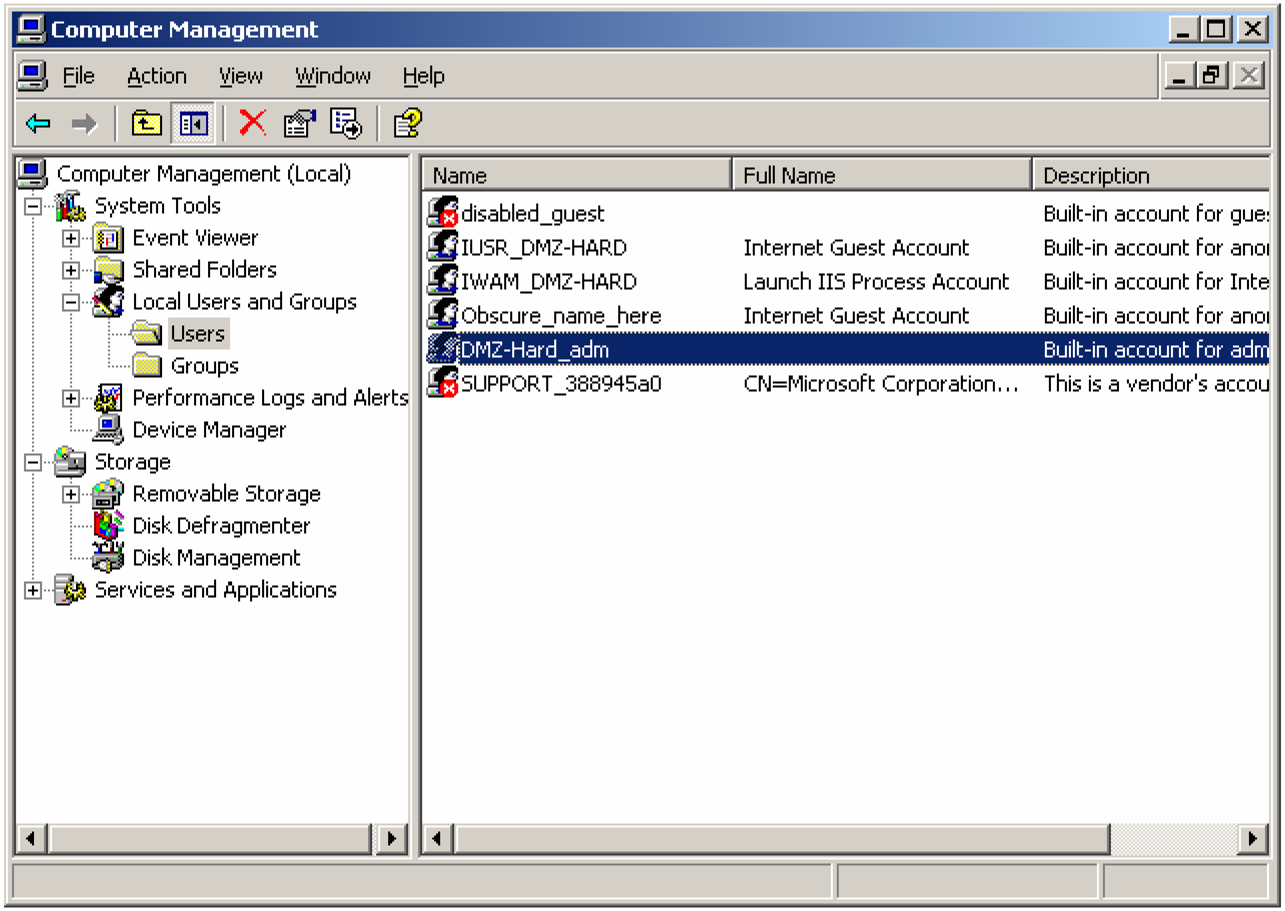
Setting	State
Prohibit use of Internet Connection Sharing on your DNS domain ...	Enabled
Prohibit use of Internet Connection Firewall on your DNS domain ...	Not configured
Prohibit installation and configuration of Network Bridge on your D...	Not configured
IEEE 802.1x Certificate Authority for Machine Authentication	Not configured

Step 23.0 – Rename and change the password to the IUSR_<*machinename*> account.

Step 23.1 – Right click on **My Computer > Manage**

Step 23.2 – 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-Hard, so the newly renamed Administrator account would be **DMZ-Hard_adm**

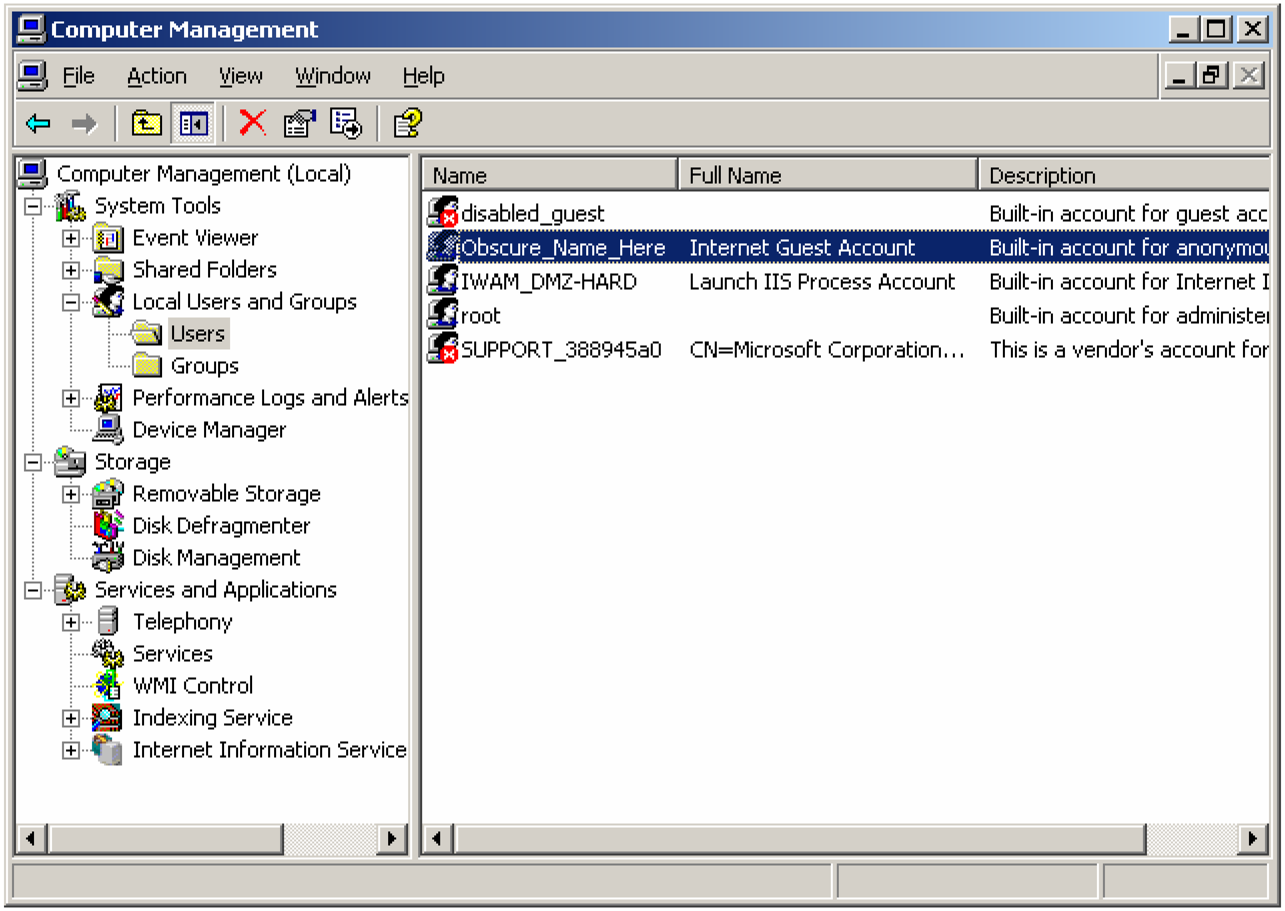


Name	Full Name	Description
disabled_guest		Built-in account for gue:
IUSR_DMZ-HARD	Internet Guest Account	Built-in account for anoı
IWAM_DMZ-HARD	Launch IIS Process Account	Built-in account for Inte
Obscure_name_here	Internet Guest Account	Built-in account for anoı
DMZ-Hard_adm		Built-in account for adm
SUPPORT_388945a0	CN=Microsoft Corporation,...	This is a vendor's accou

Step 23.3 – Choose the **IUSR_<*machinename*>** account.

Step 23.3 – Right click and **rename this account to an obscure name**. (Remember this new name, you will need it later in step 24.4). 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 account, and disable it. It is safe to ignore it after performing this step.

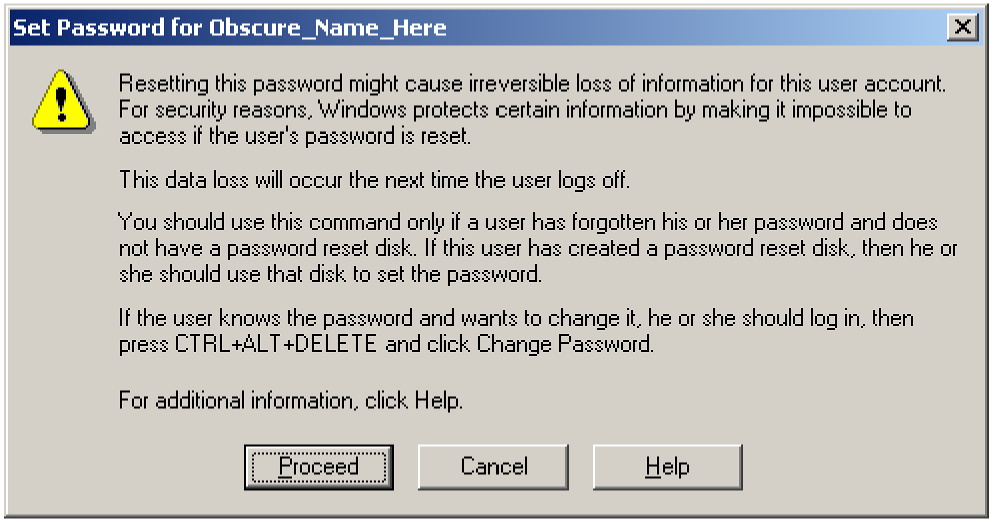
Step 23.4 – Refer back to **Step 20.5** and **change the Username** to match the name in Step 23.2.



Name	Full Name	Description
disabled_guest		Built-in account for guest acc
Obscure_Name_Here	Internet Guest Account	Built-in account for anonymou
IWAM_DMZ-HARD	Launch IIS Process Account	Built-in account for Internet I
root		Built-in account for administe
SUPPORT_388945a0	CN=Microsoft Corporation…	This is a vendor's account for

Step 23.5 – Right click on this newly renamed account and choose **Set Password**.

You will get a Warning Box like the one below.



Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user's password is reset.

This data loss will occur the next time the user logs off.

You should use this command only if a user has forgotten his or her password and does not have a password reset disk. If this user has created a password reset disk, then he or she should use that disk to set the password.

If the user knows the password and wants to change it, he or she should log in, then press CTRL+ALT+DELETE and click Change Password.

For additional information, click Help.

Step 23.6 – Click **Proceed** and select and set a strong password for this account. (Remember this password, you will need it later).

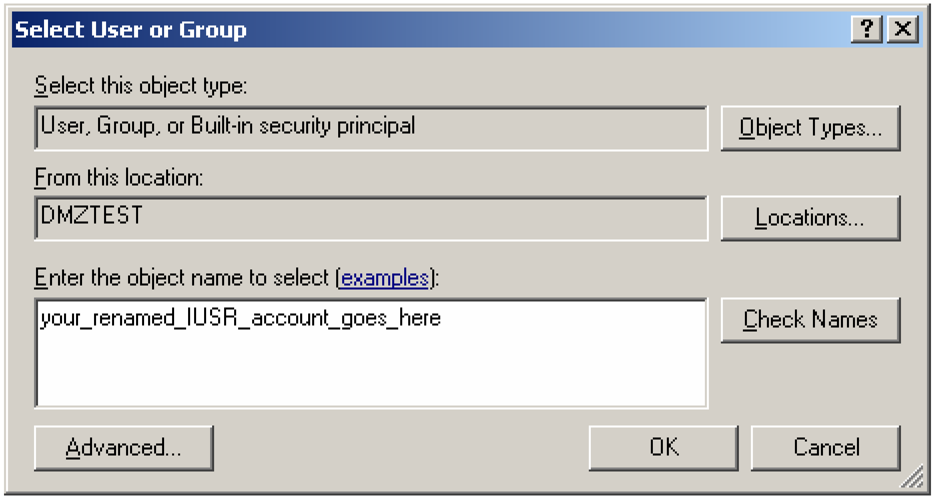
Step 23.7 – You can now close the Computer Management window.

Step 24.0 - NTFS Permissions

Step 24.1 – Double click on **My Computer**

Step 24.2 – Right click on the C:\ drive and choose **Properties** > **Security**

Step 24.3 – Click the **Add** Button



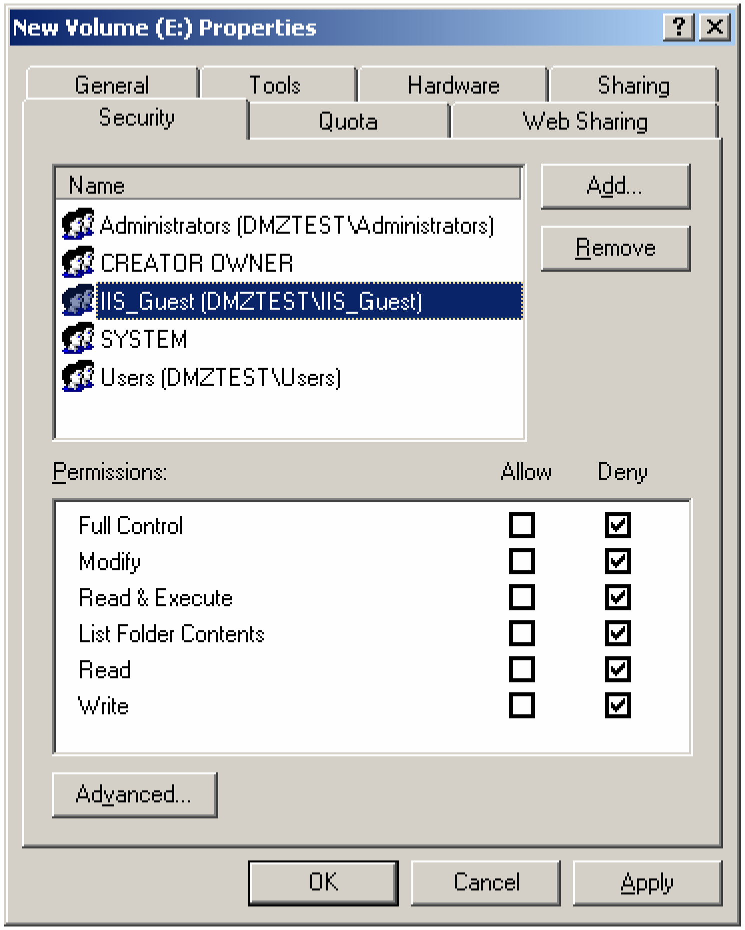
Select User or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
DMZTEST

Enter the object name to select (examples):
your_renamed_IUSR_account_goes_here

Step 24.4 – In the white space, type in your renamed IUSR account from **Step 23.3** and click **OK**



Name
Administrators (DMZTEST\Administrators)
CREATOR OWNER
IIS_Guest (DMZTEST\IIS_Guest)
SYSTEM
Users (DMZTEST\Users)

Permissions:	Allow	Deny
Full Control	☐	☑
Modify	☐	☑
Read & Execute	☐	☑
List Folder Contents	☐	☑
Read	☐	☑
Write	☐	☑

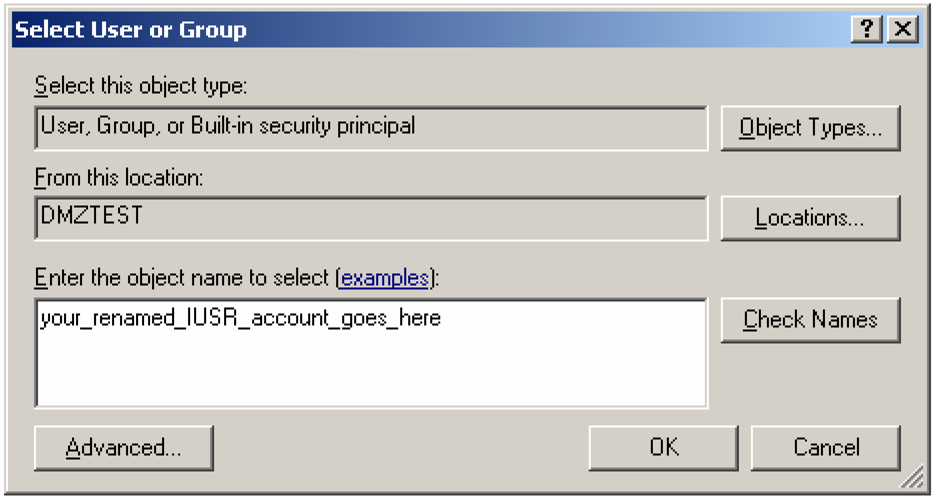
Step 24.5 - Highlight this newly added user and choose **Deny Full Control** and click **OK**.

Step 24.6 – Repeat these steps for all other volumes.

Step 24.7 – To Apply the proper NTFS permissions to the individual directories, **Right click** on the **C:\Windows** Directory and select **Properties**

Step 24.8 – Click the **Advanced** button

Step 24.9 – Click the **Add** button and in the white space, type in the name of your renamed IUSR account from **Step 23.3**.



Select this object type:
User, Group, or Built-in security principal

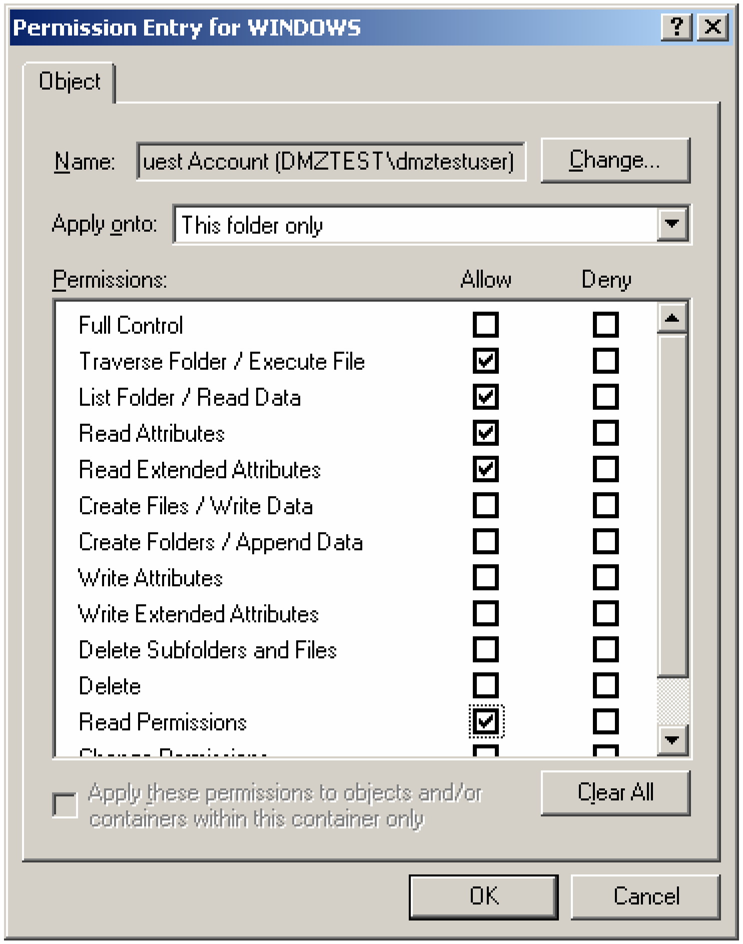
From this location:
DMZTEST

Enter the object name to select (examples):
your_renamed_IUSR_account_goes_here

Step 24.10 – Under **Apply onto:** select **This folder only**

Step 24.11 – Give permissions to:

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



Permission Entry for WINDOWS

Object

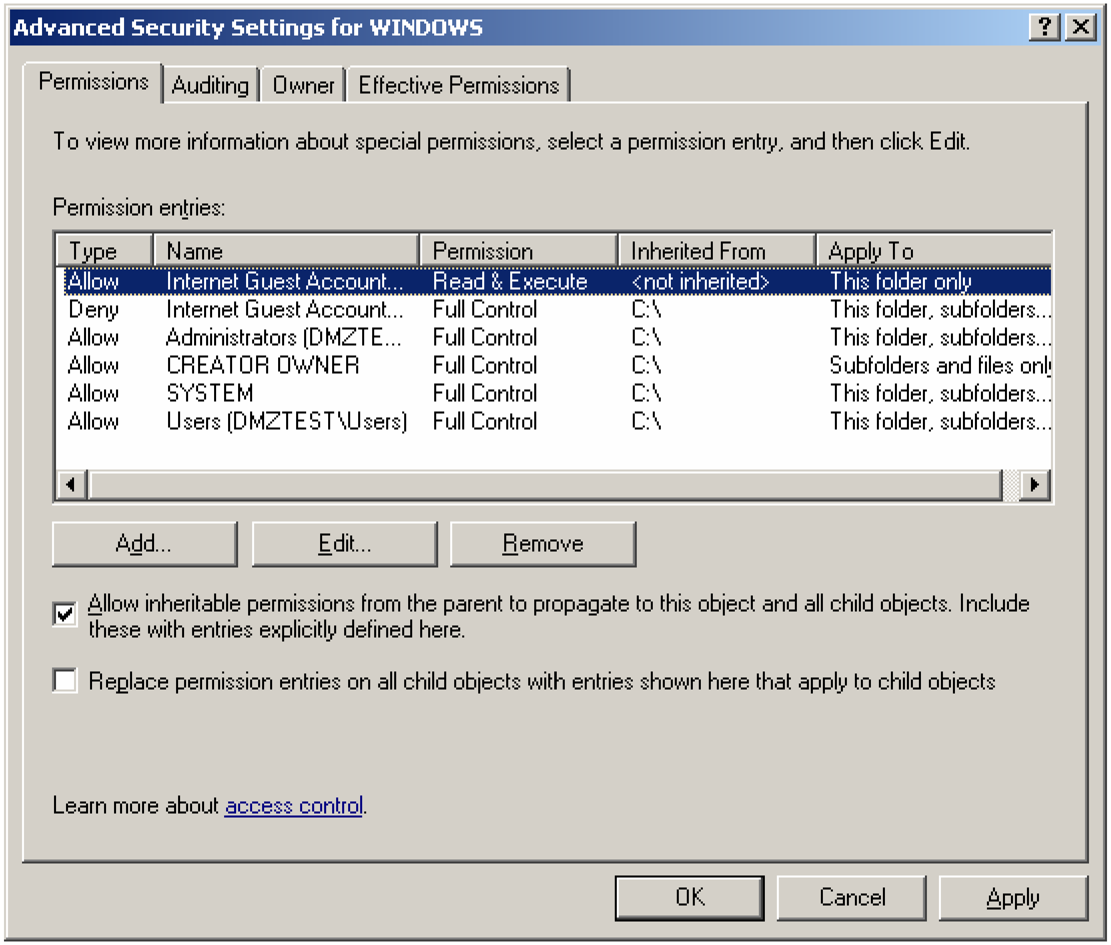
Name: uest Account (DMZTEST\dmztestuser)

Apply onto: This folder only

Permissions:	Allow	Deny
Full Control	☐	☐
Traverse Folder / Execute File	☑	☐
List Folder / Read Data	☑	☐
Read Attributes	☑	☐
Read Extended Attributes	☑	☐
Create Files / Write Data	☐	☐
Create Folders / Append Data	☐	☐
Write Attributes	☐	☐
Write Extended Attributes	☐	☐
Delete Subfolders and Files	☐	☐
Delete	☐	☐
Read Permissions	☑	☐

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

Step 24.12 – Click **OK** and your resulting screen should resemble the one below.



Advanced Security Settings for WINDOWS

Permissions | Auditing | Owner | Effective Permissions

To view more information about special permissions, select a permission entry, and then click Edit.

Permission entries:

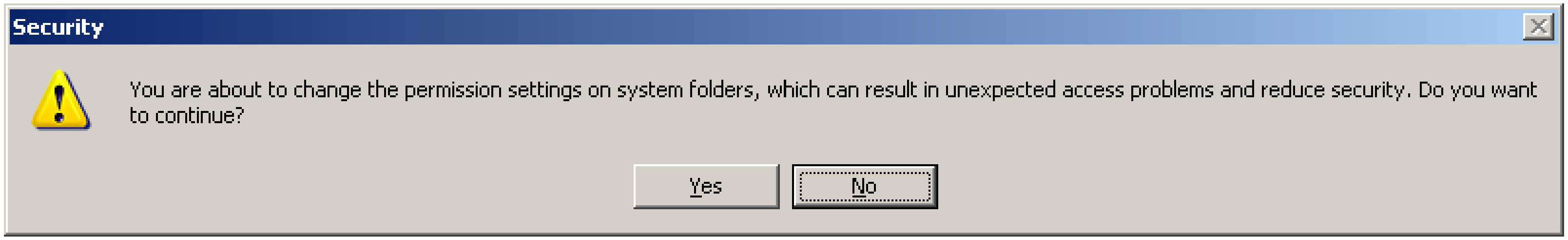
Type	Name	Permission	Inherited From	Apply To
Allow	Internet Guest Account...	Read & Execute	<not inherited>	This folder only
Deny	Internet Guest Account...	Full Control	C:\	This folder, subfolders...
Allow	Administrators (DMZTE...	Full Control	C:\	This folder, subfolders...
Allow	CREATOR OWNER	Full Control	C:\	Subfolders and files onl
Allow	SYSTEM	Full Control	C:\	This folder, subfolders...
Allow	Users (DMZTEST\Users)	Full Control	C:\	This folder, subfolders...

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

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

Learn more about access control.

Step 24.13 – Click **Apply**



Security

You are about to change the permission settings on system folders, which can result in unexpected access problems and reduce security. Do you want to continue?

Step 24.14 – Choose **Yes**.

Step 24.15 – Click **OK** to exit the editing mode.

Step 24.16 – Click **OK** to exit the permissions tab.

Step 24.17 – For each path in the below table, repeat the steps **24.7** – **24.16** above.

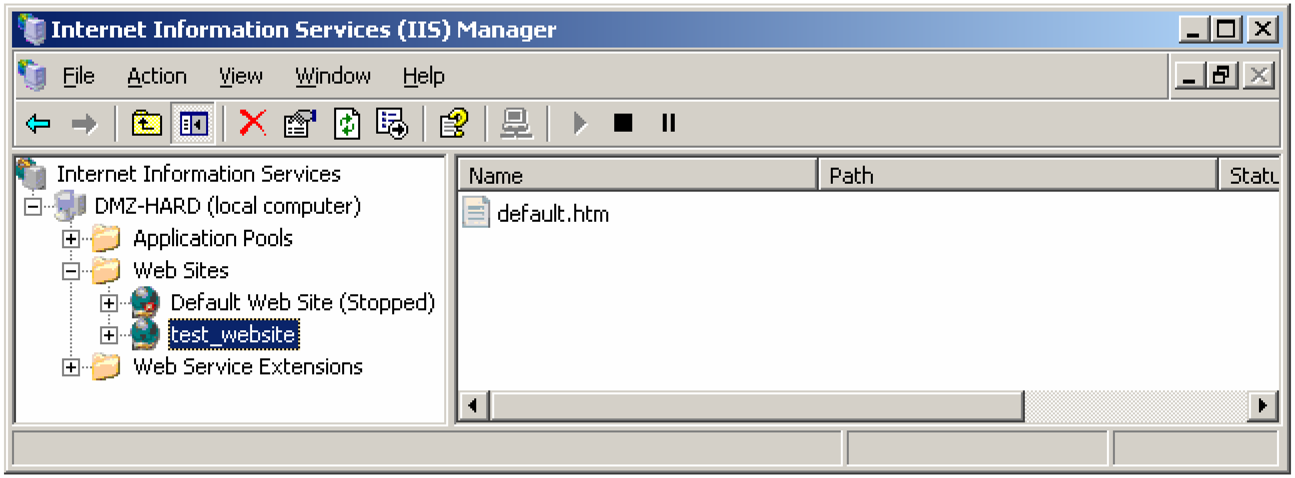
NOTE: Note which folders to apply the permissions to. The 1st column is the directory that you should navigate to and the 2nd column is the collection of folders and files that you should apply these permissions onto.

Directory	**Apply onto**
C:\Windows\System32	This Folder Only
C:\Windows\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

Step 25.0 – Change the Web Site to use the renamed IUSR account and associated password.

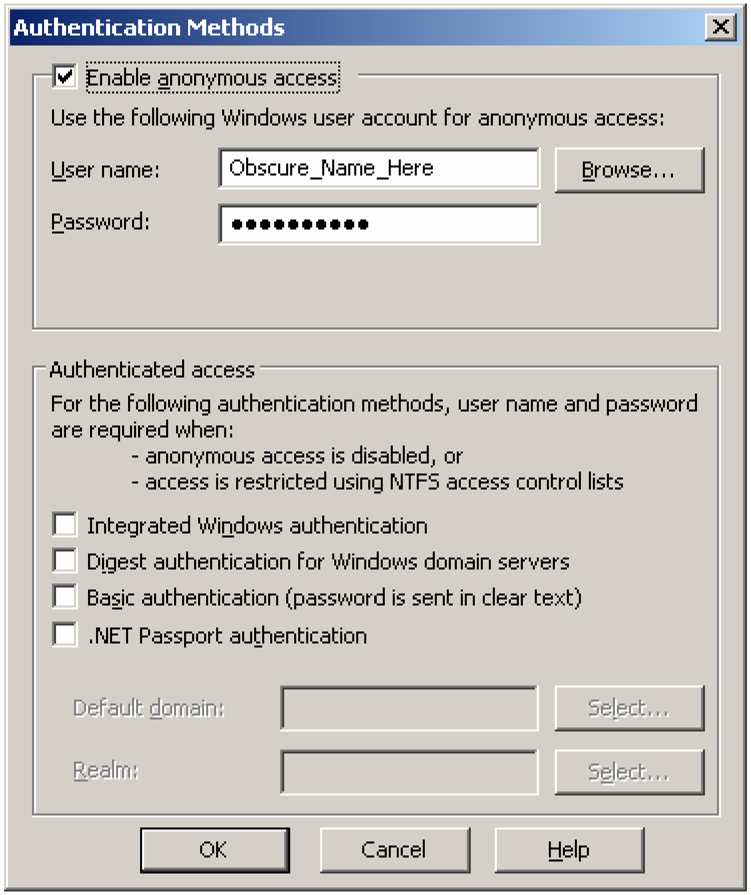
Step 25.1 – Go to **Start** > **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**

Step 25.2 – Expand the trees down to your newly created web site.


Internet Information Services (IIS) Manager
File
Action
View
Window
Help
Internet Information Services
DMZ-HARD (local computer)
Application Pools
Web Sites
Default Web Site (Stopped)
test_website
Web Service Extensions
Name
Path
Statu
default.htm

Step 25.3 – Right click on your newly created web site and choose **Properties** > **Directory Security**

Step 25.4 – Under the **Authentication and access control**, click on **Edit**



☑ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: Obscure_Name_Here

Password: ●●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

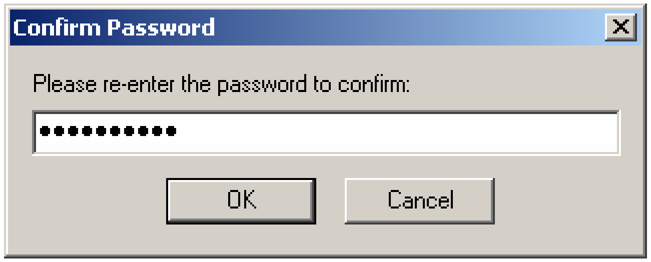
Default domain:

Realm:

Step 25.5 – Ensure that **Enable anonymous access** is checked.

Step 25.6 – For **User Name:** type in the renamed **IUSR_<*machinename*>** account from **Step 23.3**

Step 25.7 – For **Password:** type in the newly created password from **Step 23.6** and click OK



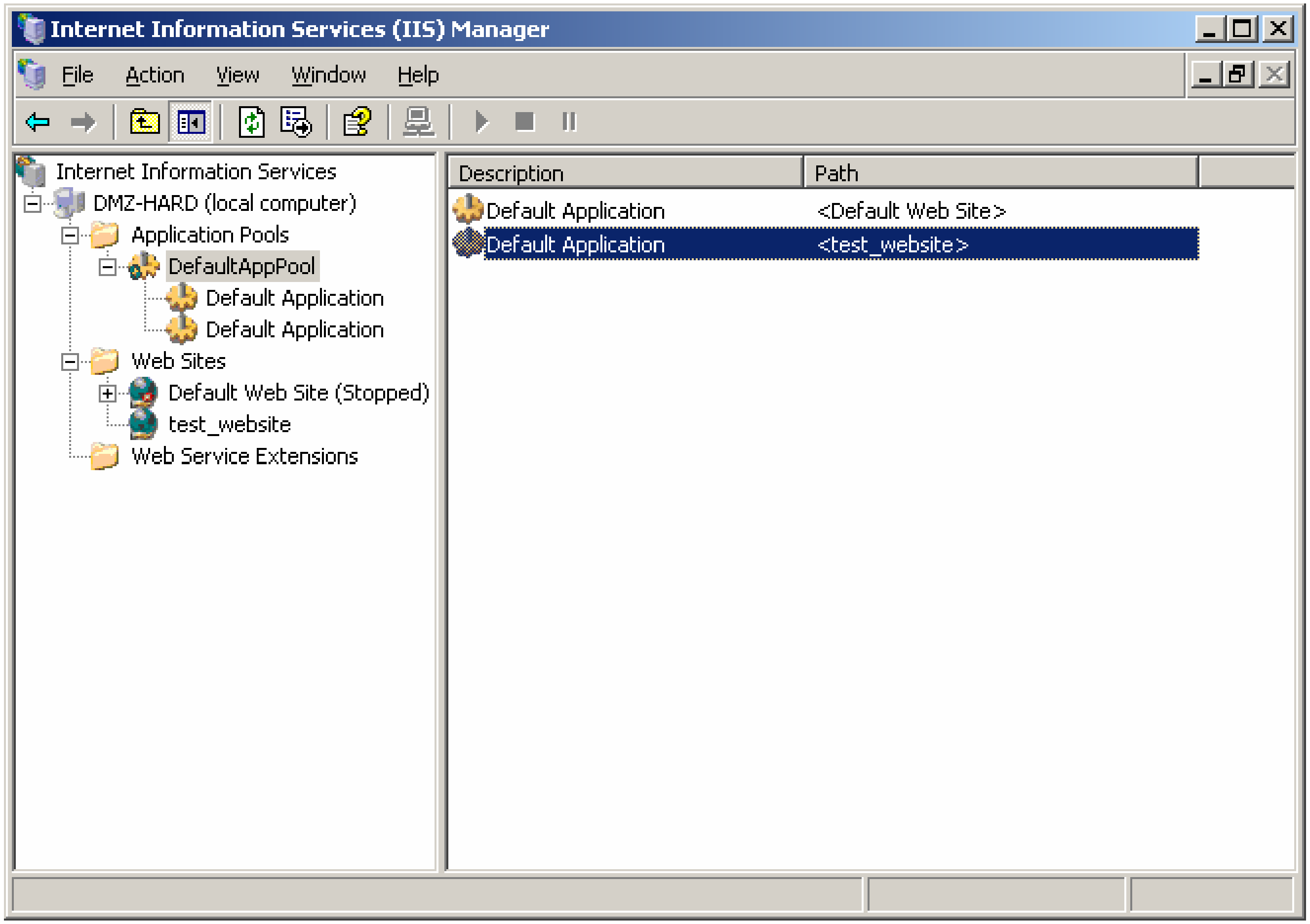
Please re-enter the password to confirm:

●●●●●●●●●●●

Step 25.8 – You will have to re-enter the password again for validation and click **OK**.

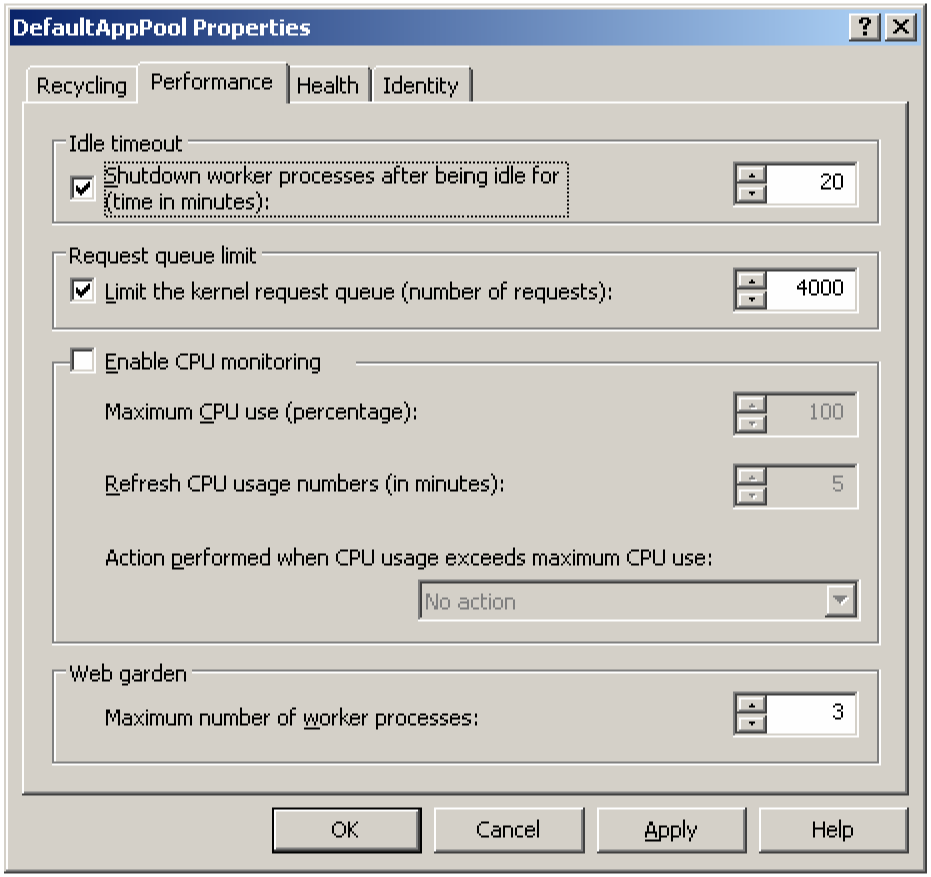
Click **OK** to close the Properties window.

Step 25.9 – Open the **Application Pools** tab and choose the **DefaultAppPool**.



Description	Path
Default Application	<Default Web Site>
Default Application	<test_website>

Step 25.10 – Right click on **DefaultAppPool** and select **Properties > Performance**.



Idle timeout

☑ Shutdown worker processes after being idle for (time in minutes): 20

Request queue limit

☑ Limit the kernel request queue (number of requests): 4000

☐ Enable CPU monitoring

Maximum CPU use (percentage): 100

Refresh CPU usage numbers (in minutes): 5

Action performed when CPU usage exceeds maximum CPU use: No action

Web garden

Maximum number of worker processes: 3

Step 25.11 – Change the value under **Web Garden > Maximum number of worker processes** to 3 and click **OK**.

Step 26.0 – (Optional) Add a robots.txt file to prevent spidering.

Step 26.1 – In the root folder of your newly created website, add a file called robots.txt that includes the following syntax:

```
User Agent: *
Disallow: /
```

Step 27.0 – Firewall rules

Step 27.1 – Have your Network Admin Group 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	**Author**	**Summary of Change**
03/15/2004	Jay Ward	Initial Hardening Guide
04/16/2004	Jay Ward	MS Patch update
10/15/2004	Jay Ward	MS Patch update